Dec 12th, 12:00 AM

The Impact of the Organizational Design of Innovation Units on the Consideration of Cybersecurity

Sebastian Heierhoff
Technical University of Darmstadt, heierhoff@is.tu-darmstadt.de

Alina Reher
Capgemini Invent, alina.reher@capgemini.com

Jessica Slamka
University of Applied Sciences München, jessica.slamka@hm.edu

The Impact of the Organizational Design of Innovation Units on the Consideration of Cybersecurity

Completed Research Paper

Sebastian Heierhoff
Technical University of Darmstadt
Hochschulstraße 1, 64289 Darmstadt, Germany
heierhoff@is.tu-darmstadt.de

Alina Reher
Capgemini Invent
Olof-Palme-Straße 14, 81829 Munich, Germany
alina.reher@capgemini.com

Jessica Slamka
Munich University of Applied Sciences
Am Stadtpark 20, 81243 Munich, Germany
jessica.slamka@hm.edu

Abstract

Digital innovations are not only associated with opportunities for value creation but also lead to threats, for example, additional cybersecurity risks. Dealing with the conflicting requirements of innovations and cybersecurity can lead to a trade-off for organizations that companies setting up innovation units outside their core organization need to address. We conducted a cross-industry interview study to investigate the impact of organizational design of innovation units on the consideration of cybersecurity. Our results, embedded in Galbraith's star model, reveal five types of innovation units and three patterns of organizational design that impact this consideration. The effect of these patterns ranges from an ill- or over-consideration to a cybersecurity-innovation equilibrium. Thereby, we extend the existing literature on the trade-off of innovation and cybersecurity by organizational design considerations regarding strategy, structure, and processes. This theoretical contribution has implications for the organizational design of innovation units in practice.

Keywords: Digital innovation; cybersecurity; organizational design; grounded theory

Introduction

For companies, digital transformation leads to increasing pressure to innovate, e.g., due to changing customer needs and the resulting demand for new digital products, services, and business models (Baregheh et al. 2009). However, new technologies do not only bring opportunities but also risks and challenges for companies. It is no surprise that cyber incidents were identified as the top global business risk for 2022 in a study of 2,650 risk management experts from 89 countries, outpacing even the Covid-19 pandemic (Allianz Global Corporate & Specialty 2022). Consequently, there is a growing need to consider cybersecurity in digital innovations and minimize risks (Payette et al. 2015). Nevertheless, cybersecurity is often given little priority in innovation practice, especially in the design and conception phases (Waidner et al. 2013). Cybersecurity is associated with delays in time to market and is considered resource-intensive and time-consuming (Chinn et al. 2014; Pearlson and Huang 2017). At the same time, there is a perceived lack of positive impact on the company's revenue, as customers are assumed to consider the value-add of other

product features to be higher (Pearlson and Huang 2017). Therefore, companies might weigh cybersecurity investments against business value (Bailetti and Craigen 2020).

In general, the importance of cybersecurity for digital innovations is well researched, for example, with respect to the effect on customers' willingness to buy (Sapin et al. 2017). From a cybersecurity perspective, tensions, e.g., regarding data privacy or usability, are well-known (Olt and Wagner 2020). Proactive management can mitigate cybersecurity risks (Gordon et al. 2015; Hutchinson et al. 2011; Payette et al. 2015), however, this is often associated with a reduction of innovativeness. Consequently, a cybersecurity-innovation trade-off arises, with organizations struggling to balance the two priorities (Nelson and Madnick 2017) and integrate cybersecurity into innovation (Schinagl et al. 2021).

From an organizational perspective, innovation units have emerged as focused, separate, dedicated, and autonomous entities for the development of digital innovations, which are to be fully integrated into the operating organization at a later stage (Holotiuk 2020). Such forms of organizational ambidexterity (Raisch et al. 2009, Gibson and Birkinshaw 2004) have been found to effectively address general tensions between exploration and exploitation (Svahn et al. 2017), with innovation units enhancing innovation capability, time-to-market, and first-mover advantage (Barthel et al. 2020; Ringel et al. 2015; Sapin et al. 2017). While the need to cohesively embed cybersecurity in day-to-day business activities has been recognized in previous studies (Poehlmann et al. 2021), it remains unclear how this should be specifically reflected in the organizational design of innovation units in terms of integration or separation (Kosutic and Pigni 2022; Schinagl et al. 2021). To address this research gap, this paper attempts to answer the following question:

How does the organizational design of innovation units impact the consideration of cybersecurity?

Thereby, the objective of our study is to discuss implications for organizations resulting from this impact on the consideration of cybersecurity and to demonstrate how the cybersecurity-innovation trade-off can be addressed in the particular organizational setting of innovation units.

Key insights will be elaborated based on an interview study. We draw on ten expert interviews with stakeholders from both an innovation management and cybersecurity perspective, representing 138 years of experience with leading corporations from various industries. Our data analysis is based on the grounded theory methodology (Charmaz 2006; Corbin and Strauss 1990), enabling us to contribute to theory development while building on existing organizational design models like the star model (Galbraith 1977).

The remainder of this paper is structured as follows. In the next chapter, we define relevant key terms and provide the theoretical background. We do then present the methodology and study design before reporting on the results of our study. Finally, our findings are discussed, including implications for theory and practice and limitations before a conclusion wraps up the paper.

Theoretical Background

The use of digital technologies and the resulting **digital innovations** are radically changing the nature of products, services, and organizations (Rachinger et al. 2019; Yoo et al. 2012). Digital innovation refers to the change of existing and the design of new products, processes, and organizational structures through the implementation of digital technologies (Condea et al. 2017; Damanpour 1996; Gassmann and Enkel 2004; Nambisan et al. 2017). A characteristic feature of digital innovations is the incorporation of technologies into objects that were previously purely material (Yoo et al. 2012). The value of digital innovations thus stems from "combinations of digital and physical components" (Yoo et al. 2010, p. 3), leading to new ways of shaping customer experiences, processes, and organizational forms. Consequently, incorporating digital technologies into innovations can help meet new requirements from the customer's perspective and promote internal efficiency gains from the company's perspective (Holotiuk 2020; Yoo et al. 2012).

Currently, companies in almost all industries are undergoing an ongoing and fundamental reorganization process due to the impact of digital innovations (Verhoef et al. 2021). As a result of the disruptive nature of digital technologies, existing organizational designs are no longer sufficient (Yoo et al. 2012), and companies are forced to change (Sänn et al. 2017). To be successful, companies must create an environment in which the potential of digital technologies can be exploited, digital innovations can be explored, and new or transformed business models can be created (Aagaard 2019; Verhoef et al. 2021; Yoo et al. 2012).

Organizations are trying to increase their innovation capability by setting up **innovation units** in which specific digital competencies are bundled. This allows them to implement digital projects and respond to the rapidly changing environment and the challenges resulting from digitalization (Holotiuk 2020; Magadley and Birdi 2009; Nowshad; Raabe et al. 2021). Enabled by their organizational design, innovation units aim to reduce complexity, enable knowledge sharing, identify ideas, and capitalize on opportunities (Guidat et al. 2014). Their purpose is to develop digital ideas and explore new ways of working in a protected space outside the core organization, detached from inhibiting processes and structures (Bärtle 2017). Thereby, innovation units are "separate in many ways from the operational parts of the organization, e.g., in terms of location, mindset, collaboration, and communication" (Holotiuk 2020, p. 1).

There are various ways to set up and anchor innovation units in organizations. Whereas in research the term 'innovation unit' is mostly used in a generic way, different terms such as digital business units, innovation labs, company builders, accelerators, and incubators are used to delineate innovation units in practice. Innovation units do not only have the goal of developing digital innovations for the customer business. These units also often represent institutionalized innovation management to accelerate the digital transformation of the organization and achieve cultural change (Di Fiore and Rosani 2018; Koen et al. 2011). In this case, they are often referred to as transformation offices (Bärtle 2017). Furthermore, the organization of innovation activities also includes corporate venturing. Unlike corporate venturing, however, innovation development in innovation units is not limited to the creation of new business models (Holotiuk 2020; Villalonga 2004).

While companies are setting up innovation units to foster digital innovation, they are also facing a growing need for **cybersecurity** consideration. Cybersecurity deals with all aspects of information and communications technology security in cyberspace. This includes all information technologies and physical systems connected to the Internet, including the applications and processes based on them. Cybersecurity can thus be distinguished from physical security, for example, hardware, and encompasses a company's business interests beyond information protection (Kosutic and Pigni 2022; Solms and van Niekerk 2013). From a company perspective, the importance of cybersecurity for digital products and services is undisputed (Pearlson and Huang 2017). Executives see cyberattacks as one of the biggest global threats to their companies. This is also reflected in growth in cybersecurity investments and budgets (Kosutic and Pigni 2022). Nevertheless, cybersecurity incidents show that the integration of cybersecurity into products and services continues to fail (Pearlson and Huang 2017). Although awareness is increasing, cybersecurity often remains purely an IT problem from the perspective of many organizations (Kosutic and Pigni 2022).

Consequently, the consideration of cybersecurity is among the difficulties companies face during the development of digital innovations (Svahn et al. 2017; Yoo et al. 2012). The reasons for the **trade-off between innovation and cybersecurity** lie in their opposing characteristics. While innovation requires creativity and freedom, cybersecurity is rather driven by compliance with regulations, policies and standards like the General Data Protection Regulation (GDPR). These conflicting objectives often carry over to the management level as well, due to the performance requirements and mindsets that underlie both disciplines. Cybersecurity is, therefore, rarely among the requirements of the early phases of digital innovations. Instead, designers focus on marketability, usability, and functionality. However, any Internet-connected product can provide an entry point for attacks that access the internal system, inject malware, or collect sensitive data (Pearlson and Huang 2017). Therefore, cybersecurity may be integrated into the design phase and the development process to avoid vulnerabilities and ensure the cybersecurity of products and services. This may make development more complex, time-consuming, and costly, but it can reduce costs and better meet customer expectations in the long run (Pearlson and Huang 2017). Nevertheless, this stands in the way of the required speed and agility of innovation (Pearlson and Huang 2017).

The conflicting priorities within organizations exacerbate the need to find a solution to the trade-off between cybersecurity and innovation. The challenge of finding a balance between innovation management and risk management, which may include cybersecurity, is not new. Previous studies on the trade-off between innovation and cybersecurity, in specific, have outlined the impact of cybersecurity on business value (Bailetti and Craigen 2020; Cresswell and Hassan 2007), tensions that hinder implementation from a digital security governance perspective (Schinagl et al. 2021), the general consideration of cybersecurity in innovative projects (Nelson and Madnick 2017), or implications for specific industries (Heierhoff and Hoffmann 2022; Heierhoff and Reher 2022). From an innovation perspective, management faces the challenge of changing the mindset of innovation teams to include cybersecurity in innovation from the

outset. To do this, managers must recognize the relevance, establish clear communication (Poehlmann et al. 2021), and make cybersecurity an important factor in product development (Waidner et al. 2013). In the context of innovations units, a suitable organizational design of these innovation units could support this process and achieve a more targeted incorporation of cybersecurity into digital innovations (Payette et al. 2015; Waidner et al. 2013), with design options ranging from integration in terms of 'security by design' to separation including temporal or structural separation of security and innovation (Kosutic and Pigni 2022; Schinagl et al. 2021) known from organizational ambidexterity theory (O'Reilly and Tushman 2004).

Organizational design is concerned with achieving coherence between an organization's strategy, organizing mode, and the integration of individuals (Galbraith 1977). In order to study the impact of innovation units' organizational design on cybersecurity consideration, we chose Galbraith's star model (Galbraith et al. 2002) as a frame of reference. The model allows for an understanding of different design parameters in alignment with an innovation unit's objective to enhance innovation capability. Our focus of analysis is set on the level of the organizing mode, which includes the design dimensions structure and processes in alignment with strategy in the star model (Galbraith et al. 2002, see Figure 1). We thereby exclude the dimensions people practices and reward systems which would warrant an analysis on the level of individual employee behavior involving downstream design choices regarding incentives and employee development. The design dimensions in focus of our study are elaborated in the following, including their relevance in the set-up of innovation units.

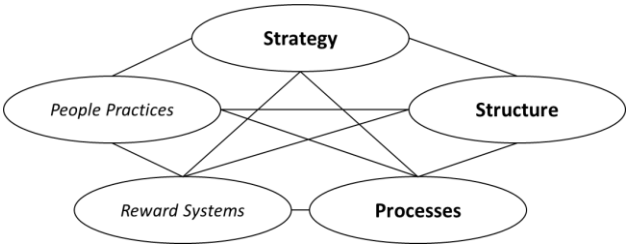

Figure 1. Galbraith's Star Model (adapted from Galbraith et al. 2002)

Strategy comprises the *vision* and *goals* of an organization and provides direction for the alignment of organizational design parameters. A company's strategy must influence the motivation and vision of setting up an innovation unit. A shared vision between the innovation unit and the company is crucial to managing the trade-off between exploitative and exploratory innovation (O'Reilly and Tushman 2008).

Structure defines the location of formal power and authority, which can be displayed in organizational charts. In innovating organizations, structural design parameters include *roles* such as orchestrators, sponsors, and idea generators, *differentiation* through separating innovation physically, financially, or organizationally from activities of the operating organization, as well as *reservations* in the form of innovation units (Galbraith 1982). Companies need to shape the structure and direction of an innovation department through organizational design, as interdependencies between the innovation units and the line organization are elementary. Measures must be taken to mitigate conflicts through the structural or temporal separation of exploration and exploitation. Reporting lines provide a level of control and support for the coordination of tasks or projects (Gibson and Birkinshaw 2004).

Processes comprise integration mechanisms to enable a connection of separate organizational units. Collaboration can be enhanced through *defined processes* as well as through *lateral connections* in the form of interpersonal networks, teams, and integrative roles. Depending on the extent of separation of an innovation unit from the operating organization, companies must decide how to bridge the gap through defined processes or lateral connections (Eirich 2020).

Methodology

Since the topic area is largely unexplored, we chose a qualitative, exploratory research approach as the **study design** (Bogner et al. 2009; Recker 2013). The need to balance exploration and exploitation provides the basis for the research context. In contrast to startups, the challenges of digital and organizational transformation are primarily found in the organizational structures of established companies. Our research

focuses exclusively on companies that have established innovation units and face the challenge of addressing cybersecurity in these units. Using the grounded theory methodology (Charmaz 2006; Corbin and Strauss 1990), we derive explanatory theory and discuss implications for companies in an iterative process.

We conducted expert interviews using a semi-structured interview guideline for **data collection**. The interview approach was chosen because of the possibility of gaining detailed insights from conversations and the flexibility in communication. The interview guideline included the following aspects. The introductory part was dedicated to the introduction of the interviewee in terms of academic background, current business unit, and position within the organization, as well as previous positions relevant to our research (Bogner et al. 2009). The main part included questions about the organizational design of the respective organization's innovation unit, including the consideration of cybersecurity in strategy, structural, and process elements. Interviewees were asked whether there was a perceived trade-off. The interviews were concluded with a request for additional comments on the topic.

ID	Industry/ Affiliation	Number of Employees	Revenue in Bn EUR	Role/ Position/ Level/ Unit	Focus	Experience	Date and Duration
1	Consultancy, Focus Energy	10.000	16	Manager Growth Strategy	Innovation	6 years	23 Sept. 21 0:39:35h
2	Retail	99.000	28	Sr. Digital Strategist, Lead Innovation Manager	Innovation	14 years	13 Oct. 21 0:39:25h
3	Energy & Engineering	25.000	9	User Experience Researcher	Innovation & Cybersecurity	12 years	14 Oct. 21 0:48:19h
4	Information Technology (IT)	98.000	23	Head of Process Management	Process Innovation	27 years	15 Oct. 21 0:54:08h
5	Energy & Engineering	92.000	27	Head of Digitalization, Strategy & Architecture	Innovation & Cybersecurity	14 years	22 Oct. 21 0:48:25h
6	Consultancy	312.000	35	Innovation Manager	Innovation	9 years	25 Oct. 21 0:44:25h
7	Consultancy, Focus Automotive	624.000	44	Cybersecurity Consultant	Cybersecurity	3 years	25 Oct. 21 1:06:16h
8	Insurance	150.000	140	Information Security Officer	Cybersecurity	6 years	26 Oct. 21 0:47:44h
9	Engineering & IT	395.000	78	Global IoT Innovation Lead	Innovation	32 years	01 Nov. 21 0:46:48h
10	Retail	174.000	16	Director Internat. IT Customer Interaction	Cybersecurity	15 years	09 Nov. 21 0:32:39h

Table 1. Overview of Interview Partners

The data collection was conducted in cooperation with a large consulting firm specializing in digital transformation with departments for both innovation and cybersecurity. Since cybersecurity is a sensitive topic that requires trust, the authors' network within this consultancy provided valuable support in acquiring interview partners from client companies. Concerning the latter, the focus was on experts working in different types of innovation units, or in the areas of cybersecurity, information, and IT security with direct contact with those units. Furthermore, care was taken to ensure that interviewees came from organizations in different industries, departments, and organizational levels, diverse positions, roles, and responsibilities, as well as different focus areas and perspectives. However, to avoid general statements, the interviewees were asked to limit their answers to one specific innovation unit and, if possible, to report on the unit in which they are currently working. To complement the view of experts reporting on innovation units from an internal perspective, three consultants were included in the sample of experts. They provide an external perspective through their involvement in client organizations' innovation development. The interview partners were acquired by e-mail, in which the objective of the study was specified. The list of interviewees can be found in Table 1.

The complete interview guideline was not sent to the participants in advance to encourage spontaneous and honest responses (Bogner et al. 2009). The interviews were conducted in German, as this is the native language of all participants. In this way, clear communication is ensured, and language barriers are eliminated (Marschan-Piekkari and Reis 2004). Depending on the information provided in the responses, the interviews lasted between 32 and 66 minutes without the informal opening and closing. All interviews took place between September 23 and November 9, 2021. Due to COVID-19, all interviews were conducted via Microsoft Teams and were recorded with the interviewee's consent.

For **data analysis**, interviews were transcribed and analyzed in a structured manner based on the recorded audio files using the software MAXQDA. Due to data privacy and the confidentiality of information about an organization's cybersecurity, the transcripts were anonymized. This was communicated to all interview participants to gain trust, encourage honest responses, and ensure the validity of the results.

A-priori concept	Refined concept	Illustrative quote
Strategy	Strategic focus	[...] you have to think of it as this unit being responsible for trying things out, testing things out, building prototypes. (I10)
	Risk propensity	Time-to-market is very relevant, and if we always looked at it that well from the beginning, we wouldn't have as many cybersecurity attacks as we currently have. [...] Time-to-market and the functionality of a product are placed far above cybersecurity [...]. As a result, unfortunately, action is often taken reactively rather than proactively. (I7)
Structure	Structural differentiation	I think there is still a need to improve integration, but there is a natural distance between the topics of innovation and security [...] because one side fears that too many rules will be imposed on them, and the other side says that they are doing all this wild stuff. (I9)
	Role of top management	The units that are successful with innovations in our company have been given a great deal of freedom by management. (I2)
Processes	Guidelines and requirements	[Cybersecurity] has not yet come up [as a requirement] at all, at least in the area where I work. [...] It was occasionally mentioned in meetings as a side sentence. [...] (I3)
	Approval and decision-making	It is tried to identify critical elements already during the development of the proof of concept, i.e., to directly involve [...] the colleagues from cybersecurity [...]. It also doesn't help when you have made a super successful POC to find out afterward that it can't be transferred to cybersecurity architecture. (I9)
	Interfaces and collaboration	I don't know at what point [...] the question of these security aspects is being dealt with seriously. We are just about to present the first approach to the developers for the initial MVPs, and then the first things will be implemented. As far as I know, no discussion has taken place yet, even though this has already been handed over to the developers. (I3)

Table 2. Code System (Excerpt)

The **analysis procedure** of the study followed the grounded theory methodology according to Corbin and Strauss (1990) and Charmaz (2006), as summarized by Berente et al. (2019). Data collection, analysis, and theory development were conducted in parallel, in an iterative, incremental process. Thus, the analysis of the initial interviews influenced how subsequent interviews were conducted (Berente et al. 2019). Data analysis involved open, axial, and selective coding (Berente et al. 2019; Corbin and Strauss 1990). This process is, again, iterative so that identified categories are sharpened in multiple passes. Data collection ceased at a point where further interviews did not exceed the range of answers and hence did not lead to the discovery of additional properties regarding the developed categories in terms of innovation units' organizational design, cybersecurity consideration as well as a perceived trade-off (Charmaz 2006). The authors are aware that coding is influenced by the theoretical research context since codes that emerge during data analysis reflect existing knowledge and vocabulary established in the research field. This "pre-

theoretical lexicon", which is inevitably drawn upon in the research context, also influenced the construction of the interview guideline and the conduct of the interviews by inculcating scientific knowledge (Berente et al. 2019; Charmaz 2006). Thus, research and evaluation cannot occur separately within the grounded theory, and theory development cannot occur without incorporating knowledge, as grounded theory originally strives to do (Berente et al. 2019).

As part of the open coding process, we started with the coding of the a-priori defined concepts: characteristics of innovation units, elements of organizational design (strategy, structure, processes), and cybersecurity consideration. These concepts were only used as a first basis in an aim to use grounded theory to achieve a more fine-grained analysis, to further differentiate the concepts and to detect logical relationships. Interview statements were first labeled with generic terms to provide an overview of the aspects mentioned in the interviews, thereby leaving room for emerging concepts. Next, the individual text passages of the transcripts were reviewed, and specific statements were given labels that described the phenomenon in practice as accurately as possible. In the next step, concepts were refined during axial coding using the constant comparison technique (Charmaz 2006; Corbin and Strauss 1990). This led to a refinement of concepts (e.g., 'processes' was refined to include 'guidelines and 'requirements' and 'approval and decision-making processes'). Finally, the relationships between the core concepts were explored during selective coding. Thereby, the properties of different types of innovation units were identified, and patterns in their configuration of organizational design elements and resulting cybersecurity consideration were detected. This final step of theory building led to the identification of five types of innovation units and three distinct patterns of cybersecurity consideration in organizational design (Markus and Robey 1988). The types and patterns detected form the basis for the presentation of results in the following chapter. Table 2 shows an excerpt from the coding system, including core concepts and illustrative quotes.

Results

The analysis of the interviews reveals **five types of innovation units** that differ in their objectives (see Table 3, rows 1 and 2). The objective of "*Type 1: Internal innovation labs*" is to drive internal innovations such as process optimizations and the introduction of digital tools. Consequently, the primary goals of innovation units of this type are increasing efficiency and reducing costs (I1, I3, I4). As the name suggests, "*Type 2: External innovation labs*" describes innovation labs with the objective of developing customer products and services. This type of innovation unit is created to reduce time-to-market (I7), build prototypes, carry out smaller market tests (I10), and in the long run, promote a culture of innovation within the company (I6). The goal of "*Type 3: Digital transformation offices*" is to manage the innovation project portfolio holistically and measure success by their company-wide benefit. This is realized by bundling activities from business and IT (I5). Central to "*Type 4: Innovation ecosystems*" is the linking and networking of the companies involved with each other and with startups (I9). Future viability is ensured by building valuable partnerships (I2, I9), developing new capabilities, and deploying new technologies (I9). The objective of "*Type 5: Spin-offs*" is growth through balancing exploration and exploitation within the subsidiary (I2, I8). This is enabled by the size and agility of the newly founded company, for example, offering benefits concerning incorporating customer feedback (I8).

Three patterns (see Table 3, rows 3*ff.*) emerge regarding the impact of organizational design on the consideration of cybersecurity in these types of innovation units.

Pattern A: Innovation Focus

Due to their **strategy,** the *strategic focus* of innovation units in Pattern A is on efficiency (Type 1) and speed of innovation development (Type 2). Consequently, these innovation units seek not to be limited by cybersecurity. It is assumed that there "won't be as big an issue with cybersecurity as in the line [organization], and I'll be faster." (I7). This is especially the case during research and idea generation but often also affects the implementation of innovations (I3).

Especially for external innovations, the *risk propensity* is perceived to be higher in Pattern A (I3, I7). Therefore, and due to little fear of being attacked, companies often act reactively when it comes to cybersecurity (I4). If cybersecurity is addressed, this is often driven by technological trends, like cloud technologies, which employees assume to have a cybersecurity impact (I3). Instead, our experts call for the topic to be mandatory (I3), like data privacy, due to the legally binding EU GDPR.

"There, the motivation comes by itself, as no one wants to bear the financial consequences." (I7)

Type of Innovation Unit		**Type 1: Internal Innovation Lab**	**Type 2: External Innovation Lab**	**Type 3: Transformation Office**	**Type 4: Innovation Ecosystem**	**Type 5: Spin-Off**
Objective		Internal processes/ tools development	External products & services development	Holistic digitalization management	Joint capability development	Business model exploration & exploitation
Pattern		**A: Innovation Focus**		**B: Cybersecurity Focus**	**C: Symbiosis**	
Organizational Design	**Strategy**					
	Strategic focus	Increasing efficiency, reducing costs, creating structured approaches for processing ideas		Manage the digitalization portfolio holistically	Linking/ unification with partners, customers, and of exploration & exploitation	
	Risk propensity / management	High risk-taking; low maturity		Low risk-taking; high maturity	Depending on business value of innovation	
	Structure					
	Structural differentiation	Separate units; disconnected		Central cybersecurity experts in innovation unit; formal connection not practiced/ lack of network	Dedicated SPOCs or cybersecurity champions embedded in innovation projects	
	Role of management	Cybersecurity not anchored in top management; low awareness		Awareness is present/ need is recognized; implementation not yet achieved	Cybersecurity anchored in top management; balanced with freedom and trust for innovation	
	Processes & Lateral Capability					
	Guidelines and requirements	Low formalization (or guidelines not applied)		High formalization (strict guidelines; established)	Situative approach depending on task/ phase in innovation process; guardrails & SPOCs facilitate compliance	
	Approval and decision-making	Only followed if stakeholders aware of added value		Centralized governance, lack of transparency	Established, guided by guardrails & SPOCs	
	Interfaces and collaboration	Missing; conflicts		Established but non-transparent	Situative adaptation of collaboration	
Consideration		Cybersecurity ill-consideration		Cybersecurity over-consideration	Cybersecurity-innovation equilibrium	

Table 3: Mapping of Types and Patterns

Concerning **structure**, there is a *structural differentiation* of innovation units and cybersecurity in Pattern A. One expert even reports that innovation development is completely disconnected from cybersecurity teams (I4). Consequently, employees from innovation and other business units find it difficult to name a common outcome of innovation projects (I1). This often results in resistance from the business units, which, in turn, are often (considered) responsible for the implementation of cybersecurity (I3, I4).

> "Part of the assumption [...] is that if a well-defined project [is handed over to] the developers, the issue of cybersecurity will somehow solve itself [...]." (I3)

If cybersecurity experts are involved in innovation units, *top management* commitment and trust that experts are making the right assessments are required (I6). In Pattern A companies, however, cybersecurity is not yet anchored in the top management, e.g., in the form of a chief information security officer, and the necessary awareness is not yet created (I7). Often, management focuses too much on financial metrics (I4, I6). As many investments in cybersecurity are not immediately noticeable, there is a lack of understanding of why these should be made (I1).

> "It didn't work because the business owners all said 'No, I won't let you talk me into it. This is my business. I'm responsible for it. [...] I decide that because that's my money in the end, and I'm measured for what profitability [...] I generate. '" (I4)

Concerning **processes**, cybersecurity is often not included in the *guidelines and requirements* and thus not perceived as a priority. Instead, innovative functionalities are prioritized (I1, I3, I4, I7), and cybersecurity is not being considered at all (I3, I4) or too late (I3, I7). It is assumed that cybersecurity can be implemented retrospectively (I3), while this involves a great deal of effort and would be avoidable (I7).

> "If you only look at it subsequently, then you have to fill in the gaps." (I7)

In theory, *approval and decision-making* are meant to overcome the structural separation by, for example, defining which departments or employees to involve. (I3, I4, I7). However, these processes are only followed if all stakeholders are aware of the added value (I4). In practice, process steps are often "thrown over the fence" when participating teams hold up the development of innovation (I4). Consequently, cybersecurity might not be involved due to fear of objections.

> "You don't want to bring in the objectors right away because that also kills innovations." (I4)

Concerning *interfaces and collaboration*, agile methodologies are deemed more likely to lead to problems in the collaboration with cybersecurity (I4). This underlines the fact that interfaces are currently often designed sequentially, and awareness of the added value of agile cybersecurity approaches is lacking.

In summary, innovation units, according to Pattern A, perceive a strong **trade-off** between innovation and cybersecurity (I1, I3, I4, I6, I7), which is solved by a **cybersecurity ill-consideration.**

Pattern B: Cybersecurity Focus

From a **strategy** perspective, the s*trategic focus* of innovation units in Pattern B is on the holistic management of the innovation portfolio. The *risk propensity* in Pattern B is lower than in Pattern A. Although risks are recognized, there is no feeling of vulnerability because of digital innovations. Due to their structured, formalized approach, companies even perceive a risk reduction (I5).

Concerning **structure** and *structural differentiation*, the digital transformation office in pattern B takes a centralized approach to cybersecurity consideration.

> "The Digital Transformation Office consists of representatives from cybersecurity, from the business units, and IT. The advantage is that thereby we have created a formal structure that leaves no room for discussion, ensuring that cybersecurity is considered because it is centralized." (I5)

Despite this formalism, cybersecurity consideration does, to a certain degree, still depend on the network of the innovation unit's employees and is not embedded into each innovation project (I5)

> "When a connection already exists, on a personal or work-related level [...], the alignment with cybersecurity and architecture is more intense. This is still a topic that is strongly driven by personal networks." (I5)

There is a strong awareness of the importance of cybersecurity and the *role of management* in anchoring the topic (I5). Management knows that cybersecurity must be embedded into the corporate culture, but there is a need to optimize implementation that still depends on informal networks (I5).

With respect to **processes,** innovation units, according to Pattern B, can be characterized by very strict cybersecurity *guidelines and requirements* that are applied without exception.

> "We have a defined process [...]. Each project needs to undergo an approval process and a review where the architectural fit is checked. And the same [applies to] cybersecurity. Cybersecurity is always a 'no-go' criterion, which is not always easy when you are trying to push an innovation." (I5)

The resulting bureaucracy in innovation development hinders the innovation unit from becoming a protective space where things can be tried out and is perceived as an obstacle that can jeopardize or slow down innovations (I5). The high degree of formalism can result in cybersecurity assessments being carried out too early. In this case, cybersecurity experts are involved when there is only a rough idea of what a solution might look like, which still has to mature and can change significantly (I5).

In terms of *approval and decision-making*, Pattern B is characterized by established decision-making processes regarding cybersecurity. However, it lacks sufficient transparency for employees executing the processes (I5). While processes are intended to standardize decision-making, this can also be counterproductive when formalism leads to delays (I5).

From an *interfaces and collaboration* perspective, this formalism can also lead to interpersonal tensions between innovators and those responsible for cybersecurity, causing conflicts and delays.

> "Cybersecurity is not 'fuzzy'. In most areas, it is clear what is allowed and what is not. The more emotional such topics get, the more I stick to my position. As an innovator, I claim 'you are stopping my innovation', while security insists 'but I am the one accountable for security.'" (I5)

Pattern B shows a strict, formal separation but standardized yet often non-transparent and inefficient bridging mechanisms.

> "Due to the IT governance and the lack of a network, many employees do not even know which steps to follow and whom to contact" (I5).

While from an innovation perspective, transparency must be increased so that employees become aware of cybersecurity contacts and requirements (I5), a trade-off arises from a cybersecurity perspective. On the one hand, it is valuable if innovation units approach those responsible for cybersecurity at an early stage. On the other hand, the overall process is more efficient if aspects can be bundled in the cybersecurity department, e.g., by using standardized tools for managing risks (I5).

The perceived **trade-off** between innovation and cybersecurity in Pattern B is not as strong as in Pattern A. It is addressed by an **over-consideration of cybersecurity**.

Pattern C: Symbiosis

In line with their **strategy**, the focus of Pattern C innovation units is on balancing formal requirements often imposed by more mature companies and the innovation focus usually driven by startups (Type 4). This attempt to balance exploration and exploitation can also be observed in spin-offs (Type 5).

Thus, the *risk propensity* in Pattern C is fine-grained. Innovation units do not have to adhere to all aspects of the core organization's rules (I2, I8), for example, due to their small customer base. Depending on the type of innovation and if the innovation uses the same IT infrastructure as the rest of the organization, cybersecurity measures can often not be fine-tuned and apply anyhow (I8, I9). In this case, Pattern C companies often rely on innovative approaches to ensure cybersecurity risk mitigation, like bug bounty programs (I2, I8).

With respect to their **structure** and *structural differentiation*, Pattern C companies employ dedicated cybersecurity SPOCs or cybersecurity champions (I8), in some cases from a staff unit of cybersecurity experts within the innovation unit. These are trained with respect to what cybersecurity aspects need to be considered and regularly scrutinize developments in this regard (I8).

Cybersecurity is organizationally anchored within the *role of management* (I8). This is underlined by the Chief Information Security Officer (CISO) receiving adequate board attention and cybersecurity initiatives receiving support (I8). At the same time, innovation units also experience freedom and trust.

> "One of the models for success [...] [is] to get the freedom and the trust and not to jump in too early, even if things don't go so well. That you can stand it, the tension." (I2)

Management in Pattern C actively tries to reduce tensions and differences between employees with different mindsets or perspectives, e.g., innovation and cybersecurity officers, to develop successful innovations (I9).

> "This requires an iterative process where both parties gradually approach each other. Ultimately, there can be added value [for both sides]. However, this doesn't work without moderation, [...] you need to actively listen and see 'what do we both need at least in order to progress?'" (I9)

Concerning **processes**, Pattern C innovation units are less concerned with defining *guidelines and requirements* than with minimizing risks (I8).

> "I think we're doing quite well in that we're really trying to keep the security function small and only have to tackle the areas where it really adds value, not just introduce a process that keeps the security function busy." (I8)

Instead of detailed requirements, guardrails and a two-step innovation process ensure future viability (I9). During the proof of concept (POC) phase, little or almost no cybersecurity requirements apply as no production IT or data is used (I9). Only when commercializing the innovation does adherence to cybersecurity policies becomes mandatory (I9).

> "When we are in a POC environment, you have flexibility, speed, but maybe not real-time and real-life data, but just sample data sets. That is sufficient to validate the POC. The moment you go into a product phase, the complete security aspects take effect." (I9)

Depending on the type of innovation, e.g., if customer data is involved, no distinctions are made, and the same strict rules as for other business units apply (I2, I9).

> "If a lot of customer data is used, we are very careful and look at it extremely closely. If customer data is involved or reputational risks are involved, then innovation is slowed down and there are very close eyes on it." (I2)

Concerning *approval- and decision-making*, Pattern C companies try to create transparency with respect to when cybersecurity experts need to be involved (I8). The aforementioned cybersecurity SPOCs act as sparring partners to simplify decision-making processes and ensure that innovations can unfold yet are not developed without cybersecurity consideration (I8). Innovation units, according to Pattern C, seek to include cybersecurity early, but not as early as possible (I8, I9).

> "That means probably not immediately when the first conversation [...] about the new feature takes place, [...] but as soon as a little bit of the requirements is solidified." (I8)

Pattern C underlines the belief that *interfaces and collaboration* need to ensure that priorities are not defined exclusively from one point of view (I8). Depending on these priorities, e.g., concerning cybersecurity, the collaboration is adapted (I8). As innovation units usually work according to agile methodologies, the cybersecurity team needs to adapt to these methodologies (I2). Through agility, efficiency, and pragmatism, cybersecurity and compliance can then be ensured (I8, I9)

Unlike companies in Patterns A and B, companies in Pattern C perceive a **trade-off** only to a limited extent (I8, I9) or recognize how the integration of innovation and cybersecurity can create added value (I9). This is explained by organizational design allowing to achieve a **cybersecurity-innovation equilibrium**.

> "I don't think that one impedes the other or one undermines the other. It mustn't be like that. It is all about finding the right dosage throughout the process." (I9)

Discussion

Evaluation of results

Our results confirm the existence of a **trade-off between innovation and cybersecurity** in line with the literature. The underlying tensions are, for example, explained by a conflict between speed or time-to-market and the time required to ensure the cybersecurity of innovations. Because of this trade-off, it is not self-evident that cybersecurity is adequately considered in innovation units. Our experts do, however, agree that companies need to make efforts to minimize the trade-off and find a balance (e.g., Cresswell and Hassan 2007; Nelson and Madnick 2017; Schinagl et al. 2021).

Regarding *strategy*, our results highlight differences in strategic focus, risk propensity, and management of innovation units that lead to different considerations of cybersecurity. With respect to their strategic focus, different types of innovation units have different objectives and thus handle cybersecurity differently. This is in line with literature on innovation units in general (Holotiuk 2020). While the risk for cybersecurity vulnerabilities and incidents cannot be reduced to zero, despite all efforts, including organizational design (Cresswell and Hassan 2007), organizations must realize that digital innovations come with considerable risks and be willing to accept the negative impact on business performance (Bailetti and Craigen 2020). Companies need to determine their willingness to take risks for innovation, recognize cybersecurity as part of risk management and therefore give it appropriate consideration (Borgelt and Falk 2007; Hutchinson et al. 2011; Shropshire et al. 2018; Vargas-Hernández et al. 2010)

Concerning *structure*, this realization could then be reflected in changes to the organizational design. Our results emphasize the impact of structural differentiation and the importance of the role of management and its influence on the consideration of cybersecurity in innovation units. If companies opt for a structural differentiation between innovation units and cybersecurity experts, they need to implement mechanisms to flexibly overcome this separation for cybersecurity-critical innovations. Alternatively, depending on the type of innovation pursued, cybersecurity experts can be incorporated into the innovation units as SPOCs or in the form of cybersecurity champions, thereby bridging the structural differentiation. Within this respect, dedicated roles have shown to be more effective than formalized processes. These bridging mechanisms are in line with more general organizational ambidexterity studies (Gibson and Birkinshaw 2004; Heierhoff and Reher 2022; Raisch et al. 2009). Furthermore, our results, e.g., in line with Johnson and Goetz (2007), show that cybersecurity needs to be anchored in the top management of innovation units to ensure consideration. Management must simultaneously promote an innovation mindset and point out the risks posed by a lack of cybersecurity in digital innovations. In line with Svahn et al. (2017), this can lead to interpersonal tensions between employees that management needs to address.

Finally, regarding *processes*, our results highlight characteristics of guidelines and requirements, approval and decision-making, and interfaces and collaboration, leading to differences in consideration. While there is a need for cybersecurity guidelines and requirements within innovation units, our results call for pragmatism and efficiency through low complexity and formalization and a focus on agile cooperation between innovation and cybersecurity. Our results are in line with the literature in that companies need to distinguish different phases of the innovation process and different types of innovations (Bowers and Khorakian 2014; Shropshire et al. 2018), e.g., depending on the data used, and adapt their guidelines accordingly. Formal stage-gate processes and feedback loops (Du Preez and Louw 2008) might, however, thus not be the right approach. Instead, adequate approval and decision-making need to ensure that the right experts are involved at the right point in time. Concerning these interfaces and collaboration, our results highlight the importance of cybersecurity SPOCs as well as a personal network of innovation unit employees with these experts. Furthermore, the importance of flexible and agile methods for the collaboration of cybersecurity and innovation units is underlined, which represents an area of research by itself (Bishop and Rowland 2019; Hutchinson et al. 2011).

According to our results, adapting the **organizational design of innovation units** could be one approach to addressing the cybersecurity-innovation trade-off. This is expressed in the three patterns we identified during data analysis. Within the star model by Galbraith, they show the impact of organizational design, i.e., its dimensions strategy, structure, and processes, on the consideration of cybersecurity in innovation units and thereby provide an answer to our research question. While many of our findings per se are backed by former, less-specialized studies not only within organizational design research (e.g., Du Preez and Louw 2008; Johnson and Goetz 2007), the value of our study lies in their combination through the identification of patterns within the specific context of innovation units and cybersecurity consideration. These patterns show that specific organizational designs are more or less effective in solving conflicting demands when pursuing innovations with certain cybersecurity requirements.

Contributions

From a **theoretical perspective**, this study provides the following contributions. Based on our theoretical background, a research gap regarding the impact of organizational design on the consideration of cybersecurity in innovation units has been identified. In this context, our study shows that there is no uniform definition of innovation units and that the boundaries of innovation units are still insufficiently

understood in research and practice. More importantly, our patterns are, to our knowledge, the first theory explaining the impact of organizational design of innovation units on the consideration of cybersecurity. According to our results, there is a match between the type of innovation unit, its organizational design characteristics, and cybersecurity consideration. By adapting the organizational design towards an alignment of the dimensions, organizations should thus be able to address the cybersecurity-innovation trade-off. By embedding these findings in Galbraith's star model, we highlight potential connections and parallels to existing research on organizational design. Thereby, this paper goes beyond the connections between innovation units and organizational design that have been discussed in the literature so far (Barthel et al. 2020; Holotiuk 2020; Raabe et al. 2021) and represents a substantial addition to organizational ambidexterity theory and structural as well as contextual ambidexterity, in particular (O'Reilly and Tushman 2004). This study does thereby largely contribute to closing the identified research gap while laying the foundation for future research.

Despite a relatively low number of interviews, we are convinced that the **mapping between types of innovation units and organizational design patterns** (cf. Table 3) is meaningful. The patterns show an alignment of organizational design dimensions based on an innovation unit's overall objective and the resulting strategic focus. Innovation labs (Type 1 and 2) are explicitly tasked to innovate quickly and focus on increasing efficiency through internal or value-adding functionalities of external innovations. It does therefore make sense for them not to allow themselves to be slowed down by cybersecurity consideration. Transformation offices (Type 3) are rather found in large corporations trying to bundle their digitalization efforts. Being founded with this traditional, rather bureaucratic background results in a strong focus on guidelines and policies. Innovation ecosystems and spin-offs (Type 4 and 5), finally, can be characterized as relatively mature approaches to innovations, typically also driven by large corporations or subsidiaries of these being handed-over full responsibility for successfully implementing innovative business models while at the same time maintaining bonds with their parent companies. Consequently, these final two types were found to show the most adaptable behavior concerning the consideration of cybersecurity reflected in or enabled by their organizational design. This ultimately leads to value-added for organizations once the balance can be achieved.

Instead of finding an adequate mapping between innovation to pursue, type of innovation unit, and organizational design patterns for the consideration of cybersecurity, companies might ask themselves whether structurally separate organizational units are the right way to achieve **organizational ambidexterity** when cybersecurity needs to be considered. Organizational ambidexterity literature does, in this regard, list various alternatives, like structural (O'Reilly and Tushman 2004), temporal (Wang et al. 2019) or contextual ambidexterity (Gibson and Birkinshaw 2004). The latter is based on a behavioral perspective and focuses on simultaneous alignment and adaptability within a business unit. In our context, cybersecurity requirements could, for example, be adapted to the particular innovation and point in time in the innovation process with simple systems and less formality (Gibson and Birkinshaw 2004). Our results do, thereby, already contain some indications for the advantages of such an organizational design, for example, with respect to adaptable guidelines and requirements or the role of cybersecurity SPOCs in helping to determine how to fulfill which requirements. In the end, when digital innovations are "the new normal", as product lifecycles are becoming shorter due to the faster development of digital technologies, innovation development will be at the core of each organization.

Besides its theoretical value, this paper provides contributions from a **practical perspective**. Our results corroborate literature findings that the consideration of cybersecurity in innovation units is not yet a matter of course. Our patterns can promote awareness and can be used as a framework for reviewing, planning, and outlining the organizational design of such units accordingly. For example, organizations could design self-assessments based on our dimensions and derive measures to adapt their organizational design accordingly. Thereby the consideration of cybersecurity in innovation units could be improved. Consequently, companies need to become aware of what type of innovations they want to pursue and which level of cybersecurity these innovations require. They should then choose the type of innovation unit and the organizational design of that unit accordingly to enable an adequate consideration of cybersecurity and reduce the cybersecurity-innovation trade-off in this particular organizational setting. Thereby, not only the type of innovation unit employed but also the consideration of cybersecurity within this unit might be associated with a maturation process. For example, relatively immature companies might start with anchoring digital innovations within the company itself or launching small speedboats before learning to "do things right". The fact that the consideration of cybersecurity is adapted to the requirements of the

innovation and that only a few companies succeed in striking a balance between innovation and cybersecurity is in line with findings, e.g., of Nelson and Madnick (2017).

Limitations

There are several limitations to this study. From a **methodological perspective**, this work can only be seen as an initial explorative study due to the relatively small number of expert interviews, and the generalizability does thus remain questionable. While we are convinced of the suitability of a grounded theory approach for this type of study, a multiple case design with more information sources per company would have allowed for more in-depth insights. Additionally, challenges have emerged in the data collection and analysis of the expert interviews. Cybersecurity is a sensitive topic that might have led to relevant experts refusing to participate and could have influenced our experts' answers. The resulting group of interviewees, their roles, and their experiences might have influenced our results. Furthermore, our scientific background and the defined a priori concepts represent a limitation. "In choosing a particular lexicon, scientists adopt the path-dependent foundation that limits the degrees of freedom for their theoretical contribution" (Berente et al. 2019, p. 52). In addition, conducting the interviews in German facilitated communication but might have led to translation discrepancies. Although partially countered by choosing semi-structured interviews enabling open communication, the data collection and analysis are thus subject to interpretation, which we tried to counteract by performing member checking. These methodological limitations have consequences from a **content perspective**. Due to our research approach and the choice of our interview partners, we are, for example, unable to compare different units within a company or the perceptions of different roles. Even if individual statements suggest that the consideration of cybersecurity in innovation units is lower than in the core organization, we are, for example, unable to verify this claim. Furthermore, it was found that senior positions, while having a deep and comprehensive understanding from a management perspective, are sometimes unable to make detailed statements regarding the operational implementation. As we use Galbraith's star model as a frame of reference but limit our analysis to the dimensions pertaining to the level of the organizing mode, we are unable to make statements about the level of human resources in terms of individual employee behavior. However, in sidenotes, our interviewees did, for example, say that companies must continue to develop skills both internally and externally. Besides these limitations, our results do, from our point of view, contribute to closing the research gap and provide valuable indications on how organizational design influences the consideration of cybersecurity in innovation units.

Future research

From these limitations, opportunities for **future research** can be derived. First, the identified types and patterns should be validated based on case studies or with a larger sample of interview partners. Further types and patterns might thereby be added. In this context, it would also be interesting to investigate whether all dimensions impact the consideration of cybersecurity equally and how dimensions influence each other. As a result, further aspects, like industry, company characteristics (e.g., company culture), or innovation unit characteristics (e.g., number of employees and unit maturity), could be included. In this regard, the two left-out organizational design dimensions of Galbraith's star model are interesting for future studies to understand how incentives and employee development measures can be implemented in alignment with the respective organizing mode in order to achieve an adequate cybersecurity consideration. Other interesting aspects from the authors' point of view are the organizational anchoring of the innovation unit within the company and the effect of culture. In this regard, it could be interesting to get two informants from the same organization to compare the cybersecurity and digital innovation experts' view, as well as to compare the consideration of cybersecurity within an innovation unit to that of other business units. Furthermore, looking at the different phases of the innovation process and task characteristics to develop the situative approach hinted at in Pattern C represents a promising research direction. In addition, it might be worth researching whether consideration at the project level, actual implementation, and the occurrence of cybersecurity incidents are correlated in a longitudinal study. Finally, future research could analyze different approaches to achieving organizational ambidexterity and their ability to drive innovations while at the same time considering cybersecurity. This could result in concrete levers for companies to improve the consideration of cybersecurity in digital innovation units and beyond.

Conclusion

Our study investigates to what extent the organizational design of innovation units impacts the consideration of cybersecurity. To our knowledge, the patterns resulting from our expert interviews analyzed using the grounded theory methodology represent the first theory explaining this impact. Thereby, our study provides valuable contributions to both theory and practice. With the growing importance of cybersecurity for digital innovations, the trade-off between the two is likely to increase in importance for innovation units. Adequately reducing this trade-off and fine-tuning the consideration of cybersecurity through organizational design will thus likely remain an interesting topic for the foreseeable future.

References

Aagaard, A. (ed.). 2019. *Digital Business Models*: *Driving Transformation and Innovation*, Cham: Palgarve Macmillan.

Allianz Global Corporate & Specialty. 2022. "Allianz Risk Barometer 2022," available at https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2022.pdf, accessed on May 3 2022.

Bailetti, T., and Craigen, D. 2020. "Examining the Relationship Between Cybersecurity and Scaling Value for New Companies," *Technology Innovation Management Review* (10:2), pp. 62-70.

Baregheh, A., Rowley, J., and Sambrook, S. 2009. "Towards a Multidisciplinary Definition of Innovation," *Management Decision* (47:8), pp. 1323-1339.

Barthel, P., Fuchs, C., Birner, B., and Hess, T. 2020. "Embedding Digital Innovations in Organizations: A Typology for Digital Innovation Units," in *15. Internationale Tagung Wirtschaftsinformatik*, pp. 780-795.

Bärtle, D. 2017. "The Digital Unit as a Game Changer," available at https://www.etventure.com/blog/the-digital-unit-as-a-game-changer/, accessed on May 3 2022.

Berente, N., Seidel, S., and Safadi, H. 2019. "Research Commentary—Data-Driven Computationally Intensive Theory Development," *Information Systems Research* (30:1), pp. 50-64.

Bishop, D., and Rowland, P. 2019. "Agile and secure software development: An unfinished story," *Issues In Information Systems* (20:1), pp. 144-156.

Bogner, A., Littig, B., and Menz, W. (eds.). 2009. *Interviewing Experts*, Basingstoke, London: Palgrave Macmillan.

Borgelt, K., and Falk, I. 2007. "The Leadership/Management Conundrum: Innovation or Risk Management?" *Leadership & Organization Development Journal* (28:2), pp. 122-136.

Bowers, J., and Khorakian, A. 2014. "Integrating Risk Management in Innovation Project," *European Journal of Innovation Management* (17:1), pp. 25-40.

Charmaz, K. 2006. *Constructing grounded theory*: *A Practical Guide through Qualitative Analysis*, London: SAGE Publications Ltd.

Chinn, D., Kaplan, J. M., and Poppensieker, T. 2014. "Transforming Cybersecurity: New Approaches for an Evolving Threat Landscape," available at https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/dttl-fsi-TransformingCybersecurity-2014-02.pdf.

Condea, C., Cruickshank, D., and Hagedorn, P. 2017. "What Co-Innovation Can Mean for Digital Business Transformation: Sharing and Managing Risk to Achieve IT Business Innovation," in *Shaping the Digital Enterprise*: *Trends and Use Cases in Digital Innovation and Transformation*, G. Oswald and M. Kleinemeier (eds.), Cham: Springer, pp. 287-307.

Corbin, J. M., and Strauss, A. 1990. "Grounded theory research: Procedures, canons, and evaluative criteria," *Qualitative Sociology* (13:1), pp. 3-21.

Cresswell, A., and Hassan, S. 2007. "Organizational Impacts of Cyber Security Provisions: A Sociotechnical Framework," in *40th Hawaii International Conference on System Sciences*, pp. 98-107.

Damanpour, F. 1996. "Organizational Complexity and Innovation: Developing and Testing Multiple Contingency Models," *Management Science* (42:5), pp. 693-716.

Di Fiore, A., and Rosani, G. 2018. "Two Questions to Ask Before You Set Up an Innovation Unit," available at https://hbr.org/2018/07/two-questions-to-ask-before-you-set-up-an-innovation-unit, accessed on May 3 2022.

Du Preez, N. D., and Louw, L. 2008. "A framework for managing the innovation process," in *Portland International Conference on Management of Engineering & Technology*, pp. 546-558.

Eirich, R. 2020. *Organization design and its impact on the digital innovation process and the digital innovation outcome*, Springer Gabler, Wiesbaden.

Galbraith, J. R. 1977. *Organization design*, Reading, Mass.: Addison-Wesley.

Galbraith, J. R. 1982. "Designing the innovating organization," *Organizational Dynamics* (10:3), pp. 5-25.

Galbraith, J. R., Downey, D., and Kates, A. 2002. *Designing dynamic organizations: A hands-on guide for leaders at all levels*, Amacom Books.

Gassmann, O., and Enkel, E. 2004. "Towards a Theory of Open Innovation: Three Core Process Archetypes," in *R&D Management Conference*.

Gibson, C. B., and Birkinshaw, J. 2004. "The Antecedents, Consequences, and the Mediating Role of Organizational Ambidexterity," *Academy of Management Journal* (2004:47), pp. 209-226.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Zhou, L. 2015. "The impact of information sharing on cybersecurity underinvestment: A real options perspective," *Journal of Accounting and Public Policy* (34:5), pp. 509-519.

Guidat, T., Barquet, A. P., Widera, H., Rozenfeld, H., and Seliger, G. 2014. "Guidelines for the Definition of Innovative Industrial Product-service Systems (PSS) Business Models for Remanufacturing," *Procedia CIRP* (16), pp. 193-198.

Heierhoff, S., and Hoffmann, N. 2022. "Cyber Security vs. Digital Innovation: A Trade-off for Logistics Companies?" in *55th Hawaii International Conference on System Sciences*.

Heierhoff, S., and Reher, A. 2022. "Balancing Digital Innovation and Cybersecurity Capabilities through Organizational Ambidexterity – An Investigation in the Automotive Industry," in *55th Hawaii International Conference on System Sciences*.

Holotiuk, F. 2020. "The Organizational Design of Digital Innovation Labs: Enabling Ambidexterity to Develop Digital Innovation," in *15. Internationale Tagung Wirtschaftsinformatik*, pp. 1019-1034.

Hutchinson, D., Maddern, H., and Wells, J. 2011. "An Agile IT Security Model for Project Risk Assessment," in *9th Australian Information Security Management Conference*, pp. 111-123.

Johnson, M. E., and Goetz, E. 2007. "Embedding Information Security into the Organization," *IEEE Security & Privacy Magazine* (5:3), pp. 16-24.

Koen, P. A., Bertels, H. M. J., and Elsum, I. R. 2011. "The Three Faces of Business Model Innovation: Challenges for Established Firms," *Research-Technology Management* (54:3), pp. 52-59.

Kosutic, D., and Pigni, F. 2022. "Cybersecurity: investing for competitive outcomes," *Journal of Business Strategy* (43:1), pp. 28-36.

Magadley, W., and Birdi, K. 2009. "Innovation Labs: An Examination into the Use of Physical Spaces to Enhance Organizational Creativity," *Creativity and Innovation Management* (18:4), pp. 315-325.

Markus, M. L., and Robey, D. 1988. "Information Technology and Organizational Change: Causal Structure in Theory and Research," *Management Science* (34:5), pp. 583-598.

Nambisan, S., Lyytinen, K., Majchrzak, A., and Song, M. 2017. "Digital Innovation Management: Reinventing Innovation Management Research in a Digital World," *MIS Quarterly* (41:1), pp. 223-238.

Nelson, N., and Madnick, S. 2017. "Studying the Tensions between Digital Innovation and Cybersecurity," *3rd International Conference on Information Systems Security and Privacy*, pp. 1-12.

Nowshad, A. "Aufbau Digital Unit," available at https://www2.deloitte.com/at/de/seiten/human-capital/artikel/aufbau-digital-unit.html, accessed on May 3 2022.

O'Reilly, C. A., and Tushman, M. L. 2004. "The Ambidextrous Organization," *Havard Business Review* (82:4), pp. 74-83.

O'Reilly, C. A., and Tushman, M. L. 2008. "Ambidexterity as a dynamic capability: Resolving the innovator's dilemma," *Research in Organizational Behavior* (28), pp. 185-206.

Olt, C., and Wagner, A. 2020. "Having Two Conflicting Goals in Mind: The Tension Between IS Security and Privacy when Avoiding Threats," in *53rd Hawaii International Conference on System Sciences*, pp. 4213-4222.

Payette, J., Anegbe, E., Caceres, E., and Muegge, S. 2015. "Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects," *Technology Innovation Management Review* (5:6), pp. 26-34.

Pearlson, K., and Huang, K. 2017. "Design for Cybersecurity From the Start," available at https://sloanreview.mit.edu/article/design-for-cybersecurity-from-the-start/, accessed on May 3 2022.

Poehlmann, N., Caramancion, K. M., Tatar, I., Li, Y., Barati, M., and Merz, T. 2021. "The Organizational Cybersecurity Success Factors: An Exhaustive Literature Review," in *Advances in Security, Networks, and Internet of Things*, Springer, Cham, pp. 377-395 (doi: 10.1007/978-3-030-71017-0_27).

Raabe, J.-P., Drews, P., Horlach, B., and Schirmer, I. 2021. "Towards an Intra- and Interorganizational Perspective: Objectives and Areas of Activity of Digital Innovation Units," in *54th Hawaii International Conference on System Sciences*, pp. 5902-5911.

Rachinger, M., Rauter, R., Müller, C., Vorraber, W., and Schirgi, E. 2019. "Digitalization and its Influence on Business Model Innovation," *Journal of Manufacturing Technology Management* (30:8), pp. 1143-1160.

Raisch, S., Birkinshaw, J., Probst, G., and Tushman, M. L. 2009. "Organizational Ambidexterity: Balancing Exploitation and Exploration for Sustained Performance," *Organization Science* (20:4), pp. 685-695.

Recker, J. 2013. *Scientific research in information systems*: *A beginner's guide*, Heidelberg: Springer.

Ringel, M., Taylor, A., and Zablit, H. 2015. "The Rising Need for Innovation Speed," available at https://www.bcg.com/publications/2015/growth-lean-manufacturing-rising-need-for-innovation-speed.aspx, accessed on May 3 2022.

Sänn, A., Richter, S., and Fraunholz, C. K. 2017. "Car-to-X als Basis organisationaler Transformation und neuer Mobilitätsleistungen," *Wirtschaftsinformatik & Management* (9:5), pp. 60-71.

Sapin, D., Cline, J., Aqua, J., and Lieberman, M. 2017. "How Consumers See Cybersecurity and Privacy Risks: Consumer Intelligence Series: Protect.me," available at https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/protect-me/cis-protect-me-findings.pdf, accessed on May 3 2022.

Schinagl, S., Khapova, S., and Shahim, A. 2021. "Tensions that Hinder the Implementation of Digital Security Governance," in *ICT Systems Security and Privacy Protection*: *Jøsang, A., Futcher, L., Hagen, J.*, Cham: Springer International Publishing, pp. 430-445.

Shropshire, J., Presley, S., and Landry, J. 2018. "Cybersecurity Threats in the Context of Project Meta-Phases," in *24th Americas Conference on Information Systems*, pp. 1-10.

Solms, R. von, and van Niekerk, J. 2013. "From Information Security to Cyber Security," *Computers & Security* (38), pp. 97-102.

Svahn, F., Mathiassen, L., and Lindgren, R. 2017. "Embracing Digital Innovation in Incumbent Firms: How Volvo Cars Managed Competing Concerns," *MIS Quarterly* (41:1).

Vargas-Hernández, J. G., Reza Noruzi, M., and Sariolghalam, N. 2010. "Risk or Innovation: Which One Is Far more Preferable in Innovation Projects?" *International Journal of Marketing Studies* (2:1), pp. 233-244.

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Qi Dong, J., Fabian, N., and Haenlein, M. 2021. "Digital transformation: A multidisciplinary reflection and research agenda," *Journal of Business Research* (122), pp. 889-901.

Villalonga, B. 2004. "Diversification Discount or Premium? New Evidence from the Business Information Tracking Series," *The Journal of Finance* (LIX:2), pp. 479-506.

Waidner, M., Backes, M., and Müller-Quade, J. 2013. "Entwicklung sicherer Software durch Security by Design: Trend- und Strategiebericht," *SIT Technical Reports,* Fraunhofer Institut für Sichere Informationstechnologie (ed.), Stuttgart.

Wang, S. L., Luo, Y., Maksimov, V., Sun, J., and Celly, N. 2019. "Achieving Temporal Ambidexterity in New Ventures," *Journal of Management Studies* (56:4), pp. 788-822 (doi: 10.1111/joms.12431).

Yoo, Y., Boland, R. J., Lyytinen, K., and Majchrzak, A. 2012. "Organizing for Innovation in the Digitized World," *Organization Science* (23:5), pp. 1398-1408.

Yoo, Y., Henfridsson, O., and Lyytinen, K. 2010. "Research Commentary —The New Organizing Logic of Digital Innovation: An Agenda for Information Systems Research," *Information Systems Research* (21:4), pp. 724-735.