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

Margareta Heidt
TU Darmstadt
heidt@is.tu-darmstadt.de

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

Peter Buxmann
TU Darmstadt
buxmann@is.tu-darmstadt.de

Abstract

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

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

1. Introduction

"*Risk analysis techniques (financial costs of event multiplied by probability of event equals exposure) are not appropriate where business survival is at issue"* [1]" – since the early phase of the Information Systems (IS) discipline, researchers and practitioners like the above-quoted Newton (1985) have pointed out the complexity of risk identification, assessment and the subsequent decision-making regarding information systems security and the thus limited applicability of purely statistical and normative approaches.

However, the predominant approach regarding organizational decisions about IT security remains heavily influenced by purely quantitative models and theories that mainly highlight economic aspects of investment decisions [e.g., 2,3,4] but do not consider organizational, environmental, and behavioral aspects (i.e., context). Especially, studies focusing on risk analysis as an aspect of the decision-making process continue to draw on statistical decision theory despite the de facto deviation from this normative approach in practice [e.g., 5]. Recently however, commonly employed cost-benefit analyses [e.g., 6] or the consideration of institutional factors [e.g., 3,7] increasingly acknowledge the presence and influence of economic, organizational or environmental aspects during the IT security decision process.

Meanwhile, decade-old findings from behavioral economics and decision sciences have not been adopted sufficiently by IS researchers as pointed out by former MIS Quartely Editor-in-Chief Paulo Goes [8] or Crossler and colleagues [9]. Both articles reinforce "that the context matters in how the cognitive effects [as stated by behavioral economists] influence the choices" [8, p. vii] and advocate the necessity to consider contextual factors in security and privacy studies given the highly complex nature of current IS environments.

Against this backdrop, this paper proposes a conceptual framework that builds on insights from organizational IT security research before employing a qualitative approach to identify which contextual aspects affect decision-makers in predominantly small and medium-sized enterprises (SME) regarding the decision-making process in organizational IT security through 25 expert interviews. Small and medium-sized enterprises have been particularly overlooked by IS security literature which continues to focus on large enterprises within specific industries, i.e., healthcare and finance [e.g., 7,10] although SME account for more than 95% of enterprises worldwide [11]. Decision-makers in SME however are directly responsible for their businesses' survival which requires them to take various internal and external factors into account and heightens the influence of individual characteristics when deciding upon investing in IT measures in general, and IT security in particular [e.g., 12,13].

URI: https://hdl.handle.net/10125/60049
ISBN: 978-0-9981331-2-6

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

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

2. Theoretical and Conceptual Background

2.1. Phases of IT security decision processes

Our initial theoretical lens employed during the analysis of our qualitative study and the subsequent literature review regarding organizational IT security risk is based upon Straub and Welke's [14] Security Risk Planning Model and Goodhue and Straub's [15] Model for Managerial Perceptions of Security Risk. Whereas the first model consists of 5 phases, namely (1) recognition of security problems, (2) analysis, (3) alternative generation, (4) decisions, and (5) implementation, the latter argues that the organizational and the IS environment along with individual characteristics strongly influence manager perceptions and thus managerial concern about systems risk.

Both models have been extensively referred to in their pure or modified form in various IT security studies [e.g., 16]. The risk planning model in particular can be considered as the foundation of established process models (e.g., ISO 27001) and among the first to build on [15] by taking socio-organizational factors into account. A focus on the role of decision makers and managers highlights the influence of their perception on IT security risks and effective controls on organizational IT systems. Due to its high-level conceptual management approach and its recognition of socio-organizational factors such as the IS environment and managerial characteristics, their model provides the core of our conceptual framework. This framework helps to later on identify and contextualize aspects that influence decision-making processes regarding IT security investments.

2.2. Organizational decision-making

Decision-making processes in general are usually categorized through the distinction between a normative or descriptive approach [17]. Whereas a normative approach focuses on how decisions *should* be made by employing mathematical models and assuming rational stakeholders, descriptive decision theories attempt to depict how decisions are *actually* made. In his seminal work on decision-making in businesses, Herbert Simon states that "if human decision makers are as rational as their limited computational capabilities and their incomplete information permit them to be, then there will be a close relation between normative and descriptive decision theory" [17, p.499] before arguing for the existence of bounded rationality and the influence of external factors. Thus, the close relation between both theory types is attenuated and the influence of external factors such as legal and social structures promoted. In this regard, IS studies which employ an Institutional Theory approach, have investigated and demonstrated the influence of environmental aspects such as conformity with external norms and social influence on investment decisions [7,18].

Against this backdrop, a plethora of studies in business investment decisions either follow classic economic approaches such as cost-benefit analyses or value estimations or build on Contingency Theory or a Resource-Based View which acknowledge the distinct influence of external factors such as available resources or organizational structures [19,20,21].

Based on these findings and influenced by Dor and Elovici's categories [20], we aggregate influencing factors into behavioral/cognitive aspects, organizational aspects, environmental aspects, and economic aspects and presuppose their influence on the IT security decisions process introduced by Straub und Welke [21] as illustrated in the following Figure 1.

In addition, we make a further distinction within the decision phase and propose four nuances as the decision can either be fundamental, i.e., (1) the initial adoption decision whether to invest at all (Y/N), or directed at the specifications of the intended IT security investment, i.e., (2) where/into what to invest (area or content of investment like recovery or prevention measures on an abstract level; one- or two-factor authentication on a more detailed level), (3)

from whom or where to source (self-developed or selection of provider), and (4) how much to invest (level or extent of the investment). These nuances are also depicted in Figure 1.

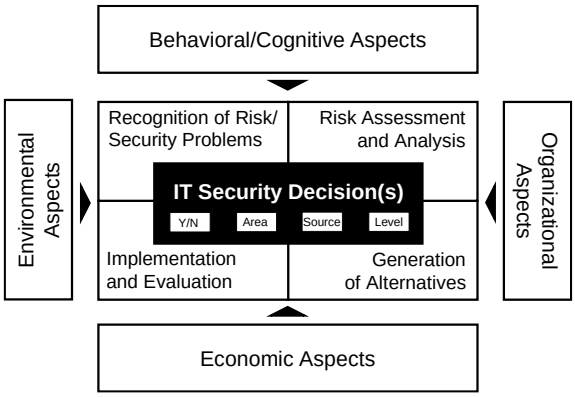

Figure 1: Conceptual Framework of Literature Analysis

3. Research Methodology

The conceptual framework is first applied during the analysis of an interview study and the subsequent literature review. Therefore, a robust and versatile method like content analysis can serve both as a tool to analyze qualitative data derived through interviews and in order to review relevant literature thoroughly and comprehensibly [e.g., 22,23]. While this paper predominantly employs a directed content analysis approach as we build on prior research about decision-influencing factors to validate our conceptual framework, we also draw on inductive aspects of conventional content analysis to allow for new insights to emerge from the data [23].

3.1 Research design, sample, and coding process

Drawing on guiding principles for qualitative IS studies [24], we collected our data within a European country through semi-structured interviews with a total of 26 participants from 25 organizations in six industries (namely manufacturing; construction; wholesale and retail; information and communication; professional, scientific and technical activities; administrative and support service; education). These participants were either managing directors (14), IT executives (8), business developers (2), or consultants (2). Whereas 19 experts are employed in pure user companies, 5 experts work in IT provider companies and 2 experts in hybrid companies that offer IT services in addition to their traditional (non-IT) product portfolio. Disregarding one company with roughly 660 employees worldwide but less than 250 in the sample country, all other companies can be unconditionally classified as SME with 28 % medium-sized (50-250 employees), 52% small (10-49 employees), and 16% very small enterprises (1-9 employees). The data collection took place between November 2017 and March 2018 and resulted in over 30 hours of recorded interviews, which were transcribed after mutual agreement and analyzed with the software analysis tool NVivo 12 Plus as demonstrated in Figure 2.

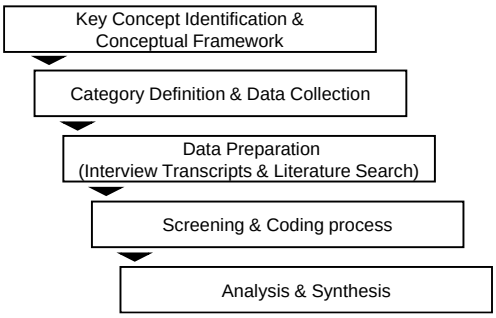

Figure 2: Content Analysis Process (based on [22])

Based on the initial conceptual framework, the transcribed interviews were screened and coded if the description matched the terminology of categories [20]. Following Mayring's steps of deductive category assignment after the initial screen, subcategories were identified, labeled, and iteratively revised in several coding steps [23, p. 96]. The final codes were analyzed through coding comparisons and crosstab queries within NVivo. In order to demonstrate rigor and trustworthiness, our coding process followed a clear research agenda, was critically discussed and assessed with several IS researchers, and the selected interviews stemmed from diverse backgrounds including triangulation by including both a user and a provider perspective. Additionally, direct quotes of the subjects contribute to further transparency and accountability.

3.2. Findings

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

Environmental aspects were mentioned most frequently, in terms of information sharing activities (through mostly informal networks and partnerships),

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

We additionally investigated the overall mentions of all aspects via crosstab queries in order to report the relative share of all four categories for descriptive insights [23]. Whereas environmental aspects were most often mentioned (33.74%), behavioral and cognitive aspects followed at 26.67% and organizational aspects at 25.42%. Economic aspects were less frequently mentioned at 15.34%.

All contextual aspects were further fragmented into the identified subcategories, e.g., environmental aspects were subdivided into micro- and macro-environmental elements such as the influence of the industry, customers or state-level legislation and regulations affecting the organization on an abstract level. Whereas a further subcategory comprising elements of social influence and information sharing relates to the environment of the individual. These subcategories are enriched by verbatim quotes and the identified effect on nuances of the investment decision. By means of example, we could identify that requirements or auditing activities posed by customers or regulations exhibit a strong effect on the initial adoption decision whether to invest at all into IT security and the particular area of investment, e.g., recovery measures such as data backups and archives. Social influence via predominantly non-formal information sharing also directs decision-makers towards the area of investment as well as the sourcing option, i.e., provider selection.

Table 1: Exemplary Qualitative Study Findings

	Manifestation		Effect on Investment Nuance			
	Subcategories and Verbatim Quotes	%	y/n	area	source	level
Environmental Aspects [29,58%]	Micro-Environment	44,15%	+	+	o	o
	"Because customers today actually require […] that you are ISO certified, because they say that they also have to adhere to these terms […]" , Firm I, CIO (User)					
	Macro Environment	31,92%	+	+	o	+
	"It (IT security investment) appears on the agenda with the GDPR and because it is a required course, it gets the necessary priority", Firm J, MD (User)					
	Information Sharing / Social Influence	23,93%	o	+	+	o
	Through our association […] or simply via wisdom-of-the-crowds where we just ask around for experiences like „that's what we need, what would you say?". Or we ask friendly competitors for insights into what they use and why.", Firm M, MD (User)					
+ = stated positive effect ; o = no clearly stated effect ; - = stated negative effect						

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

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

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

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

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

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

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

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

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

4. Literature Analysis

In the following section, we provide an overview of our literature review method and the utilized tools. In order to ensure rigor and replicability, we adhere to clearly defined guidelines through a combination of several approaches prevalent in IS research [25-28]. Our literature review is structured following Okoli and Schabram [28] and visualized in Figure 3:

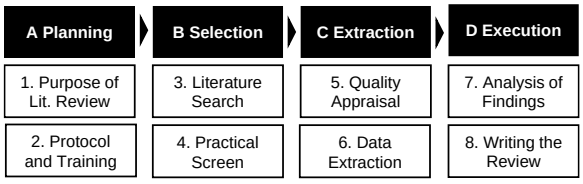

Figure 3: Literature Review Process [28]

4.1. Search and selection strategy

In accordance with Figure 3, we first defined the purpose and review scope before conceptualizing the general topic. The literature search was performed following an explorative search using Business Source Premier and Google Scholar to achieve a better understanding of the topic, synonyms, and the existing research landscape. This resulted in the identification of an appropriate search term as indicated in Table 2. We screened the following databases: AIS Electronic Library (AISeL), Business Source Premier (Ebsco), and Science Direct (SD) along with Web of Science (WoS). Drawing on Cooper [25], we opted for an exhaustive selective coverage and thus searched by title, abstract, and keywords and arrived at 4295 initial total hits including 140 duplicates. During the selection phase, initial title and abstract screening, which served as practical screen, the analyzed literature was drastically condensed. Thus, only a total of 220 articles were further scrutinized during the extraction phase because they explicitly focused on IT security from an organizational rather than technical or legal perspective. A clustering process ensued along with a quality screen that excluded articles that were published outside of leading IS outlets as defined by Lowry [29] leading to a total of 87 remaining articles. Full text-screening was combined with the conceptual framework: all articles which did not or only marginally cover phase 4, i.e., the actual decision phase according to Straub and Welke's model were excluded along with conference proceedings which were subsequently extended into journal publications resulting in a total of 31 articles [e.g., 10,30]. A backward and forward search revealed eight relevant publications which were not identified via the initial search term due to ill-fitting keywords [e.g., 31]. These articles were analyzed following the same approach and criteria.

The rather extreme condensation of the initial total hits can be largely explained with our choice to draw on Cooper [25]. Whereas the search term example aimed at an exhaustive coverage and thus included several keywords that are highly prevalent in numerous studies, the following iterative screening process pursued a selective approach. Selection criteria were mostly determined by the theoretical framework and the resulting focus on the decision process. As a result, publications like Angst and colleagues' investigation of institutional factors in healthcare security investment [7] which detail the evaluation and implementation of investments rather than the decision process leading towards the investment, were excluded. Similarly, Baskerville's [5] study on risk analysis covers only the second phase of Straub and Welke's [14] model and was thus suspended after full text screening. Additionally, literature reviews and meta-studies that primarily systemize IS security literature without identifying further aspects of investment decision [e.g., 16] were omitted from further analysis.

Detailed exclusion criteria such as a focus on end-users or compliance and employees misconduct along

with the exact number of screened articles can be extracted from Table 2.

Table 2: Structured Literature Review [27]

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

4.2 Literature analysis

In contrast to existing literature reviews and meta-studies [e.g., 16,32] on organizational IT security and investment decisions, our analysis is based on a qualitatively validated framework and includes aspects other than only economic valuation or socio-organizational perspectives. Further, the execution phase of the analysis and synthesis stage was performed through a thorough content analysis based on the theoretical framework adapted from Straub and Welke [14] combined with the identified and extended contextual factors and investment nuances derived through the qualitative interview study in SME companies. As opposed to previous literature reviews, a distinct SME perspective – which has been largely neglected by organizational IT security research in general – added another analysis layer. Thus, the analysis of the final selection of all 39 articles which can be found in the online appendix also considered whether the particular study focused on an SME context.

Evidently, most studies largely focus on economic aspects of IT security decisions by proposing a value-at-risk or return on (security) investment approach (ROSI) [e.g., 33-35]. This is also reflected by the slight surplus of predominantly normative studies (56%) based on mathematical modelling (64% proportionately) [2,6,10,33,34,36-54]. Whereas two studies pursue a purely qualitative approach [20,55] and six are purely conceptual [56-61], eleven studies employ a combination of several approaches [4,14,33,35,37,39,40,41,48,51,62] and three are based on panel data [3,31,63].

As already indicated, our search strategy was directed at studies that explicitly focus on the actual (investment) decision, i.e., phase 4 in Straub and Welke's risk planning model [14]. Several studies focus on a specific investment decision, e.g., investing in a particular authentication system [36] or an intrusion detection system [2]. Other studies propose a generic model and use a specific tool or application as example [47,48]. The investment nuances that are most often considered in these specific investment studies, but also in publications that pursue a more generic approach, are the specific area or content and the optimal level of investment [4,10,33,34,47,53,56, 60,62]. Only a single study is dedicated towards to the decision regarding the source or origin of the investment [48] and a total of six studies consider the fundamental decision whether to invest at all [31,38,44,47,54,55].

The extensive focus on investment nuances such as the specific area of the investment (53%) and the optimal level (49%) is often in line with the intended audience or the specific sample of the respective study. This was determined either by analyzing descriptive statistics in the result section (sample) or the stated practical contributions (audience). More than 53% of studies are directed at decision-makers with a pronounced IT focus such as IT executives and CIOs [e.g., 3,4,34] or take a company level perspective [e.g., 10,41,60]. Executives with a non-IT or business background like CEOs, managing directors, and business executives were only considered by a third of all studies, whereas provider or employee perspectives could be found in a total of five studies.

The shortage of studies looking at non-IT decision-makers hints at the non-generalizability of their results for the SME context: many SME executives do not possess a particular IT background or extensive knowledge and could thus be best compared to other non-IT decision-makers. Further, only two of the analyzed studies focus explicitly on the SME context [31,41] and a handful consider organizational aspects like budget constraints and additional resource restrictions such as a limited workforce which are all highly prevalent in SMEs as pointed out by several SME studies [e.g., 12,13,64].

In total, slightly more than half of all analyzed studies consider organizational aspects, most often regarding the available resources in terms of budget or workforce as decision criteria during IT security

investments. Even more prevalent and often directly connected to the aforementioned subcategory of organizational aspects are considerations of budgeting activities and especially cost-benefit analyses (61%). However, only a few studies point out specifically that "the selection of security controls should be driven by business needs" [57, p.185] or that "the security budget is set exogenously by management decision" [38, p.370]. The latter study is one of the few that highlights the necessity of a holistic view that integrates technology and organizational with behavioral aspects.

Even though we did find evidence in 15 studies of behavioral and cognitive aspects, most of them approach decision-making only from a cognitive point of view, i.e., focusing on analytical or deliberative decision-making processes of decision-makers or their risk attitude. Only six studies account for emotional factors or other behavioral aspects like certain managerial character traits [14,20,31,38,40, 61]. With regard to organizational aspects, decidedly fewer studies consider the influence of the micro- (15%) or macro-environment (20%) of the organization or social influence and information sharing (8%) on the decision process. The most prominent subcategory, macro-environment, solely regards regulations or specific legislations to have an impact on investments. However, with the exception of Purser's study [60], this influence is considered to affect the area or content of the analysis (e.g., data protection laws promoting backup strategies) rather than stating the connection of legislations on the fundamental decision to invest altogether.

5. Discussion

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

Similar to Dhillon and Backhouse [16], our literature analysis demonstrates how current IS security research still heavily relies on normative approaches assuming purely rational decision-makers or the existence of formalized decision processes. Contrary to these assumptions, evidence from organizational research, behavioral economics and more recently neuroscience demonstrates how decision-makers draw on a variety of cognitive shortcuts such as heuristics and biases [e.g., 8,64], how decisions are better approximated by behavioral game theory which takes individual characteristics, time perspectives, and trade-offs into account [66], and how a multitude of factors is usually consulted in organizational IS decision-making [e.g., 17].

Particularly in an SME context, findings from our qualitative study suggest that decision-makers are heavily influenced by their environment, individual characteristics, and certain characteristics of their organization, in particular resource constraints regarding budget, workforce, but also time and knowledge. These factors in turn restrain the use of economic tools and methods like ROI estimations which prevail in the analyzed studies [e.g., 33-35]. Exemplary, many managing directors in a dual role mentioned that they are aware of cost-benefit analyses and ROI or even ROSI estimations but limited time and often inadequate data necessary for such economic calculations are hindering their application in practice.

Surprisingly, the majority of interviewed companies do not perform IT budgeting and investments in IT, or more specifically in IT security, are often viewed as exclusive expense associated with no visible benefit. Decision-making processes thus include cost (rather than benefit) analyses, but the final decisions are often based on gut feeling rather than 'number-crunching'. Additionally, we found evidence that the often stated long-term orientation of family-owned or small businesses does not seem to influence decision-making even though previous entrepreneurial research suggests that investment activities are directed at wealth preservation for future generation [e.g., 67,68]. Furthermore, current research is negligent of the multitude of role-identities, i.e., owner as general manager and head of IT. Role-identities, however, have been shown to impact the evaluation and selection of business opportunities and economic decisions [69,70] and their influence was confirmed through our qualitative approach. Individual or behavioral aspects like these remain largely disregarded in studies IT security decisions and could not be identified during our literature review.

A further discovery is the importance of environmental aspects on IT security decisions: interviewees very often mentioned how customer requirements and frequent quality audits "forced" them to adopt certain data protection and recovery security measures or to establish security policies and processes. Similarly, state-level interventions in terms of regulations also transpired to be the origin of fundamental IT security decisions and defined the area and level of investment. These factors along with social influence are largely neglected by extant IS security research even though peer influence has been consistently shown to impact organizational decision-making [71]. Especially, the GDPR appeared to have rather large rippling effects as decision-makers in SME feel forced to deal with data protection and security issues in order to avoid possible sanctions. Whereas individual IT security research has, for example,

employed General Deterrence Theory to account for such mechanisms [72], current organizational research in this regard has overlooked how regulation affects certain nuances of IT security investment decisions.

Regarding the influence of customers, we could identify first evidence into how IT security investments are increasingly considered as a potential profit center by younger firms in our SME sample. These firms regard IT (security) investment as an economic opportunity or incentive which could increase customer loyalty or acquisition – a point of view that is seldom accounted for by IT security studies [9].

6. Conclusion, Limitations, and Future Research

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

The contribution of this paper is twofold: first, our qualitative analysis not only confirms the assumption that IS security decision-making processes are affected by various contextual aspects [e.g., 20,61] but zooms in on the particular context of SME and thus uncovers the most prevalent and significant influencing aspects in this – still rather neglected – context. Further, we identify that these aspects also vary in their influence on investment nuances which could serve as a first step to uncover the reasons why SMEs still refrain from investing in IT security [73].

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

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

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

7. Acknowledgments

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

8. References

[1] Newton, J., “Strategies for Problem Prevention,” IBM Systems Journal, 24(3/4), 1985, pp. 248-263.

[2] Cavusoglu, H., B. Mishra, and S. Raghunathan, “A model for evaluating IT security investments,” Communications of the ACM, 47(7), 2004, pp. 87-92.

[3] Cavusoglu, H., H. Cavusoglu, J.Y. Son, and I. Benbasat, “Institutional pressures in security management. Direct and indirect influences on organizational investment in information security control resources,” Information & Management, 52(4), 2015, S. 385-400.

[4] Bodin, L.D., L. Gordon, and M.P. Loeb, “Evaluating information security investments using the hierarchy,” Communications of the ACM, 48(2), 2005, pp. 79-83.

[5] Baskerville, R., “Risk analysis as a source of professional knowledge,” Computers & Security, 10(8), 1991, pp. 749-764.

[6] Khansa, L. and D. Liginlal, “Quantifying the Benefits of Investing in Information Security,” Communications of the ACM, 52(11), 2008, pp. 113-117.

[7] Angst, C.M., E.S. Block, J.D’Arcy, John, and K Kelley, “When do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches,” MIS Quarterly, 41(3), 2017, pp. 893-916.

[8] Goes, P.B., “Editor's comments: information systems research and behavioral economics,” MIS Quarterly 37(3), 2013, pp. iii-viii.

[9] Crossler, R.E., A.C. Johnston, P.B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "Future directions for behavioral information security research," Computers & Security, 32, 2013, pp. 90-101.
[10] Huang, C.D., R.S. Behara, and J. Goo, "Optimal information security investment in a Healthcare Information Exchange. An economic analysis," Decision Support Systems 61, 2014, pp. 1-11.
[11] Organization for Economic Co-operation and Development, "Small Businesses, Job Creation and Growth: Facts, Obstacles and Best Practices", Paris, 1997.
[12] Thong, J.Y.L, C.S. and Yap, "CEO Characteristics, Organizational Characteristics and Information Technology Adoption in Small Businesses," Omega International Journal of Management Science, 23(4), 1995, pp. 429-442.
[13] Dholakia, R.R. N. Kshetri, "Factors impacting the adoption of the Internet among SMEs," Small Business Economics 23(4), 2004, pp. 311-322.
[14] Straub, D.W. and R. Welke, "Coping with Systems Risk. Security Planning Models for Management Decision Making," MIS Quarterly, 22(4), 1998, pp. 441-469.
[15] Goodhue, D.L. and D. W. Straub, "Security concerns of system users: a study of perceptions of the adequacy of security," Information & Management, 20(1), 1991, pp.13-27.
[16] Dhillon, G. and J. Backhouse, "Current directions in IS security research: towards socio-organizational perspectives," Information Systems Journal, 11(2), 2001, pp. 127-153.
[17] Simon, H.A. "Rational decision making in business organizations," The American Economic Review, 69(4), 1979, pp. 493-513.
[18] Salge, T.O., R. Kohli, and M. Barrett, "Investing in Information Systems: On the Behavioral and Institutional Search Mechanisms underpinning Hospitals Investment Decisions," MIS Quarterly, 39(1), 2015, pp. 61-90.
[19] Vroom, V.H. and P.W. Yetton, Leadership and decision-making, University of Pittsburgh Press, Pittsburgh, 1973.
[20] Dor, D. and Y. Elovici, "A Model of the Information Security Investment Decision Making Process," Computers & Security, 63, 2016, pp. 1-13.
[21] Weishäupl, E. E. Yasasin, and G. Schryen, "Information security investments: an exploratory multiple case study on decision-making, evaluation and learning," Computers & Security, in press, 2018.
[22] Hsieh, H.F. and S.E. Shannon, "Three Approaches to Qualitative Content Analysis," Qualitative Health Research, 15(9), 2005, pp. 1277-1288.
[23] Mayring, P., Qualitative content analysis: theoretical foundation, basic procedures and software solution, Klagenfurt, 2014.
[24] Sarker, S., X. Xiao, and T. Beaulieu, "Qualitative studies in information systems: a critical review and some guiding principles," MIS Quarterly, 37(4), 2013, pp. iii-xviii.
[25] Cooper, H.M., "Organizing Knowledge Syntheses: A Taxonomy of Literature Reviews," Knowledge in Society, 1, 1988, pp. 104-126.
[26] Webster J. and R.T. Watson, "Analyzing the Past to Prepare for the Future: Writing a Literature Review," MIS Quarterly, 26(2), 2002, pp. xiii-xxiii.
[27] vom Brocke, J., A. Simons, B. Niehaves, B. Niehaves, K. Reimer, R., Plattfaut, and A. Cleven, "Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process," Proceedings of the 9th European Conference on Information Systems, 2009, pp. 2206-2217.
[28] Okoli, C. and K. Schabram, "A Guide to Conducting a Systematic Literature Review of Information Systems Research," Sprouts: Working Papers on Information Systems, 10(26), 2010, pp. 1-46.
[29] Lowry, P., D. Romans, and A. Curtis, "Global journal prestige and supporting disciplines: A scientometric study of information systems journals," Journal of the Association for Information Systems, 5(2), 2004, pp. 29-80.
[30] El-Gayar, O.F. and B.D. Fritz, "A web-based multi-perspective decision support system for information security planning," Decision Support Systems, 50(1), 2010, pp. 43-54.
[31] Lee, Y. and K.R. Larson, "Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software," European Journal of Information Systems, 18(2), 2009, pp. 177-187.
[32] Schatz, D. and R. Bashroush, "Economic valuation for information security investment: a systematic literature review," Information Systems Frontiers, 19(5), 2017, pp. 1205-1228.
[33] Lee, Y.L., R. Kauffman, and R. Sougstad, "Profit-maximizing firm investments in customer information security," Decision Support Systems, 51(4), 2011, pp. 904-920.
[34] Sawik, T. "Selection of optimal countermeasure portfolio in IT security planning," Decision Support Systems, 55(1), 2013, pp. 156-164.
[35] Wang, J., A. Chaudhury, and H.R. Rao, "A value-at-risk approach to information security investment," Information Systems Research, 19(1), 2008, pp. 106-120.
[36] Altinkemer, K. and T. Wang, "Cost and Benefit Analysis of Authentication Systems," Decision Support Systems, 51(3), 2011, pp. 394-404.
[37] H. Cavusoglu, S. Raghunathan, and W.T Yue, "Decision-theoretic and game-theoretic approaches to IT security investment," Journal of Management Information Systems, 25(2), 2008, pp. 281-304.
[38] Dutta, A. and R. Roy, "Dynamics of organizational information security," System Dynamics Review, 24(3), 2008, pp. 349-375.
[39] Ekenberg, L., S. Oberoi, and I. Orci, "A Cost Model for Managing Information Security Hazards," Computers & Security, 14(8), 1995, pp. 707-717.
[40] El-Gayar, O.F. and B.D. Fritz, "A web-based multi-perspective decision support system for information security planning," Decision Support Systems, 50(1), 2010, pp. 43-54.
[41] Fielder, A., E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment," Decision Support Systems 86, 2016, pp. 13-23.
[42] Finne, T., "The Three Categories of Decision-Making and Information Security," Computers & Security, 17(5), 1998, pp. 397-405.
[43] Gordon, L.A., M.P. Loeb, "Economic aspects of information security. An emerging field of research," Information Systems Frontiers, 8(5), 2006, pp. 335-337.

[44] Grossklags, J., N. Christin, and J. Chuang, "Security Investment (Failures) in Five Economic Environments: A Comparison of Homogeneous and Heterogeneous User Agents," Proceedings of the 7th Workshop on the Economics of Information Security, 2008, pp. 160-169.
[45] Guarro, S.B. "Principles and Procedures of the LRAM Approach to Information Systems Risk Analysis and Management," Computers & Security, 6(6), 1987, pp. 493-504.
[46] Gupta, M., J. Rees, A. Chaturvedi, and J. Chi, "Matching information security vulnerabilities to organizational security profiles. A genetic algorithm approach," Decision Support Systems, 41(3), 2006, pp. 592-603.
[47] Herath, H.S.B. and T.C. Herath, T, "Investments in Information Security. A Real Options Perspective with Bayesian Postaudit," Journal of Management Information Systems, 25(3), 2008, pp. 337-375.
[48] Kim, S and H.J. Lee, "A Study on Decision Consolidation Methods Using Analytic Models for Security Systems," Computers & Security, 26(2), 2007, pp. 145-153.
[49] Kolfal, B., R.A. Patterson, and M.L. Yeo, "Market Impact on IT Security Spending," Decision Sciences, 44(3), 2013, pp. 517-56.
[50] Liu, D, Y. Ji, and V. Mookerjee, "Knowledge sharing and investment decisions in information security," Decision Support Systems, 52 (1), 2011, pp. 95-107.
[51] Miller, S., C. Wagner, U. Aickelin, and J.M. Garibaldi, "Modelling Cyber-Security Experts' Decision Making Processes Using Aggregation Operators," Computers & Security (62), 2016, pp. 229-245.
[52] Nazareth, D.L. and J. Choi, "A system dynamics model for information security management," Information & Management, 52 (1), 2015, pp. 123-134.
[53] Rees, L.P., J.K. Deane, T.R. Rakes, and W.H. Baker, "Decision support for Cybersecurity risk planning," Decision Support Systems, 51 (3), 2011, pp. 493-505.
[54] Ryan, J.J. and D.J. Ryan, "Expected Benefits of Information Security Investments," Computers & Security, 25(8), 2006, pp. 579-588.
[55] Qian, Y., Y. Fang, and J.J. Gonzalez, "Managing Information Security Risks During New Technology Adoption",Computers & Security, 31(8), 2012, pp.859-869.
[56] Baker, W.H. and L.P Rees, and P.S. Tippett, Necessary measures - Metric-driven information security risk assessment and decision making," Communications of the ACM, 50 (10), 2007 S. 101-106.
[57] Barnard, L. and R. van Solms, "A Formalized Approach to the Effective Selection and Evaluation of Information Security Controls," Computers & Security, 19(2), 2000, pp. 185-194.
[58] Baskerville, R., "Information Systems Security Design Methods: Implications for Information Systems Development," ACM Computing Surveys, 25(4), 1993, pp. 375-414.
[59] Kwok, L. and D. Longley," Information Security Management and Modelling," Information Management & Computer Security, 7(1), 1999, pp. 30-40.
[60] Purser, S.A. "Improving the ROI of the Security Management Process," Computers & Security, 23(7), 2004, pp. 542-546.
[61] Wood, C.C. "A Context for Information Systems Security Planning," Computers & Security, 7(5), 1988, pp. 455-465.
[62] Fenz, S., A. Ekelhart, and T. Neubauer, "Information Security Risk Management. In Which Security Solutions is it Worth Investing?," Communications of the Association for Information Systems, 28, 2011, pp. 329-356.
[63] Young, R.F. and J. Windsor, "Empirical Evaluation of Information Security Planning and Integration," Communications of the Association for Information Systems, 26 (1), 2010, pp. 245-266.
[64] Salavou, H., G. Baltas, and S. Lioukas, "Organisational innovation in SMEs: The importance of strategic orientation and competitive structure," European Journal of Marketing, 38(9/10), 2004, pp. 1091–1112.
[65] Kahneman, D. "Maps of bounded rationality: Psychology for behavioral economics," American economic review, 93(5), 2003, pp. 1449-1475.
[66] Camerer, C.F., "Strategizing in the brain," Science, 300(5626), 2003, pp. 1673-1675.
[67] Lumpkin, G.T, and K.H. Brigham, "Long–Term Orientation and Intertemporal Choice in Family Firms," Entrepreneurship Theory and Practice, 35(6), 2011, pp.1149-1169.
[68] Zellweger, T., "Time horizon, costs of equity capital, and generic investment strategies of firm," Family Business Review, 20(1), 2007, pp. 1-15.
[69] James, H.S., "Owner as manager, extended horizons and the family firm," International journal of the economics of business, 6(1), 1999, pp. 41-55.
[70] Mathias, B.D. and D.W. Williams, "The impact of role identities on entrepreneurs' evaluation and selection of opportunities," Journal of Management, 43(3), 2014, pp. 892-918.
[71] Aral, S. and D. Walker, "Creating Social Contagion through Viral Product Design: A Randomized Trial of Peer Influence in Networks," Management Science, 57(9), 2011, pp. 1623-1639.
[72] Lebek, B., J. Uffen, M. Neumann, B. Hohler, and M. Breitner,"Information security awareness and behavior: a theory-based literature review," Management Research Review, 37(12), 2014, pp.1049-1092.
[73] Zurich. 2017. "As Many as 875,000 UK SMEs Suffer Cyber Security Breach in the Last 12 Month." Retrieved 04/03/2018, from 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.