Tensions that Hinder the Implementation of Digital Security Governance

Stef Schinagl, Svetlana Khapova, Abbas Shahim

Tensions that hinder the implementation of digital security governance

Stef Schinagl[0000-0002-4455-7287], Svetlana Khapova [0000-0002-6842-6644], and Abbas Shahim

[1] {s.schinagl, s.n.khapova, a.shahim}@vu.nl

Abstract. Today's organizations are exposed to high risk because the established digital technologies are vulnerable to security attacks. The increased impact of security on business demands a strategic approach to information security, commonly referred to as digital security governance. While there is a growing understanding that digital security is one of the leading risks and challenges of today's organizations, organizations still find it difficult to implement security governance as part of their regular organizing change activities. This study focuses on providing more empirical insight into "tensions that are present during the implementation of digital security governance".

We conducted an inductive study and interviewed 42 CISOs and CIOs of large organizations in the Netherlands. The study reveals the tensions that hinder the implementation of digital security governance. We draw from management theories to provide a fresh understanding of and guidance for how to unravel the tensions.

Keywords: Information Security Governance, Information Security Implementation, Digital Security, Digital Transformation, Digital Security Governance

1 Introduction

Recent studies argue that digital security is becoming of strategic importance in contemporary firms [1, 7, 13, 21]. Specifically, these studies argue that governance needs to be organized around digital security. This is because businesses have become technology centered as a result of digital transformation. Businesses are now exposed to high risk because established digital technologies are vulnerable to security attacks [13, 16]. Security attacks increasingly have direct business impacts and costs and therefore force boards to consider alternative ways to govern security and anticipate the growing number of attacks. To this extent, security governance approaches must fundamentally shift from being an isolated technical issue to being a strategic business issue. In this way digital security governance is positioned and implemented as an institutionally wide effort that supports digital business strategies and business innovation [8, 16].

While many organizations understand the need to transform their current security governance approaches so that they fit the digital era, few of them succeed, have trouble with adoption, or lack behind in implementing their security approaches [1, 6, 21]. For example, according to the 2020 Thales Data Threat Report[1], organizations remain

[1] https://cpl.thalesgroup.com/data-threat-report

cognitively dissonant of security. Organizations believe that they are secure when they are not implementing the processes and investing in the technologies required to appropriately protect their organization. Most often, security implementation is mistakenly seen as an isolated, separate and disintegrated activity from business [1, 13, 16]. This means that security remains a concern of the IT department instead of the collaborative business function that is part of the company's DNA.

Additionally, in research, security remains an underexposed concern of digital transformation. In particular, most studies have not comprehensively or clearly explained the processes of establishing security governance in organizations or provided guidelines for its implementation [6, 21]. Implementing security governance remains difficult in complex connected digital environments because of "cutting ties", i.e., tensions [14]. Conflicts between information security values and work efficiency are the most common [5]. An example is the tension between simultaneously maintaining a high pace of innovation and securing one's business.

Security governance research still lacks an empirical and theoretical understanding of its implementation in a digital context [9, 13]. Therefore, why do organizations still find it difficult to implement security governance as part of their regular organizing change activities when digital security is one of the top priorities and challenges of today's organizations? In particular, what tensions occur during the implementation phase of digital security governance?

Our inductive study prompts us to address the research gap within the "digital security governance" phenomenon. To accomplish this, we collected data via 42 interviews with Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs) working in large organizations in the Netherlands. Our data reveal that although there is a common understanding of a "need for change" in digital security approaches, there are tensions that hinder the implementation of digital security in organizations. The tensions are mainly determined by the digital context. We have consolidated our research findings to a data structure based on the Gioia methodology [3], as shown in figure 1, 2 and 3. To explain the data, we draw from management and organization theories that help describe the theoretical tensions presented in this paper.

This paper continues with a brief overview of related research. Then, after explaining our methods, we provide an in-depth analysis of our empirical findings describing three tensions. As our aim is to build theory, each tension includes a brief theoretical background. Then, on that basis, we explain the theoretical tensions that exist in the digital security governance implementation phenomenon. The study concludes with a discussion of the implications of our findings and suggestions for future research that these findings present.

2 Related research: digital security governance

Security governance research has seen a steady progression, moving from a narrow focus on "technical controls" towards a more holistic approach, including organizational and behavioral or social elements [13]. Yet, in today's technology driven environments, organizations are required to consider information security at a strategic

(board) level to achieve the organization's sustainability and its protection [1, 6, 13, 21]. In recent literature, this strategic consideration of information security in the digital context is referred to the concept called digital security governance [1, 9, 13]

Digital security governance is achieved by "steering", or direct & controlling [19] the system by which security is embedded in the organizational structures, and in all of the related business dimensions and organizational factors as a whole (machines, people, objects, processes et cetera). Such a security throughout the firm approach is seen as the key to improve the level of security in contemporary organizations [8, 13].

However, security governance literature is relatively immature, i.e. largely descriptive and provides both limited practical and theoretical guidance [6, 13, 14]. In particular, studies lack empirical understanding about the processes of establishing security governance in organizations or provided guidelines for its implementation [6, 21].

In this study we bridge this research gap and provide empirical insight on implementation tensions. As explained earlier, implementing digital security governance in complex connected digital environments remains difficult because conflicting forces often exist that reveal tensions [14, 15]. Focusing on tensions can provide important insights for both researchers and practitioners, helping them to become aware of possible tensions in security governance designs as well of coping strategies and practices to tackle these tension. We believe by providing this research lens on tensions we gradually help to build knowledge that offers a deeper understanding in the security governance phenomenon.

3 Methods

We applied a qualitative research approach to inductively develop the tensions in digital security governance implementation. This approach is in line with the principles of an iterative approach to qualitative research – in particular, grounded theory. Concerning this inductive research approach, it may seem contradictory that we offer a brief overview of the relevant literature in each of the tensions presented in the findings section. However, because the question addressed in this study had yet to be investigated, our primary objective was to inductively identify the tensions that hinder the implementation of security governance. Hence, although we draw from different management theories to clarify and explain the tensions, as our vantage point we used a grounded theory approach to identify the tensions from our interview data, without being aware of the theories yet.

To analyze our data, we applied the Gioia methodology, which comprises three different levels of abstraction and is tailored to inductive inquiry [3]. We began by openly coding, grouping and classifying the individual descriptions that our informants provided as 'interview samples' to perform a first-order analysis. Our next step was to perform a second-order analysis by comparing these categories and examining the patterns that emerged. This analysis provided the basis on which we developed our third-order theoretical propositions e.g. the tensions. We created a data structure for each tension as described in the findings section below, as shown in figure 1, 2 and 3.

3.1 Data collection

The first author collected qualitative data in three stages between May 2019 and February 2020 (10 months) in the form of 42 semistructured interviews. The interviews were conducted mainly face-to-face or by telephone (#3), were tape-recorded, and were fully transcribed. In total, the data sample includes 39 different companies as sometimes both the CIO and CISO were interviewed. Most of the semistructured interviews were held in Dutch, and some were held in English. The interviews lasted between 25 and 99 min (an average of approximately 60 min).

To build trust and to allow a higher probability of uncovering rich data, we ensured all interviewees' anonymity in the data analysis. Additionally, we strived for transparency, so the transcripts were sent back to the participants for review. If corrections to the transcript were suggested, they were primarily related to the use of popular language about the company, their boss or information about sensitive cases. This did not impact the data's richness as we are more interested in understanding the abstract level of security governance tensions within the organizations.

3.2 Research context

Our empirical data are collected from large organizations in the Netherlands. In particular, the Netherlands is an interesting research context for this study. On the one hand, the Netherlands proves to be in the top 10 countries in digital competitiveness[2]. On the other hand, the Netherlands is not a frontrunner in cybersecurity[3]. In this context, we believe to find rich data on implementation tensions as organizations in the Netherlands are working to shift their security approaches fitted for the digital business processes. Additionally, we focus on large organizations as they have high-risk profiles due to the processing of large quantities of personal data and large financial streams. This context makes it more likely for organizations to truly cope with information security.

3.3 Research process

We increased the analytical rigor by dividing our investigation into three subsequent research phases. Dividing the data sample in three different phases provided direction for understanding the problem of the research phenomenon.

Table 1. informants and phases

Phases	CISOs	CIO or CTO	Other (experts)	Total
Phase 1	2	2	2	6
Phase 2	11	3	3	16
Phase 3	20			20
Phases 1 to 3	**33**	**5**	**5**	**42**

[2] https://www.imd.org/globalassets/wcc/docs/release-2020/digital/digital_2020.pdf

[3] http://www3.wefrum.org/docs/GCR2018/05FullReport/TheGlobalCompetitivenessReport2018.pdf

In the first phase, the research goal was to collect data, via a case study, from technology-driven organizations with both security-oriented informants and informants with business roles. We expected to find rich data on how digital security was organized in fast, innovative and agile environments. In the exploratory phase, six face-to-face interviews with informants were conducted via semistructured interviews. First, we found that the research approach was possibly too narrow to obtain an in-depth understanding of how and why security was organized and that talking with mainly business informants would not lead to an in-depth conversation or understanding of security in the organization. Additionally, informants commented on the narrow research context. This led us to adapt the research approach.

In the second phase, the research approach was therefore an qualitative study seeking to obtain a better understanding of how security was organized across different sectors and large organizations in the Netherlands. CISOs were interviewed across a variety of sectors: healthcare, maritime, financial, technology, e-commerce, education, government and utilities. We also interviewed prominent experts e.g. journalist, lecturers, researchers and public figure[4]. These interviews helped us collect data and gradually build our knowledge of the field. In this phase, 16 interviews were conducted, of which 13 were face-to-face interviews and 3 interviews were conducted by phone. In multiple cases, after asking the opening question "can you describe how information security is organized?", the informants started describing or emphasizing the "digital transformation" that the organization is currently in and how this affects the way security is governed, organized and implemented. By the end of the second phase, we identified "tensions" that informants discussed in relation to the rapidly changing environment, such as security vs. innovation, business, and awareness.

In the third phase, we continued the inductive study but further narrowed it down by only interviewing CISOs of large organizations in the Netherlands. We interviewed CISOs because they best fit the criteria to be "knowledgeable agents", namely, that people in organizations know what they are trying to do and can explain their thoughts, intentions, and actions. In the third phase, we conducted 20 face-to-face interviews. In this phase, we did not use the semistructured interview protocol and mainly focused on discussing the tensions found in phase two to provide a richer understanding of their presence and impact.

It was not until the end of analyzing and discussing the data in more depth that we could clearly identify the empirical story of the digital security governance phenomenon and theoretical tensions that occur in relation to the implementation phase. This is where the role of the second and third authors contributed to the collaborative team as they adopted an outsider's perspective—a devil's advocate whose role was to critique interpretations [3].

[4] Experts also have experience in CISO positions but often where self-employed or ex CISO of large organizations. We named them experts to be transparent about the fact they do not currently work in large-organizations.

4 Findings

In our findings section, we present an informative story of the theoretical tensions that are present in the data on the digital security governance phenomenon. These tensions are present due to the current digital 'force' that pushes organizations to transform their security approaches. The theoretical tensions reveal and explain why organizations have difficulties adapting and implementing their security governance approaches. Sometimes these tensions even reveal that due to the paradoxical situation, the organization will not achieve the desired digital security. We refer to informant quotes with the aim to carefully present our evidence of data-to-theory connections and show how data are aligned with the data structure, as shown in figure 1, 2 and 3. Anonymized interview identifiers are used to code direct quotes (# of interview-interview phase).

4.1 Institutionalization-professionalization tension:

The first tension that is identified in this research is related to a debate in the literature on the relation between institutionalization and professionalization. A long-held assumption in this literature is that there is a symmetric relation between both because of the 'reciprocal dynamics between processes of institutionalization and processes of professionalization' [11, 17]. On these grounds, the two theoretical constructs are generally described as inseparable concepts having a 'symmetric' relationship. In essence, professionals are key drivers of institutional change. However, recent studies have challenged the central institutionalization-professionalization assumption and have shown that it is more likely that the relation is asymmetric [11]. For instance, Risi & Wickert (2017), show that corporate social responsibility (CSR) professionals envision the ideal state in which 'their job is done'[11]. CSR managers strive to make their jobs obsolete so that the CSR function shifts from the organization center towards the periphery. In other words, if CSR is performed by everyone in the organization without strong guidance from CSR professionals, CSR is strongly institutionalized. We use this theoretical background to understand how security can become the institutional-wide effort that a digital context demands.

Asymmetric perspective towards institutionalization and professionalization

Synergy was found between the CSR study and the study presented in this paper on CISOs. The informants (mainly CISOs) also propagate a vision that in a perfect organization, their jobs should become obsolete:

"[...] Actually, what I am doing is making myself obsolete" (20-2), and

"[...] What I hope and expect is that I can make my own job obsolete"(7-2).

By striving to make their jobs obsolete, the security function becomes the responsibility of the firm. Instead of being the responsibility of a central professional position in the organization, security should be everyone's responsibility and part of all employees' DNA. The more employees conduct security functions as part of their natural habits, the more security becomes institutionalized without the need for a central security function.

"[...] In an ideal organization, everyone is a security officer. Then, you don't need a separate security function" (21-2), and

"[...] Security should be in the mores of the company. If you can achieve that, you have already arranged your governance because you really shouldn't have a CISO at all" (20-2).

To further substantiate the full institutionalization of security from an asymmetric perspective, informants believe that security should not be organized separately or treated differently from day-to-day business. The business is ultimately responsible for making decisions regarding risks and taking sufficient security measures [13]. If security is integrated into existing business processes, security becomes more natural and self-evident and eventually suited for institutionalizing throughout the firm's concepts.

To this extent, our findings are consistent with recent studies that argue that the relation between institutionalization and professionalization is asymmetrical [11].

Symmetric perspective towards institutionalization and professionalization

However, the data also is consistent with the assumption that professionals play a key role from the symmetric perspective towards institutional change. Our data reveal doubts about institutionalizing the security function via a security throughout the firm model.

For instance, there is a general understanding among our informants that security is a profession and demands specialized knowledge in complex technical domains. The demand for specialized knowledge in performing security functions builds central professional security functions.

"[...] I soon found out that security is a field where it is useful if you also have professional knowledge, and then we thought that it is actually smart to make a specialist team, a separate unit" (32-3).

Our findings are in line with the literature that states that aspects of security require substantial effort and perseverance for conceptual understanding to be gained [4]. Due to the complexity, the security function is not performed naturally by individuals in the organizational context, so professionals need to do it.

Second, we found that the professional role is related to the extent to which security is institutionalized. Informants show that it is a timely process to achieve intuitional change towards digital security and that in this transformation phase, the demand for professionals as key drivers of institutional change is high. Informants share the belief that the need for a central and professional security function is temporary since security is seen as a new topic where full institutionalization has not yet been accomplished.

"[...] Security is just another business risk... Only I had to help with that because it is a new risk, and the expertise is not there yet. They [business] may be even less aware of it. They may not yet know the threat. So as a CISO, you are making your organization aware. You are educating your organization. You are training them. You are coaching them" (42-3).

CISOs that execute the security function adopt development aid tactics to transfer knowledge with the ultimate goal of teaching the business how to stand on its own two feet. The process of knowledge transformation costs time and requires professionals to guide the transition.

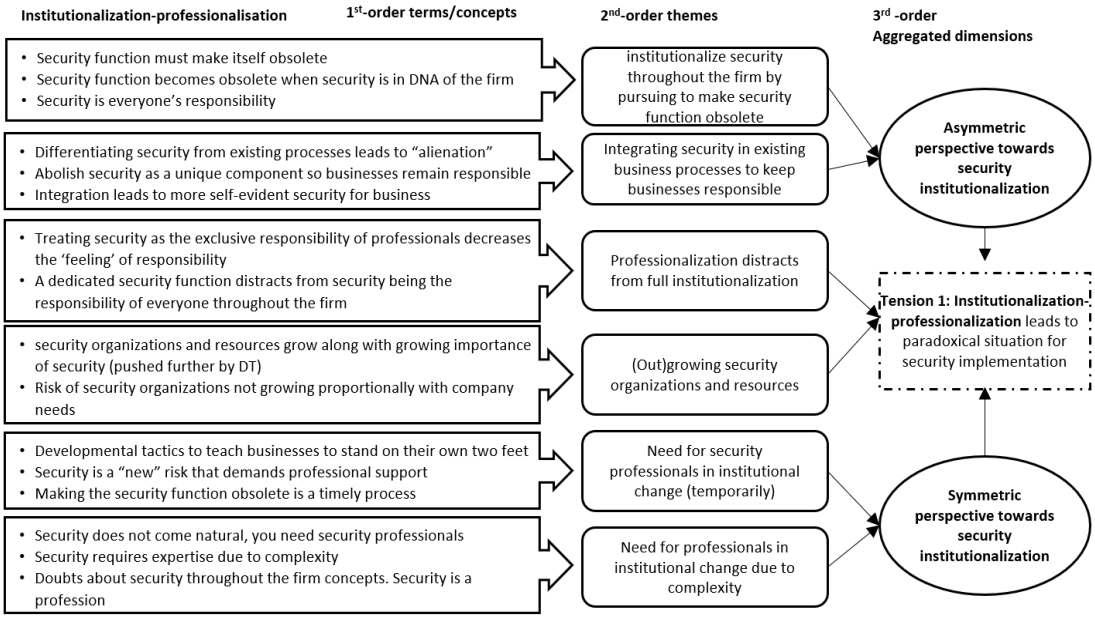

Fig. 1. Data structure presenting the institutionalization -professionalization tension

Digital context pushes towards a paradoxical situation

Narrowing this tension down in the context of this study, e.g., digital transformation, the data show that the institutionalization-professionalization relationship in security governance even becomes paradoxical. First, digitalization increases professional security resources and organizations in a more natural way. The importance of security is felt, and therefore resources are increased. Second, due to digitalization and growing risks, organizations feel the temporary need and pressure of "getting the work done". Informants show that this pressure overwhelms security organizations and in response to grow out of organizational needs.

"[...] "The only thing that is happening now is that we are actually setting up very large security organizations that sometimes no longer fit the organizational needs, and that is double because I also have a lot of work to do" (14-2).

The overfocus on professionals eventually creates the paradoxical effect that pushes away from institutional change. Individuals do not feel the responsibility for security (throughout the firm) because security is seen as exclusive for professionals.

To conclude, our data reveal that in the context of digital transformation, the relationship between institutionalization and professionalization is under pressure and exposes a paradoxical situation. Although CISOs strive to institutionalize security functions via a model where everyone feels the responsibility for security and executes the security function as part of their DNA, they built large professional security organizations to address the challenges and work related security and related risks that digital transformation creates. This leads to the result that employees consider security "not for me" because there are large professional groups that do the work, decreasing the desired full institutionalization throughout the firm demanded in a digital security

approach. This tension hinders the implementation of security governance, also see figure 1 for an overview.

4.2 Ambidexterity: Security vs innovation

The second tension identified in this paper shines light on the tension between innovation and security. Organizations embrace new technology and continually innovate to remain competitive and survive in today's digital context. However, in doing so, organizations rush to modernize their systems and operations and therefore introduce vulnerabilities across their businesses and expose themselves to a growing number of risks. This reveals tensions between innovation and security that hinders security governance implementation.

In framing this tension, we draw from the literature on ambidexterity. This literature is rich in understanding how to tackle complex tensions in performing difficult tasks simultaneously without sacrificing efficiency [10, 15]. In particular, we reflect on the security-innovation tension from the exploration-exploitation perspective.

Security by design

We found that informants mainly address the tensions between security and innovation by positioning security as an enabler of business innovation "by design". From this point of view, security should be considered and embedded in every new initiative, business product or process.

"[...] y*ou cannot lay the foundation for a house afterwards. So, it [security] must have already been included in the first thought formation, in the first architectural sketches. Otherwise, it will not work" (31-3).*

Integrating security in the design process has multiple advantages. First, when security is implemented in the early stages by design, this leads to more efficiency in the innovation process and lowers the effect that security hinders business innovation. Second, investing in security in an early stage leads to cost savings in the long term [2]. It costs less effort to implement security in products or processes in an early stage so that the design does not have to be rebuilt or adapted afterwards. It is the security surprises that cause security to be perceived as delaying, timely and expensive. Third, latency towards implementing security features increases over time to a point where adding security after the fact is impossible. Security latency describes the time that is needed to actually implement security in relation to the total development process. The quote of informant (#1) describes this with great detail:

"[...] making a system secure has a relatively big latency. See, the latency is increasing massively over time. So, it takes you a little bit of effort in the beginning; if you're a year in development, it takes you a bit more time; two years in development, it takes days or even more time. At some point if you have systems over 30 years of development, it becomes impossible to make it secure, so you just need to start again from scratch. That's basically the situation" (1-1).

Organizations should be aware that participating in a digital innovation should not only be seen from an "innovate or die" perspective without understanding that security is a concern. It is extremely difficult to retrofit protections into systems initially built

without them; therefore, security should be integrated primarily in the design stages. The vision on digital innovation will become "securely innovate or die".

One-sided perspective of security versus innovation tensions

Although the benefits of security by design principles are clear, our theoretical lens of ambidexterity provides insight that the security profession heavily relies on a one-sided perspective focused on integration. Accordingly, our informants adhere to the thought that security must come at the expense of agility or speed in the security by design process:

"[...] Maybe you should take a step back in speed every now and then, and you should say dude, let's take a look again without wanting to stop them [business]. But let's see, how can we together maintain that speed, but maybe 80 kilometers per hour instead of 100 kilometers per hour. But in a safe way and not 100 kilometers per hour so that you fly out of bend." (33-3). and

"[...] Every organization must consciously accept security that in order to do things safely, it slows down business, it becomes more complex, that efficiency is lost. You really have to get that through your organization." (37-3)

The above quotes shine light on the fact that the security-innovation tension is so far, both in practice and academia, mainly addressed from a one-sided "quid pro quo" perspective. Security by design, despite its clear benefits, therefore creates difficult barriers to overcome. The security-innovation tension is not understood from the perspective of ambidexterity, where we can learn to run security and innovation simultaneously without affecting efficiency.

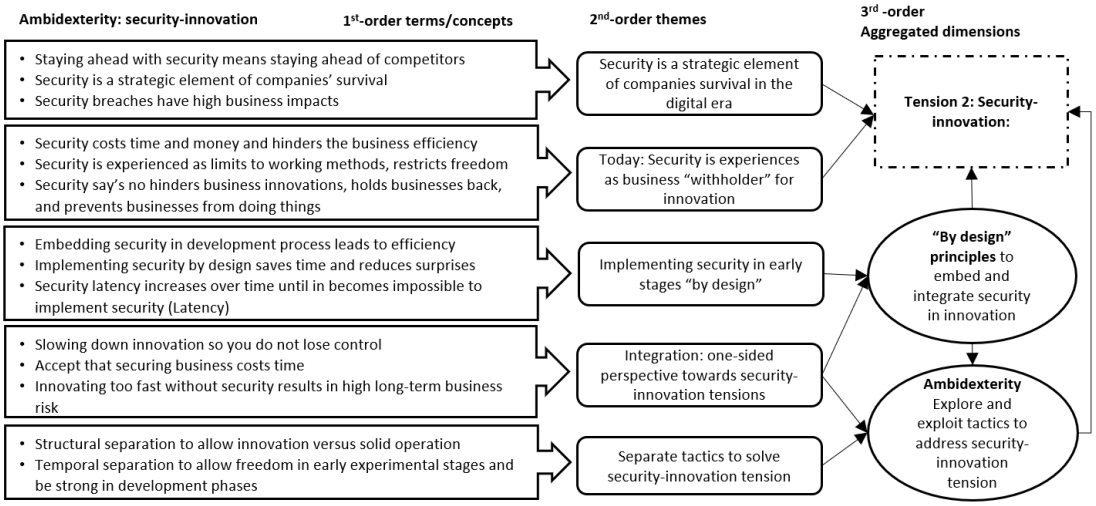

Fig. 2. Data structure presenting Ambidexterity: security-innovation tension

Exploitation-exploration: integration and separation

How to solve the complex trade-offs and tensions in the context of innovation is studied in organizational research. For example, the ambidexterity literature has focused on how firms can differentiate and balance their exploration and exploitation efforts [10,

15]. Ambidexterity focuses on being able to do both with equal effectiveness. A common mainstay within this literature is solving the tension by distinguishing integration and separation strategies [10, 15]. Integration examples include digital activities being integrated into firms' existing structures, thus remaining close to the traditional business. This entails, for instance, security by design as described above. Separation strategies include temporal separation, in which firms alternate between exploration and exploitation activities; and structural separation, in which the two activities are spatially separated by creating distinct organizational units [15]. Solving barriers within the security-innovation tension demands drastic changes to balance integration and separation strategies of organizational structures, instead of relying heavily on one aspect e.g. in our case integration.

In our data, we found supporting evidence of informants who share insights about solving the security-innovation tension from a separation perspective. For instance, informants emphasize the importance of temporal separation in security and innovation. Informants share the insight that innovation mainly exists in very experimental phases where security does not have to be a dominant factor, e.g., risk is low due to lower scale and not experimenting with sensitive data. However, security is too often positioned as a black and white trade-off without thoroughly understanding what and when security is demanded in the innovation process.

"[...] often you only need freedom in the innovation phase. .... What we try is we give them [business] a kind of playground with preconditions. .... You are not allowed to use company data in this environment. As soon as this goes to production, you end up in the standard process because as soon as the developers have to go to production, you notice that that freedom is not that important at all". (37-3)

The quote acknowledges the importance that the experimental phase is temporary but indeed separate from the formal development process.

Second, our informants accentuate the importance of structural separation of the security function.

"[..]when I look at innovation, that also means something for your security organization. If you still have difficulties implementing the basic measures ... and also want to be an innovative organization, that takes a lot of energy from your security team ... About the really new innovation AI, blockchain, that kind of thing, perhaps you should split up to get started with. " (16-2),

and

*"[...] well, my time is mostly spent on yesterday's sh*t: patch nightmares, bullshit bonanza and here [basic security measures] we do it, and there [innovation] I would actually like to set up my whole team" (38-3).*

Both quotes address that without structural separation of the security function, security becomes a trade-off between implementing basic measures vs innovation, where the time spent on innovation decreases.

To conclude on this tension, in today's world, security and innovation are inaccurately seen as mutually exclusive. Security by design principles is implemented to address the tension. Shifting security in the early stages of the development process saves time, money and effort. However, we found that the security by design principle is so far seen from a one-sided integrative perspective. The lens of how ambidextrous firms understand to simultaneously run conflicting tasks (exploration-exploitation),

supported our data in a wider understanding of how to solve security-innovation tensions. To this extent, we discussed the necessity to balance integration-separation tactics, also see figure 2 for an overview.

4.3 Organizing for high reliability: mindfulness-mindlessness

The third tension also exposes a contradictory goal of contemporary firms: they need to handle digital threats at scale and speed while also avoiding errors that result from digital and automated processing [12]. The tension discussed in this paragraph arises at the intersection of this contradiction, namely, to what extent organizations can trust human effort (mindfulness) versus technology and automation (mindlessness) in achieving high reliability and security in these high-risk environments.

High reliability organization (HRO) scholars have largely focused on studying near-error-free organizations in typical complex interactive settings: nuclear power plants, airplane cockpits, air traffic control, aircraft carriers, et cetera [20]. Today's digital organizations increasingly show similarities with traditional HRO characteristics. Digital businesses are highly interconnected and complex and therefore continuously exposed to (high) risk [13]. Scholars increasingly show interest in studying HRO theory in the digital context, so-called digital HROs [12, 13]. A principal challenge that digital HROs face is that highly automated and IT-based operations are antithetical to forms of mindfulness, e.g., heedfully anticipating failure; hence, according to theory, these increase the risk of failure [12]. At this point, digital HROs stand in stark contrast to traditional HROs wherein mindlessness arises mainly from cognitive limitations in human operations [12, 20]. The central issue for digital HROs is how to overcome the mindful-mindless conundrum and still achieve high reliability and security. We use this theoretical lens to analyze our data with regard to the mindfulness-mindlessness tension from the security perspective.

Security perspective: lack of mindful organization

According to HRO theory, the collective mindfulness of individuals accounts for high reliability [12, 20]. However, in digital HROs, the demand for capabilities in achieving high reliability might transcend individual competence, especially in the case of security. For example, first, informants notice that the indirect effect on security risk leads to a lack of security awareness and behavior. People do not understand security risk because the "pain" of security failures is not directly heard, seen or felt.

"[...] Those technological changes, everything that is happening here, it is not tangible. The security impact is not visible. What does that actually do?" (39-3), and

"[...] The core message that I did indeed get from it is: you know that something is wrong, but you don't feel it, you don't see it. So it remains very abstract" (32-3)

Additionally, security risk is experienced as an abstract, intangible, elusive and invisible risk. Due to this abstractness, the experience of security risk is placed outside of the "sphere of influence" of the employees.

Second, organizational boundaries push towards the "security is not for me" effect. Employees have a better understanding of the impact of security breaches in their private environments. When employees act within organizational boundaries, confidence

is felt that the organization and their IT/security departments have created a secure environment for them. To this extent, individuals show less secure behavior.

"[...]that is the same if you have a house and a storm is expected, that you do a check on the windows. In an office building, employees lack to do a check on the windows. You also see the same mentality with IT Security".(36-3), and

"[...] Also human behavior. If you are not the one who has to pay the fine ... if the boss pays the fine, I drive too fast" (29-3), and

"[...]I think that employees are less, well, perhaps less inclined to comply with security measures, because they think: IT-security will take care of that anyway" (28-3)

Third, automation transcends human capabilities. Security attacks are becoming increasingly more sophisticated. New technologies such as artificial intelligence and machine learning also provide attackers with enhanced tools and software for more complex attacks [13]. The number of security attacks is increasing, the attacks are becoming smarter, and qualified security analysts are scarce.

"[...] and I can guarantee you that due to the automation of the bad guys, they know how to find those blind spots flawlessly (33-3), and

"[...]and we think that in our field okay we need humans, but we can't do it with humans because our attackers don't have humans either. Do you understand?" (41-3)

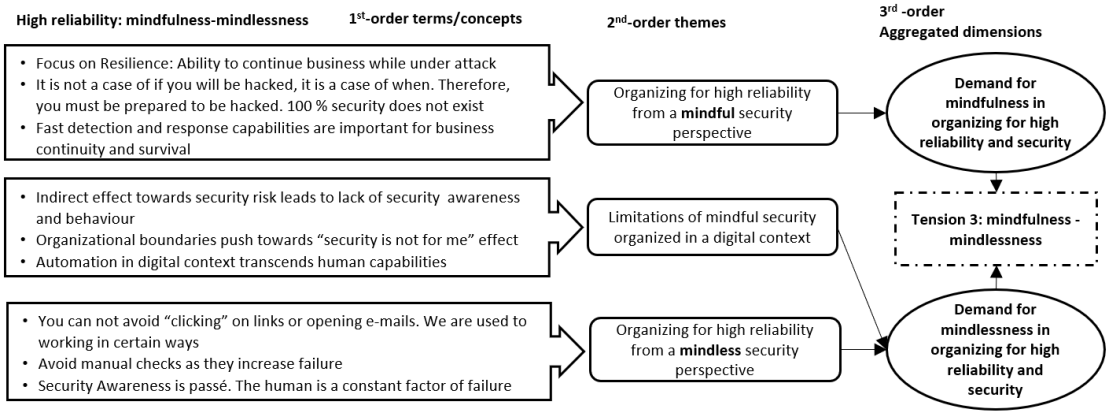

Fig. 3. Data structure presenting mindful-mindlessness tension

Achieving high reliability with mindfulness-mindlessness balance

The above limitations of organizing for high reliability from a mindful perspective show the need for mindless aspects in organizing for security in the digital era. Informants emphasize different elements of mindlessness that rely more heavily on tooling without trusting manual controls of human activities.

To conclude this section, the security profession long held the assumption that humans are the weakest link in security. We argue that security profession and research might have overly focused on solving imperfect human capabilities. In an increasingly automated digital context, mindlessness contributes to high reliability as it compensates for the lack of human capabilities, also see figure 3 for an overview. One of our informants describes this spot-on as follows.

"[...] And often we say that the human is the weakest link, only I think that the human is just the last link. The last measure we have."(14-3)

5 Contributions and research implications

Our work responds to reoccurring calls to provide more in-depth empirical studies on security governance [9, 13]. We offer the following contributions. First, we built a theory of the digital security governance phenomenon, in particular, on "implementation". Discussing the tensions from a theoretical view helps research indicate, label and further understand the relations of what actually hinders organizations when implementing security governance. Second, our work is relevant for practitioners. The findings described in this paper help to become aware of possible tensions in today's security governance designs. Also the paper provides a deeper understanding of how and why security implementation is affected by the tensions. Managing the tensions can lead to more effective and established digital security approaches. Third, we provide freshness by using security as an illustrative case to study the challenges within digital transformation. By doing so, we contribute to a question of how security can be effectively turned from a potential issue of digital transformation into a positive source of impact for an organization, e.g., resilience and business survival [18].

This study has limitations since it strongly focused on identifying tensions and explaining why tensions are present. This study did not yet examine underling relations or barriers. Also our paper provides little insight into how this knowledge can be made operational. Further research can examine the underlying relations of the presented tensions. For example, it is valuable to understand in more depth the tipping point when overfocusing on security professionals distracts form institutionalization, how to organize for and deploy ambidexterity techniques to securely innovate without haggling on efficiency and last, understand what the right balance is between mindful-mindlessness in achieving high reliability and security within the organization.

6 Conclusions

Our study discusses three tensions that hinder organizations in implementing security governance, e.g., institutionalization-professionalization, ambidexterity in security-innovation and mindful-mindlessness in organizing for high reliability. For each tension, we discuss why tensions are present and how they hinder implementation. We provide fresh insight by introducing management theories to further discuss and express why tensions occur. Our key take away is that the context of the digital transformation determines that the tensions are present. Organizations should therefore seriously consider how digitalization impacts their business processes and understand the essence of implementing digital security governance

References

1. AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security*, *99*, 102030.
2. Assal, H., & Chiasson, S. (2018). Security in the software development lifecycle. In Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018) (pp. 281-296).
3. Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. Organizational Research Methods, 16(1), 15–31. https://doi.org/10.1177/1094428112452151
4. Kam, H. J., Menard, P., Ormond, D., & Crossler, R. E. (2020). Cultivating Cybersecurity Learning: An Integration of Self-Determination and Flow. Computers & Security, 101875.
5. Karlsson, F., Karlsson, M. and Åström, J. (2017), "Measuring employees' compliance – the importance of value pluralism", Information and Computer Security, Vol. 25 No. 3, pp. 279-299. https://doi-org.vu-nl.idm.oclc.org/10.1108/ICS-11-2016-0084
6. Lidster, W., & Rahman, S. S. (2018, August). Obstacles to Implementation of Information Security Governance. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 1826-1831). IEEE.
7. Manjezi, Z., & Botha, R. A. (2019, August). From Concept to Practice: Untangling the Direct-Control Cycle. In *Proceedings of the 9th International Conference on Information Communication and Management* (pp. 101-105). https://doi-org.vu-nl.idm.oclc.org/10.1145/3357419.3357427
8. Maynard, S. B., Tan, T., Ahmad, A., & Ruighaver, T. (2018). Towards a Framework for Strategic Security Context in Information Security Governance. Pacific Asia Journal of the Association for Information Systems, Vol. 10, No. 4.
9. Nicho, M. (2018). A process model for implementing information systems security governance. *Information & Computer Security*, Vol. 26, Issue 1, pp. 10-38, https://doi.org/10.1108/ICS-07-2016-0061
10. O'Reilly III, C. A., & Tushman, M. L. (2013). Organizational ambidexterity: Past, present, and future. Academy of management Perspectives, 27(4), 324-338.
11. Risi, D., & Wickert, C. (2017). Reconsidering the 'symmetry' between institutionalization and professionalization: The case of corporate social responsibility managers. *Journal of Management Studies*, *54*(5), 613-646.
12. Salovaara, A., Lyytinen, K., & Penttinen, E. (2019). High reliability in digital organizing: Mindlessness, the frame problem, and digital operations. MIS Quarterly. DOI: 10.25300/MISQ/2019/14577
13. Schinagl, S. and Shahim, A. (2020), "What do we know about information security governance? "From the basement to the boardroom": towards digital security governance", Information and Computer Security, Vol. 28 No. 2, pp. 261-292. https://doi.org/10.1108/ICS-02-2019-0033
14. Slayton R. (2021) Governing Uncertainty or Uncertain Governance? Information Security and the Challenge of Cutting Ties. *Science, Technology, & Human Value* ;46(1):81-111. doi:10.1177/0162243919901159
15. Smith, P., & Beretta, M. (2020). The Gordian Knot of Practicing Digital Transformation: Coping with Emergent Paradoxes in Ambidextrous Organizing Structures. Journal of Product Innovation Management.
16. Spremić, M., & Šimunic, A. (2018). Cyber security challenges in digital economy. In *Proceedings of the World Congress on Engineering* (Vol. 1, pp. 341-346).
17. Suddaby, R., & Viale, T. (2011). Professionals and field-level change: Institutional work and the professional project. Current Sociology, 59(4), 423–442. https://doi.org/10.1177/0011392111402586

18. Vial, G. (2019). Understanding digital transformation: A review and a research agenda. The Journal of Strategic Information Systems, 28(2), 118-144.https://doi.org/10.1016/j.jsis.2019.01.003
19. Von Solms, V., & Von Solms, B. (2006a). Information security governance: A model based on the Direct–Control Cycle'. Computers & Security, Vol. 25, Issue 6, pp. 408-12. https://doi.org/10.1016/j.cose.2006.07.005
20. Weick, K. E., Sutcliffe, K. M., and Obstfeld, D. 1999. "Organizing for High Reliability: Processes of Collective Mindfulness," in Research in Organizational Behavior (Volume 1), R. S. Sutton and B. M. Staw (eds.), Stanford, CT: JAI Press, pp. 81-123
21. Wong, C. K., Maynard, S. B., Ahmad, A., & Naseer, H. (2020). Information Security Governance: A Process Model and Pilot Case Study. *Forty-First International Conference on Information Systems, India*