Balancing Digital Innovation and Cybersecurity Capabilities through Organizational Ambidexterity – An Investigation in the Automotive Industry

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

Alina Reher
Capgemini Invent
alina.reher@capgemini.com

Abstract

An organization's digital innovation capability, i.e., its ability to leverage (technological) trends and developments, is not only associated with opportunities but also entails challenges and risks. Various incidents underline the importance of cybersecurity in this context. While organizations in the automotive industry have recognized both as inevitable, they perceive a trade-off between their innovation and cybersecurity capabilities. As digital innovations are often prestigious, they might prioritize factors like time-to-market and postpone cybersecurity to development and operations. To identify factors enabling organizations to balance the ambidextrous requirements of the two, we conducted an interview study in the automotive industry. Our findings indicate that organizational ambidexterity enabled by strategic and operational elements can minimize the trade-off and the associated risks, with implications for both theory and practice.

1. Introduction

Digital transformation and innovation capabilities of organizations have become imperative and have led to a paradigm shift, not just in the automotive industry [1]. The growing reliance on technology creates opportunities like connected cars but is also associated with new cybersecurity risks [2], as shown by recent incidents. For example, in 2021, security researchers managed to take over a Tesla via its infotainment system [3]. Due to increasing customer awareness, which affects the willingness to buy innovative products [4], cybersecurity needs to be considered in strategic decisions like business-model innovations [5].

In this context, organizations do not want to limit freedom and creativity too early [6]. At the same time, it is expensive to integrate cybersecurity too late, e.g., as technology decisions might have to be revoked [7]. While, for example, cybersecurity is often integrated into development and operations [8], it could make sense to consider the topic in the innovation or ideation phase. Consequently, innovativeness and cybersecurity are often regarded as ambidextrous. Organizations perceive a trade-off and struggle to find the right balance when integrating the two dimensions [9–11]. Organizational ambidexterity, enabling organizations to exploit established while exploring new opportunities [12], could represent a vital solution approach [13]. However, while the terms have been put into context, studies usually focus on balancing exploitation and exploration of cybersecurity mechanisms [14, 15]. The effect of ambidexterity on the ability to balance digital innovation and cybersecurity capabilities is scarcely researched [10].

To examine these ambidextrous tensions between digital innovation and cybersecurity, the automotive industry is particularly suitable as this industry is characterized by a high level of dynamic and instability due to digital transformation. There is a large share of more traditional, rather formal multinationals coining competition [16]. As suggested [12], we did therefore decide to conduct an interview study in this specific industry and answer the research question:

"What is the role of organizational ambidexterity in balancing digital innovation and cybersecurity capabilities in the German automotive industry?"

2. Theoretical Background

We understand innovation and cybersecurity as capabilities, i.e., the ability of "an organization, person or system" that "typically require[s] a combination of organization, people, processes and technology to achieve" [17]. Innovation capability, also called innovativeness or innovativity, refers to the ability to create and leverage (digital) innovations [18]. Driven by trends like car sharing, the automotive industry is under growing pressure to innovate in shortening innovation cycles [19]. Cybersecurity capability goes beyond the protection of information resources and includes the management and mitigation of the effect of cyberattacks on assets and human beings [20]. Examples, like the hack of a Jeep Cherokee [21], underline the relevance from an automotive perspective.

URI: https://hdl.handle.net/10125/80115
978-0-9981331-5-7

Their ambidextrous characteristics and objectives can explain the need to balance digital innovation and cybersecurity capabilities [10]. The former deals with the freedom and creativity required for the agile adaptation of technological trends and their rapid market introduction to secure first-mover advantages [22]. As "organizations rush to modernize their systems and operations […] [they] introduce vulnerabilities across their businesses and expose themselves to a growing number of risks" [10]. The latter, however, is associated with risk prevention and management. Consequently, it is often not seen as added value but as the avoidance of possible losses [23]. Cybersecurity is considered complex, thus time-consuming as well as costly, and often heavily driven by policies and standards [24]. While expenditures for retrofitting cybersecurity could be prevented by early consideration [25], complex cybersecurity requirements might be perceived as obstacles if trying to gain a competitive advantage through the speed of innovation [26]. A trade-off can manifest itself in different, often mutually intensifying dimensions like department structures or performance requirements [11]. Thus, organizations need to find a balance between an innovation focus that might lead to cybersecurity gaps and a prioritization of cybersecurity that could decelerate the innovation process [2]. It is, however, not widely researched how to balance and integrate digital innovation and cybersecurity capabilities. Existing approaches focus on agile software development methodologies [e.g., 27] often used in innovation projects. They frequently ignore the organizational perspective and postpone cybersecurity to implementation, leading to increased costs and delays [28]. Others focus on a specific, innovative technology, e.g., the use of Big Data in IoT [e.g., 29].

Due to the ambidextrous characteristics and objectives, we believe **organizational ambidexterity** might represent a framework enabling organizations to successfully deal with the conflict of digital innovation and cybersecurity. The concept describes the ability to simultaneously exploit current competencies and explore new opportunities [30]. While the former focuses on efficiency and refinement, flexibility and risk-taking are crucial for the latter [31]. Ambidextrous companies can handle the conflicting goals and thereby secure their competitiveness [12]. Contrary to the previous belief that the two stages of the innovation process, initiation and implementation, require separate organizational structures as 'characteristics that facilitate the initiation of innovations impedes the implementation of innovations and vice-versa' [32], recent research shows that this is not necessarily the case [33–36]. Various forms of organizational ambidexterity might positively impact corporate performance, e.g., structural ambidexterity, having separate units focused on alignment and adaptability [32], or contextual ambidexterity, taking a behavioral perspective and providing processes to differentiate within the same business unit [12]. These different forms can be categorized according to four tensions: differentiation vs. integration, individual vs. organizational level, static vs. dynamic perspective, and internal vs. external perspective [30].

Schinagl et al. identify a tension between **innovation and cybersecurity** and use organizational ambidexterity theory as a frame. They observe that this tension is "mainly addressed from a one-sided 'quid pro quo' perspective" [10]. Instead of balancing integration and separation between the two capabilities, concepts like security by design do thus lead to conflicts [10]. Besides, the term ambidextrous cybersecurity has been used to describe the capability to protect information resources while leveraging technological innovations expressed in a stage-gate model [14]. Furthermore, the need for organizations to take a dual approach to cybersecurity response, i.e., to explore new while exploiting old mechanisms, has been examined, mapping 87 organizations to a 2x2 matrix [15]. Detached from organizational ambidexterity, a cybersecurity matrix has been proposed to rank companies' ability to deal with the conflicting requirements. Thereby, the impact of cybersecurity on innovation projects depends on industry, as well as company factors, technology management practice, and technology maturity. Leadership, risk measurement, organizational structures, culture, education, and awareness are further influencing aspects [11]. The two domains do, however, not necessarily conflict. While innovativeness was not found to be significantly correlated with cybersecurity management [37], assertions regarding cybersecurity and scaling value of new companies suggest the former should be part of the unique selling point (USP). This can be enabled by a culture based on beliefs like the willingness to protect the company and its customers from cyberattacks [38].

Focusing on the **innovation perspective**, culture and structures that promote flexibility positively affect innovation capability [39]. While both influence the cultural climate, productivity and efficiency can be increased if negative tensions are reduced while positive tensions are used [40]. Furthermore, innovation capability can be increased by separation and specialization creating freedom [41], as well as by information exchange and networking between explorative and exploitative departments [33]. Especially the integration of knowledge management can increase the efficiency of the innovation process [42]. Finally, innovativeness and risk management can coexist through appropriate leadership, enabling knowledge and identity development [43]. Enabling risk

assessments and management requires suitable methods [2], which differ per phase of the innovation life cycle [40]. Simpler techniques were found to fit the earlier and more complex quantitative methods the later phase [25].

From the **cybersecurity perspective,** the notion of a trade-off, e.g., regarding convenience [44] or data privacy [45], is not new. In this context, information asymmetry negatively influences the balance between business value and cybersecurity risk. In contrast, information sharing can promote proactive risk management and reduce the risk of cybersecurity under-investment [46]. Regarding project management in general, risk assessments are expensive and time-consuming. If they are performed before the project start, an agile IT security model can help organizations decide which projects to invest in. Applying this model does, however, require management commitment [47]. Another study recommends using cybersecurity capability maturity models to perform maturity self-assessments and 'design in' cybersecurity. This does, in turn, require creating awareness among project managers [48]. As with the different phases of the innovation life cycle, project phases must be differentiated. Based on a literature analysis regarding known breaches, risks can already arise during conception, can result from harmless activities, and effects can occur long after completion [49].

Our study aims to validate the assumption regarding the role of organizational ambidexterity, considering previously identified factors from the literature such as management awareness and early integration [32], while remaining open to additional factors mentioned by interviewees. We aim to gather these factors and formulate research propositions that can be further examined by a more in-depth study.

3. Methodology

Intending to conduct a first initial explorative study, we opted for an open, inductive research approach. Aiming to derive implications where causes and correlations are mainly unknown, we chose a qualitative **study design** using semi-structured expert interviews with mostly open-ended questions [50]. Based on the theoretical background, an interview guideline with five sections was created. After a brief introduction of our study, including relevant definitions, the first section covers the introduction of the interviewee. Interview partners were asked to describe projects within the automotive industry they were involved in and the role of cybersecurity in these. The second section deals with the balance of innovativeness and cybersecurity. This includes, for example, questions regarding a trade-off between the two, as well as regarding risks and challenges in this context. Besides, we asked about the prioritization of digital innovation or cybersecurity. The third section focuses on the strategic level and aims to determine which role the management plays in finding a balance between the two domains, whether managers are willing to take risks to speed up time to market and how prerequisites for finding a balance are created. The fourth section concentrates on the operational level in terms of interfaces between project teams, innovation, as well as cybersecurity capability, and their collaboration. Among others, transparency, as well as responsibilities within the teams, were examined, and decision-making processes were addressed. A final section tried to ensure all relevant aspects were covered.

The **data collection** was conducted in cooperation with a leading digital transformation consultancy. Our partner firm has units specialized in digital innovation and cybersecurity, focusing on global players in the automotive industry, thus possessing the required expertise. Since cybersecurity is a sensitive topic for which acquiring interview partners requires trust, our network within the company represented a valuable opportunity. The cooperation with a consultancy enables us to gain multi-faceted insights into various client projects simultaneously. Thus, care was taken to ensure that our interview partners contributed their experience from different clients to ensure a holistic perspective detached from organization-specific settings. To confirm that our interviewees' insight into organization-internal affairs was sufficient, we interviewed employees directly working for a market-leading automotive OEM. Furthermore, to rule out that our partner's consultants were biased, we interviewed an employee from a second consultancy. Potential interviewees were contacted with a one-pager providing background information on our study. Interview partners were selected based on their experience regarding digital innovation and cybersecurity capability in the automotive industry. All interviewees have at least six years of professional experience and have been part of the core team of multiple digital innovation projects, in which cybersecurity aspects had to be considered. Therefore, we focused on interviewing partners with a leadership role, defining strategies according to which these projects run. Furthermore, we took care to find interviewees with a distinct focus, from different organizational levels and business units, as well as with work experience in or, in the case of consultants, with other companies [50]. The interviews took place between May 5th and May 28th, 2020, and were recorded (see Table 1 for an overview). Conducting the interviews in German, the native language of all participants, ensured unambiguous communication and the elimination of language barriers [51]. Interview recordings were transcribed for **data analysis**. As communicated to all participants, the

conversations were anonymized to ensure company-specific information remains confidential. Next, we created a code system by clustering statements from the transcripts. This code system consists of main categories, split into sub-categories, summarizing various codes (see Table 2 for an excerpt). The first main category, 'General importance and trade-off', is, for example, subdivided into 'Importance due to digital transformation' or 'Trade-off between innovation and cybersecurity'. These codes aim to cluster the results regarding the need to consider cybersecurity and the justifications for a trade-off. The second main category, 'Strategic level', consists of sub-categories like 'Corporate culture', 'Management awareness and commitment', or 'Organizational structures'. They summarize the significance of culture, the importance attributed by leadership, and organizational structures in finding a balance. Finally, the third main category, 'Operational level', is, among others, subdivided into 'Communication', 'Processual integration', and 'Decision-making processes'. Under these codes, we clustered insights regarding the operational level, focusing on communication, risk management, timing, and decision-making.

Table 1. Overview of Interview Partners

ID	Level/ Unit	Focus	Experience	Affiliation	Duration
1	Manager; Digital Acceleration	IT strategy, operating model	10 years	Consultancy 1	34:27 min
2	Manager; Digital Services & Platform	e-Commerce, IT strategy	12 years	Consultancy 1	21:13 min
3	Senior Consultant; Automotive	Customer experience	11 years	Consultancy 1	26:18 min
4	Senior Manager; Inventive Finance, Risk and Compliance	Data management, process optimization	6 years	Consultancy 1	33:33 min
5	Consultant; Automotive Digital	Brand and customer experience	8 years	Consultancy 1	46:59 min
6	Vice President; Automotive	Sales, strategic transformations	22 years	Consultancy 1	26:05 min
7	Managing Partner Consulting Europe	Innovation Lead EMEA	23 years	Consultancy 2	28:01 min
8	Specialist Org. Design	Processes and organization	15 years	Automotive	23:19 min
9	Specialist Research	Research automotive security	6 years	Automotive	32:55 min

Table 2. Code system (Excerpt)

Main category	Sub-categories	Example
General importance and trade-off	Importance due to digital transformation	"Digital business models only work with very strong and functioning IT security." (I1)
	Trade-off between innovation and cybersecurity	"The biggest challenge is to find the right trade-off." (I2)
Strategic level	Corporate culture	"You need tolerance on all sides. In an innovation team, I naturally have very different cultures." (I8)
	Management awareness and commitment	"Management only wants the issues to be dealt with." (I4)
Operational level	Processual integration	"And what we can learn or do better is to always integrate cyber experts directly into the teams from the beginning." (I6)
	Decision-making processes	"With cybersecurity, we don't have a decision-making process […] as it would be the case with legal or integration." (I3)

4. Findings

4.1. General Importance and Trade-Off

Regarding the **relevance of innovativeness and cybersecurity** for the automotive industry, our interviewees stated that the digitalization of existing and the creation of innovative business models have become a necessity. Increasing investments show that premium manufacturers have understood this (I6). However, companies like Apple, Google, and Tesla are ahead in innovations (I2, I6) "because cybersecurity is a very integral part of their business" (I1). Besides their innovativeness, their reputation is not immune to damage from cybersecurity incidents (I5). Due to the multitude of databases, interfaces, as well as channels to customers, dealers, and third parties in various markets (I6), cybersecurity risks were considered relatively high in this industry. Developments associated with digital innovations, like increasing data volume, lead to the need to secure the vehicle (I6, I9) and the data flow to it to prevent a loss and misuse of both customer as well as company data (I5, I6). Therefore, it is necessary to constantly raise cybersecurity maturity and consider new technologies like quantum-secure encryption (I9). Consequently, cybersecurity is recognized as integral, and a holistic approach embedded in the digital strategy can even result in competitive advantages (I1, I4).

Five interviewees saw a **trade-off between innovativeness and cybersecurity** (I2-I4, I7, I8), while another two partly agreed or gave examples of such a trade-off later (I1, I5). The remaining two stated that cybersecurity risks should never be accepted (I6, I9). They consider cybersecurity to largely depend on the technical architecture and understand the existence of a trade-off as an indicator that it is ill-designed (I6). Our interviewees argue that ideally there shouldn't be any trade-offs. However, their experience shows that this often is not (yet) the case in practice. Interviewees perceiving a trade-off agreed that cybersecurity should ideally be a zero-tolerance issue, as cybersecurity breaches can render innovations obsolete (I7). They consider the time-to-market as the primary reason for this trade-off since this is "becoming increasingly important in today's world" (I2). According to them, testing minimum viable products (MVP) with customers as early as possible is essential. Despite knowledge about the importance of cybersecurity (I1; I3), companies do thus focus on an early go-live (I7) and core features promoting sales (I3). This is partly explained by the intangible benefit of cybersecurity (I3, I7), although shortcomings can lead to easily hackable products (I7). Furthermore, innovators fear that the involvement of cybersecurity experts might lead to a negative attitude towards technologies and reduce innovativeness (I1, I3). The same is true for having to compromise between secure and attractive solutions (I5). The cumbersome coordination with those responsible for cybersecurity might delay the innovation process (I1, I2, I4, I5), at worst resulting in the go-to-market being stopped (I2, I4, I5). Innovation projects being prestigious does, then, paradoxically lead to less attention being paid to regulations and cybersecurity not being integrated (I2-I4, I7). This effect is higher for internal, procedural than for customer-facing innovations (I4). The trade-off was considered important (I8) and potentially the biggest challenge in dealing with the two aspects (I2). Finding the right balance and increasing the cybersecurity maturity of innovations while maintaining agility and speed (I7) requires a pragmatic approach (I2, I3).

In terms of balancing innovation and cybersecurity capabilities, and as suggested in P2, our interview partners underlined the importance of organizational ambidexterity created by various factors (I1-I7). These factors are differentiated between strategic and organizational level.

4.2. Strategic Level

Organizational culture, awareness & commitment, and organizational structures were named influencing factors on the strategic level.

The perception of cybersecurity as a roadblock rooted in the organizational culture (I2, I4) was explained by a bilateral lack of tolerance by one interviewee. He claimed that both sides lack the willingness to open up, understand that both work differently, and collaborate (I7). An ideal culture was underlined to lead to tolerance for the different personalities of experts based on the understanding that investments in innovations are financed by the core business, which secures the company's future (I7). A start-up feeling with openness to risks created in centers of excellence or innovation hubs allows projects to develop freely (I8). While innovation was said to require safe spaces to experiment without consequences, guard rails were considered necessary to avoid risks when the go-life is forthcoming (I7).

Only three interviewees were convinced that the level of cybersecurity **awareness** in the automotive industry is appropriate (I6, I8, I9). Another five thought that there is awareness, without it leading to the topic being sufficiently considered in terms of implementation (I1-I5). As depicted above, cybersecurity is still considered less important than innovativeness (I2, I3), although the recognized importance of the topic increases (I2, I3, I5), e.g., driven by data integration (I5). In the context of innovation capabilities, our interviewees saw a need to improve the awareness for and the integration of cybersecurity (I1, I5). Without this, the consideration of cybersecurity is often merely a coincidence and does, for example, depend on a team member's earlier experiences (I3). If cybersecurity becomes an organization-wide requirement and projects must develop a technical architecture blueprint considering the topic, this was stated to be different (I9).

The lack of **management commitment** to consider cybersecurity despite potential consequences for innovativeness was considered another major challenge (I1, I3, I4), as "the management is not involved at all" (I2). Due to the amount of risk associated with cybersecurity (I6, I8, I9), this should be self-evident, but for the reasons depicted above, it often is not (I1-I4, I7). While innovativeness is positively incentivized, cybersecurity is often only driven by fear of negative consequences for management (I6). As there is much attention on data privacy due to EU GDPR penalties, cybersecurity risks are often further de-prioritized (I3). Furthermore, explicit knowledge in terms of integrating cybersecurity was reported to decrease with increasing hierarchy level (I4) since "the required skills are available in most companies but not understood at the management level (I1). In the long run, only awareness and management commitment to deal with the topic, not solely because of regulatory requirements, will ensure that issues like limited cybersecurity resources are

addressed (I2, I3). As one of our interviewees underlined, in Germany and Europe, more attention is already being paid than in the USA (I7). However, only two interviewees could refer to examples of high awareness and commitment (I8, I9).

Awareness and management commitment are expressed in **organizational structures**, starting with the Chief Information Security Officer. Without this function, cybersecurity is perceived as less important (I1). The impact of this role was said to depend on the function being reported to, as, for example, a Chief Financial Officer was considered more likely to be risk-averse than a Chief Marketing Officer (I1, I7). Establishing an innovation board representing both innovativeness and cybersecurity (I7) was mentioned as a best practice. In addition, a structural separation of exploration and exploitation was considered necessary (I1-I7). It does, however, not exist in every company, which was declared a mistake (I7). While essential to achieve effectiveness in innovations (I1-I7), this separation was claimed to lead to the neutrality required for their correct assessment from a cybersecurity perspective (I8). It can, however, lead to a disconnect from given frame conditions and silo-thinking. To overcome this, the separation on a structural level should be bridged through regular exchange with line functions and interdisciplinary teams on a project level (I1, I4). This requires tailor-made solutions and processes as these for exploration often do not fit exploitation and vice-versa (I8). Consequently, the existence of central and decentral cybersecurity units was considered positive (I1, I8). Balancing between centralization and decentralization requires flexibility and units with specific skills from which teams can be formed depending on objectives (I7). Even outside innovation units, organizations need to quickly adapt their organizational structure, as the development of process innovations needs resources while automation reduces routine activities freeing them (I8).

4.3. Operational Level

Communication, early integration, risk management, and decision-making processes were named as influencing factors on the operational level. According to our interviewees, the lack of awareness and knowledge to integrate cybersecurity into innovation capabilities is also common on this level (I3, I4). The involvement of cybersecurity experts is associated with a focus shift from building innovative solutions to managing risks (I2, I4) as “innovation takes a back seat to meet some crazy requirements” (I2). Complex cybersecurity requirements (I1, I2, I4) quickly become obstacles that block the implementation and prevent the go-live (I2, I4). They are associated with higher costs and sales price (I4, I9), which leads to the perception of cybersecurity being hindering (I1, I2, I4).

Regular **communication**, structured information exchange, and collaboration between innovation and cybersecurity capability were reported to be vital in establishing guard rails for innovations. They are required to ensure a timely, risk-based integration, as well as quick decision-making (I1-I4, I6). From a holistic perspective, the lack of communication leads to innovation teams developing solutions in isolation. They invest time and money without knowing whether they will get the cybersecurity’s approval (I5). From the innovation capability’s perspective, communication and knowing relevant counterparts can significantly contribute to project speed, as an informal exchange does then suffice in many cases (I2, I4). While this is often already the case for data privacy due to the EU GDPR, it is yet to be established for cybersecurity (I3).

Seven interviewees stated that an **early integration** of cybersecurity into innovations is needed (I1, I3, I5-I9). They agreed that the topic is often integrated too late as innovation teams “build their playground” (I1, I4) instead of “creating secure sandboxes to test and approve innovations” (I7). Often, cybersecurity reviews are conducted at the end of the implementation phase, before go-life (I2-I4), and “no one from IT security is involved right from the start” (I4). This can result in additional pressure on the cybersecurity capability (I7) and intensifies the disconnect (I2). Only two interviewees had experienced cybersecurity being discussed in an early workshop (I1, I5). Another two had experience with cybersecurity integrated into the evaluation phase when it is decided if an idea should be further invested into (I7, I9). To ensure an early integration, a criteria catalog to be fulfilled by innovations can help (I7, I9), although it might have to be regularly extended due to the increasing impact of cybersecurity (I9). This, or the integration into technical conception and architecture, both supported by the cybersecurity capability (I2), were considered best practices. Like this, cybersecurity can become indispensable and self-evident (I5), an essential requirement like data privacy (I5, I6).

Cybersecurity **risk management** and perception (I2, I5) were mentioned as key factors regarding the balance between innovation and cybersecurity. When asked about the digital innovations they have worked on, about 50% of the interviewees acknowledged that early versions might have been hackable (I3, I4, I6-I8). All others considered their innovations secure, and the security mechanisms implemented sufficient (I1, I2, I5, I9). Besides by a lack of awareness, this inhomogeneous risk perception was explained by the complexity of risk assessments in large companies and system landscapes (I7). Interview partners admitted this could be disastrous

when innovations have interfaces to systems requiring high security (I7, I8). If risk assessments are performed, these assessments are neither critically evaluated nor put into relation to the limitations their mitigation would impose on the innovation (I2). Integrating cybersecurity risk assessments in the innovation process was considered beneficial. However, it was deemed necessary to make risks tangible as with EU GDPR (I5). If the consequences of a cybersecurity breach are perceived to be less drastic, the issue will be de-prioritized (I5), and security gaps might result (I3).

Missing coordination, the lack of a structured **decision-making process** with suitable interfaces, and the unavailability of experts to support this process were said to be further limiting factors (I3, I7). This lengthy process usually results in too many, too complex requirements (I1, I2, I4). For the, in some respects, heavily regulated automotive industry, the usage of external, open-source software components while considering complex, internal regulations (I7), as well as the cooperation with suppliers, were mentioned as incredibly challenging examples. The latter often requires the same certification as for security-critical departments. These requirements can often not be met by start-ups involved in the innovation process, for which more flexible approaches need to be found (I7).

5. Discussion

As indicated by existing research [2, 11], experts in the automotive industry perceive a trade-off between digital innovation and cybersecurity capabilities, stating the prioritization of the former as the key reason. While cybersecurity can add value for customers, innovation often takes precedence in prestigious projects. Thus, cybersecurity risks arise by focusing on sales features and time-to-market strengthened by factors like the difficulty of risk assessments, for example, due to limited cybersecurity resources [25, 43, 49].

This paper tried to determine the role of organizational ambidexterity to overcome this trade-off. As suggested by the literature on cybersecurity in specific [10], as well as on exploratory and exploitative capabilities in general [12, 30], our interviewees considered organizational ambidexterity essential in finding a balance between innovation and cybersecurity capability. Even though literature suggests that rigid organizational structures impede organizations from simultaneously meeting the requirements of both [9], structural ambidexterity, i.e., the separation between explorative and exploitative business units, was regarded as necessary. According to our interviewees, innovativeness requires a certain failure culture and a degree of freedom, while the standardization enabled by centralization benefits cybersecurity. Our findings suggest that it is beneficial to bridge this structural separation depending on the risks associated with an innovation, i.e., to combine aspects of structural and contextual ambidexterity. This has, to our knowledge, not been proposed so far and can, according to our interviewees, be enabled by factors on both a strategic and operational level.

Regarding the strategic level, it was confirmed that the role of innovativeness and cybersecurity in strategy, vision, and business models must continuously be questioned [1]. Conforming with the literature [26], this leads to the importance of a holistic cybersecurity strategy covering innovation capabilities. A corporate culture promoting tolerance [39] and managers with the necessary understanding that show the required commitment to balance innovation and risks [43] like cybersecurity will result. Flexible, hybrid organizational structures, like centralized and decentralized cybersecurity resources [11, 12, 30, 32], are another essential countermeasure to prevent cybersecurity from being perceived as less important than innovation and not being adequately addressed [11, 47].

Concerning the organizational level, our research emphasizes the need for a risk-based and early integration of cybersecurity into the innovation process, which overlaps with literature findings [47]. Pragmatic approaches to compare risks with potential disadvantages for innovativeness [3, 44] can thus become relevant. Overall, they can help to minimize expensive and time-consuming projects [25]. However, as emphasized in the literature, interview partners criticize the missing communication, e.g., a regular and structured exchange and collaboration between both innovation and cybersecurity capabilities. Transparent communication and decision-making processes must be implemented, enabling the seamless integration of cybersecurity [11]. Like this, the conflict between the two capabilities can proactively be minimized while maximizing efficiency and effectiveness.

We have summarized our findings in a set of research propositions to be verified in future studies:

Proposition 1 (P1): Organizations in the automotive industry perceive a trade-off and prioritize innovation over cybersecurity in new products and business models.

Proposition 2 (P2): Organizational ambidexterity enabled by strategic and operational elements is significant in finding this balance.

Proposition 3 (P3): On a strategic level, corporate culture, management awareness & commitment, and organizational structures enable organizational ambidexterity in terms of digital innovation and cybersecurity.

Proposition 4 (P4): On an operational level, transparent communication, risk-based & early

integration, and clearly defined decision-making processes support finding the balance between digital innovation and cybersecurity.

Our propositions are hierarchically related. Elements on the strategic influence those on the operational level and jointly lead to increased organizational ambidexterity. This, in turn, influences the balance of digital innovation and cybersecurity capability and leads to organizational benefits, like improved innovation output and fewer cyber incidents.

Our study provides various **contributions**. From a theoretical perspective, we created a short overview of the literature regarding the trade-off between innovation and cybersecurity. To our knowledge, the role of organizational ambidexterity in this context constitutes a research gap. Especially as our interviewees proposed to bridge structural ambidexterity with contextual elements, our results hint at a potential expansion of organizational ambidexterity theory. Therefore, our study contributes insights concerning several influencing factors summarized in our research propositions. As we focus on governance, instead of methodology or technology aspects more thoroughly researched in the context of cybersecurity and innovativeness, we believe our findings to be of high relevance. From a practitioner's perspective, we think that the identified factors can, after further validation, serve as a frame of reference for organizations trying to balance innovation and cybersecurity. These can be used to ensure that both strategic and operational perspectives are considered. However, as organizations are different, these influencing factors must be adapted to the specific characteristics and requirements.

Besides its contributions, this paper has some **limitations**. Due to the relatively small number of interviews, it can only be considered an initial exploration. As it proved difficult to find interview partners from the automotive industry, we decided to conduct expert interviews with management consultants and verify them against a small number of automotive industry employees. While consultants can undoubtedly provide valuable insights, they might lack insights and information for an unbiased assessment of client organizations. Besides, since interviewees can only provide their personal experience, the interview partner selection may have affected the results. Our interview questionnaire specified certain aspects to ensure their discussion during the interviews. Although we formulated questions carefully, this might have influenced our interviewees. The evaluation may be methodically biased, which we tried to counteract through member checking. Still, findings remain subject to interpretation [52]. Conducting the interviews in German eases communication but leads to potential inaccuracies due to translation. While our findings might not be limited to the automotive industry, they have only been verified in discussions with fellow researchers and must be evaluated in practice. Finally, we did intentionally focus on the governance perspective. A holistic approach would require integrating implementation methodology- or technology-specific findings.

These limitations lead to a potential for **further research**. To create a holistic view on balancing innovativeness and cybersecurity and verify the identified influencing factors, a survey with a significantly higher number of participants is required. Since the findings may not be exhaustive, further research could aim to expand them. It would be interesting to measure their contribution in balancing innovation and cybersecurity. Even though our interviewees provided valuable and far-reaching insights, it would thereby be important to focus on internal employees of the automotive industry. In addition, it would be of interest to analyze the factors in different companies in the automotive industry and other industries. It could be revealing to choose an industry with comparable characteristics in which organizational ambidexterity is equally important. Doing so, company- or industry-specific adaptations of our findings could be derived, which would again have to be tested for practical relevance.

As the balance between innovation and cybersecurity is increasing in relevance, we hope that our findings will help to improve organizational ambidexterity in this context. Secure innovations could result, leading to competitive advantages for organizations and better products for customers.

Appendix. Interview Guideline

Opening [36]

- Could you please introduce yourself?
- In the context of which project have you already been involved with innovations in the automotive industry?
- How innovative do you think it is compared to the competition? Is it more of a laggard or a pioneer in the industry in terms of innovation/ cybersecurity?

Innovation & Cyber Security [11, 48]

- Do you see risks in the use of innovations? Which ones? Do solutions already exist to minimize them?
- Have you worked on an innovation that was found to be potentially "hackable" at an early stage? Which innovation, to what extent was it hackable?
- How would you describe the importance of cybersecurity aspects in the projects? Is there a high priority attributed relative to the implementation of innovations?
- At what point in a project is cybersecurity integrated?
- Do you see the need to consider cybersecurity more strongly in the context of innovation projects?

- Has a project ever been canceled early due to cybersecurity concerns?
- In your opinion, is there a trade-off between digital innovations and cybersecurity?
- Can you give an example of where the balance between driving digital innovation and a focus on cybersecurity has been exceptionally well or particularly poorly?
- What are the challenges you see in dealing with innovation and cybersecurity?
- Why do they exist, and how can they be eliminated? E.g., early integration of cybersecurity in innovation
- Are there factors that are holding the innovation project back? Which ones?

Strategic level [12, 33, 34]

- What role does management play in shaping the innovation process regarding the integration of cybersecurity?
- Are managers willing and able to accept risk if this has a positive impact on speed and time-to-market?
- Does management focus on the capabilities required to implement the overall strategy/vision with respect to innovation and cybersecurity?
- Does segregation of duties exist with respect to exploration (i.e., new product development) and exploitation (e.g., efficiency improvement or product quality)? How would you describe and rate this?

Organizational and operational level [33, 36]

- How is the innovation process shaped at the customer level? Rather through team innovations or by implementing existing innovations?
- How would you evaluate the interfaces between your project team and the cybersecurity department? Does collaboration take place, or does cybersecurity remain ignored if it is not part of the project?
- Is there a dedicated function/expert in the project teams who takes over the interface function? How is transparency ensured among all project participants?
- How has the work with the teams in the cybersecurity/ innovation department been structured? How is cybersecurity included in innovation projects?
- How is the decision-making process regarding cybersecurity for innovations? Which decisions must be approved by the cybersecurity function, and which ones can be made by the project team?
- To what extent does speed/time-to-market suffer because of these decision-making processes?

Conclusion

- This concludes the structured part of the interview. Is there anything else you would like to add?

References

[1] Hoerlsberger, M., "Innovation Management In a Digital World", Journal of Manufacturing Technology Management, 30(8), 2019, pp. 1117–1126.

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

[3] Lambert, F., "Tesla car hacked using drone; a patch has already been released", Electrek.co, 13.5.2021.

[4] Sapin, D., J. Cline, J. Aqua, and M. Lieberman, How Consumers See Cybersecurity and Privacy Risks: Consumer Intelligence Series: Protect.me, 2.3.2020.

[5] Hida, E., B. Melo, M. Devine, and T. Alstein, Future of Risk Management in Financial Services: Integrating Risk Management and Agile Projects, 2019.

[6] Fuchs, C. and F.J. Golenhofen, Mastering Disruption and Innovation in Product Management, Springer, Cham, 2019.

[7] Chinn, D., J.M. Kaplan, and T. Poppensieker, Transforming Cybersecurity: New Approaches for an Evolving Threat Landscape, 2014.

[8] Schmittner, C. and G. Macher, "Automotive Cybersecurity Standards - Relation and Overview", in Computer Safety, Reliability, and Security, A. Romanovsky, E. Troubitsyna, I. Gashi, E. Schoitsch, and F. Bitsch, Editors. 2019. Springer: Cham.

[9] Kaplan, J., W. Richter, and D. Ware, Cybersecurity: Linchpin of the digital enterprise, 2019.

[10] Schinagl, S., S. Khapova, and A. Shahim, "Tensions that Hinder the Implementation of Digital Security Governance", in ICT Systems Security and Privacy Protection, A. Jøsang, L. Futcher, and J. Hagen, Editors. 2021. Springer International Publishing: Cham.

[11] Nelson, N. and S. Madnick, "Studying the Tensions between Digital Innovation and Cybersecurity", in 23rd Americas Conference on Information Systems 2017.

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

[13] Clauss, T., S. Kraus, F.L. Kallinger, P.M. Bican, A. Brem, and N. Kailer, "Organizational ambidexterity and competitive advantage: The role of strategic agility in the exploration-exploitation paradox", Journal of Innovation & Knowledge, 2020.

[14] Carayannis, E.G., E. Grigoroudis, S.S. Rehman, and N. Samarakoon, "Ambidextrous Cybersecurity: The Seven Pillars (7Ps) of Cyber Resilience", IEEE Transactions on Engineering Management, 68(1), 2021, pp. 223–234.

[15] Jeyaraj, A. and A.H. Zadeh, "Exploration and Exploitation in Organizational Cybersecurity", Journal of Computer Information Systems, 2021, pp. 1–14.

[16] Chanias, S. and T. Hess, "Understanding Digital Transformation Strategy Formation: Insights from Europe's Automotive Industry", in 20th Pacific Asia Conference on Information Systems 2016.

[17] https://pubs.opengroup.org/architecture/togaf91-doc/arch/, accessed 6-8-2021.

[18] Mohd Bukhari, A.M. and M. Faiz Hilmi, "Challenges and Outcome of Innovative Behavior: A Qualitative Study of Tourism Related Entrepreneurs", Journal of technology management & innovation, 7(2), 2012, pp. 131–143.

[19] Kuhnert, F. and C. Stürmer, eascy - Die fünf Dimensionen der Transformation der Automobilindustrie, PricewaterhouseCoopers, 2017.

[20] Solms, R. von and J. van Niekerk, "From Information Security to Cyber Security", Computers & Security, 38, 2013, pp. 97–102.

[21] Harloff, T., "Hacker-Angriff auf einen Jeep Cherokee in den USA", Süddeutsche Zeitung, 22.7.2015.
[22] https://www.bcg.com/publications/2015/growth-lean-manufacturing-rising-need-for-innovation-speed.aspx, accessed 3-1-2021.
[23] Chronopoulos, M., E. Panaousis, and J. Grosskags, "An Options Approach to Cybersecurity Investment", IEEE Access, 6, 2018, pp. 12175–12186.
[24] Chang, S.E. and C.B. Ho, "Organizational factors to the effectiveness of implementing information security management", Industrial Management & Data Systems, 106(3), 2006, pp. 345–361.
[25] Bowers, J. and A. Khorakian, "Integrating Risk Management in Innovation Project", European Journal of Innovation Management, 17(1), 2014, pp. 25–40.
[26] Abbosh, O. and K. Bissell, Securing the Digital Economy: Reinventing the Internet for Trust, 2019.
[27] Baca, D., M. Boldt, B. Carlsson, and A. Jacobsson, "A Novel Security-Enhanced Agile Software Development Process Applied in an Industrial Setting", in 10th International Conference on Availability, Reliability and Security 2015. IEEE.
[28] Backes, M. and J. Müller-Quade, Entwicklung sicherer Software durch Security by Design: Trend- und Strategiebericht, SIT Technical Reports, 2013.
[29] Sollins, K.R., "IoT Big Data Security and Privacy Versus Innovation", IEEE Internet of Things Journal, 6(2), 2019, pp. 1628–1635.
[30] Raisch, S., J. Birkinshaw, G. Probst, and M.L. Tushman, "Organizational Ambidexterity: Balancing Exploitation and Exploration for Sustained Performance", Organization Science, 20(4), 2009, pp. 685–695.
[31] March, J.G., "Exploration and Exploitation in Organizational Learning", Organizational Science, 2(1), 1991, pp. 71–87.
[32] Duncan, R.B., "The Ambidextrous Organization: Designing Dual Structures for Innovation", in The Management of Organizations: Strategy, Structure, Behavior, R.W. Griffin, Editor. 1992. Houghton Mifflin Co.: Boston.
[33] Jansen, J.J.P., M.P. Tempelaar, F.A.J. van den Bosch, and H.W. Volberda, "Structural Differentiation and Ambidexterity: The Mediating Role of Integration Mechanisms", Organization Science, 20(4), 2009, pp. 797–811.
[34] Liu, L. and D. Leitner, "Simultaneous Pursuit of Innovation and Efficiency in Complex Engineering Projects: A Study of the Antecedents and Impacts of Ambidexterity in Project Teams", Project Management Journal, 43(6), 2012, pp. 97–110.
[35] O'Reilly, C.A. and M.L. Tushman, "Organizational Ambidexterity in Action: How Managers Explore and Exploit", California Management Review, 53(4), 2011, pp. 5–22.
[36] Zaidi, M.F.A. and S.N. Othman, "Structural Ambidexterity vs. Contextual Ambidexterity: Preliminary Evidence from Malaysia", Social sciences, 10(6), 2015, pp. 1200–1207.
[37] Ernest Chang, S. and C.-S. Lin, "Exploring organizational culture for information security management", Industrial Management & Data Systems, 107(3), 2007, pp. 438–458.
[38] Bailetti, T. and D. Craigen, "Examining the Relationship Between Cybersecurity and Scaling Value for New Companies", Technology Innovation Management Review, 10(2), 2020, pp. 62–70.
[39] Bock, A.J., T. Opsahl, G. George, and D.M. Gann, "The Effects of Culture and Structure on Strategic Flexibility during Business Model Innovation", Journal of Management Studies, 49(2), 2012, pp. 279–305.
[40] Isaksen, S.G. and G. Ekvall, "Managing for Innovation: The Two Faces of Tension in Creative Climates", Creativity and Innovation Management(19), 2010, pp. 73–88.
[41] Andriopoulos, C. and M.W. Lewis, "Exploitation-Exploration Tensions and Organizational Ambidexterity: Managing Paradoxes of Innovation", Organization Science, 20(4), 2009, pp. 696–717.
[42] Du Plessis, M., "The Role of Knowledge Management in Innovation", Journal of Knowledge Management, 11(4), 2007, pp. 20–29.
[43] Borgelt, K. and I. Falk, "The Leadership/Management Conundrum: Innovation or Risk Management?", Leadership & Organization Development Journal, 28(2), 2007, pp. 122–136.
[44] Kim, B.C. and Y.W. Park, "Security versus convenience? An experimental study of user misperceptions of wireless internet service quality", Decision Support Systems, 53(1), 2012, pp. 1–11.
[45] Olt, C. and A. Wagner, "Having Two Conflicting Goals in Mind: The Tension Between IS Security and Privacy when Avoiding Threats", in 53rd Hawaii International Conference on System Sciences (HICSS 2020). 2020.
[46] Gordon, L.A., M.P. Loeb, W. Lucyshyn, and L. Zhou, "The impact of information sharing on cybersecurity underinvestment: A real options perspective", Journal of Accounting and Public Policy, 34(5), 2015, pp. 509–519.
[47] Hutchinson, D., H. Maddern, and J. Wells, An Agile IT Security Model for Project Risk Assessment, 2011.
[48] Payette, J., E. Anegbe, E. Caceres, and S. Muegge, "Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects", Technology Innovation Management Review, 5(6), 2015, pp. 26–34.
[49] Shropshire, J., S. Presley, and J. Landry, "Cybersecurity Threats in the Context of Project Meta-Phases", in 24th Americas Conference for Information Systems 2018.
[50] Myers, M.D. and M. Newman, "The qualitative interview in IS research: Examining the craft", Information and Organization, 17(1), 2007, pp. 2–26.
[51] Marschan-Piekkari, R. and C. Reis, "Language and Languages in Cross-cultural Interviewing", in Handbook of qualitative research methods for international business, R. Piekkari, Editor. 2004. Edward Elgar: Cheltenham, UK.
[52] Kaptchuk, T.J., "Effect of interpretive bias on research evidence", BMJ (Clinical research ed.), 326(7404), 2003, pp. 1453–1455.