# Cybersecurity vs. Digital Innovation: A Trade-off for Logistics Companies?

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

Nils Hoffmann
Technical University of Darmstadt
nilshoffmann@outlook.com

## Abstract

*Digital innovations are essential for companies in the 21st century. However, due to their reliance on (new) technologies, they are associated with cybersecurity risks. As the reduction of these can negatively affect an organization's innovation capability, a trade-off might result. This trade-off has, to our knowledge, not yet been sufficiently researched. Our paper contributes to closing this research gap using semi-structured interviews with 14 digital innovation and cybersecurity experts in the German logistics industry. Findings from these interviews suggest that there are different types of tensions between digital innovation and cybersecurity capabilities detrimentally influencing innovations in three ways: by slowing down (temporally), requiring more resources (economically), or restricting innovative freedom (functionally). Furthermore, we were able to identify triggering and resolving factors. Thereby, our paper offers valuable contributions from both a theoretical as well as practical perspective.*

## 1. Introduction

The digital transformation puts companies under pressure to innovate. However, it not only brings opportunities but also leads to a changing risk landscape, e.g., in terms of cybersecurity [17, 57]. Interestingly, cybersecurity is perceived as hindering the innovation capability. This leads to a potential trade-off for companies. A balance between the two needs to be found to prevent adverse effects [7, 44, 50]. Only about 13% of the companies are convinced to have solved this challenge [44]. Although tensions between the two capabilities have been documented [2, 12, 35, 44, 50, 52], research is still in its infancy.

In the logistics industry, digitalization and digitization are considered central challenges. In addition to the investment costs themselves, companies are deterred by the costs of cybersecurity and the danger of industrial espionage [7]. While various studies examine the potential of digital innovations [3, 31, 38], the relevance of cybersecurity is underlined by recent incidents. The attack on Toll, for example, caused damage in the hundreds of millions of euros [20]. According to predictions, the importance of both digital innovation and cybersecurity will increase [4, 51].

From our perspective, industry specifics, i.e., the degree of innovativity and the relevance of cybersecurity, play an essential role in the trade-off. We thus argue that an industry-specific study is a reasonable next step. Despite their relatively low importance in the logistics industry today, it makes sense to examine the current attitude towards the two capabilities, identify existing tensions, and research ways to overcome them. Like this, cybersecurity vulnerabilities can hopefully be prevented from being built-in when innovations are being rashly developed in the future.

To contribute to the understanding of the interplay between cybersecurity and innovation capabilities, we chose an inductive, grounded, theory development approach. Thereby, we want to uncover the emic perspectives of the participants toward the tensions between the two capabilities and compare those with the etic perspective provided by literature. Aiming at tension recognition (i.e., what are different types of tensions), salience (i.e., when and how do certain types of tensions become visible), and resolutions (i.e., how can tensions be resolved in practice), we decided to conduct an interview study with innovation and cybersecurity experts in the German logistics industry to answer the following research questions:

*Do companies in the German logistics industry perceive a trade-off between cybersecurity and digital innovation?,*
*How can tensions be classified?, and*
*What are triggering and resolving factors?*

In the next chapter, we describe the theoretical background and derive research propositions. Next, our research methodology is explained before the findings of our study are presented. We discuss the results and limitations of our work and finish with a conclusion.

## 2. Background and research propositions

Digital innovation and cybersecurity are growing fields with a considerable amount of research. We use

URI: https://hdl.handle.net/10125/80161
978-0-9981331-5-7

both terms as placeholders for the respective capabilities, i.e., an organization's, person's, or system's ability achieved by "a combination of organization, people, processes and technology" [54].

**Digital innovation** refers to the ability to create new products, services, or business models based on digital technologies [19]. Such digital innovations have been predicted to generate up to 1.5 trillion US$ in sales potential in worldwide logistics [60]. Consequently, there are various examples, e.g., the usage of digital voice assistants [31]. However, the German logistics sector is relatively slow in implementing these [60].

**Cybersecurity**, mistakenly used as a synonym for information security, is not limited to the ability to protect information resources from cyber-attacks but goes beyond and includes other assets like humans [53]. It attempts to make the associated risks controllable and mitigate them [14]. This is particularly complex in the interwoven supply chains of logistics companies [23]. These represent an attractive target for hackers [51] as numerous incidents underline [8].

Despite our grounded approach, we are not starting at zero but base on existing research. As there is limited logistic-specific research, we primarily draw on non-sector-specific contributions to derive propositions.

Digital innovations are often associated with tensions. When seeking to overcome such tensions, a theory frequently referred to is organizational ambidexterity theory [1, 13]. It seeks to explain how companies can balance exploration and exploitation [6]. The notion that risk-mitigating activities are time and resource-intensive [14] and can restrict innovative freedom is not new [11]. Consequently, a tension between innovation and cybersecurity has been identified, and organizational ambidexterity theory has been used as a frame [50]. The term ambidextrous cybersecurity has been proposed for a stage-gate model describing the capability to protect information resources while leveraging technological innovations [12]. Furthermore, it has been argued that organizations need to explore new while exploiting old cybersecurity mechanisms [35]. The relationship between cybersecurity and scaling value has been examined to improve the understanding of these factors in innovations and for start-ups [2]. An approach for evaluating risk-reward trade-offs has been proposed and applied. Industry-, firm-, technology management- and technology maturity-specific factors influencing the trade-off were identified [44]. A framework to prioritize cybersecurity at the beginning of projects was established [45]. We are unaware of logistics-specific research of this trade-off.

**P1** – *Companies in the German logistics industry perceive different tensions between cybersecurity and innovation capabilities that result in a trade-off.*

In this context, (industry-specific) external factors like competitive pressure and regulations are believed to be important. Managers tend to higher risk-taking under competitive pressure [39]. Given this pressure, organizations are likely to prioritize competitive advantages through innovation while neglecting the side effects of insufficient cybersecurity [44]. In cybersecurity, they do not see the added value but the avoidance of possible losses through additional costs [18]. However, research suggests that high cybersecurity standards can lead to competitive advantages [22, 36]. Regulations have a two-sided purpose in this context: they shall enable innovation while preventing damage to society [59]. The EU, for example, is trying to create innovation-friendly conditions, but regulations like its data protection regulation can also cripple innovation [40]. This effect has been confirmed for the logistics industry, e.g., the railroad business [24]. Concerning cybersecurity, the European Critical Infrastructure (ECI) regulation strongly affects the industry [56]. Despite the industry's high innovation potential [60], this might explain that many companies have small innovation budgets and adopt incremental innovations [58].

**P2** – *External factors like competitive pressure and regulations influence innovation and cybersecurity capabilities. Both are equally important for most German logistics companies, e.g., due to a pressure to innovate in a regulated environment.*

Besides external factors, internal factors like organizational culture, structures, and the collaboration between the capabilities are likely to have an influence.

Regarding the organizational culture, cybersecurity benefits from control-oriented cultures that emphasize effectiveness and consistency. This is typically the case in risk-averse industries, like the logistics industry [14, 58]. A company's ability to innovate was found to be negatively related to cybersecurity management [15]. Instead, it is positively influenced by flexibility [9, 25]. Additionally, the cooperativeness within a company is negatively related to confidentiality, one of cybersecurity's objectives [15]. At the same time, the accompanying knowledge transfer within a company is a strong driver of innovation [46]. An organization's management is vital for implementing its culture. Regarding innovation, management has a role in balancing ideas and personal tensions [33]. Concerning cybersecurity, it was shown that the awareness of and commitment to cyber risks at this level varies and influences the importance given to the topic [41]. Thus, it has been argued that regulations and risk management are no substitute for expertise, awareness, and cooperation between leadership and management [10].

**P3a** – *Organizational culture: Risk-averse or control-oriented organizational cultures, predominant*

*in German logistics, negatively influence innovation but positively affect cybersecurity capabilities.*

Organizational structures are supposed to play a role in the trade-off. Innovation capabilities are usually anchored in explorative units prepared to take risks to leverage opportunities, while cybersecurity capabilities are defined by exploitative units, prioritizing the minimization of (cyber) risks [cf. 21]. Thus, organizational ambidexterity, especially structural ambidexterity, might help to frame the trade-off. It has been shown that knowledge exchange and networking between explorative and exploitative departments promote innovative strength [34]. At the same time, it is necessary to create freedom through specialized fields of work to increase the departments' performance [1]. Interestingly, an information asymmetry resulting from separation can throw the prioritization between risk and business value off balance. Thus, information sharing promotes a proactive approach to (cyber) risk and reduces cybersecurity under-investment [28]. As German logistics is rather immature with respect to digital innovations, small units separated from the rest of the organization can be expected.

**P3b** – *Organizational structure: The trade-off between digital innovation and cybersecurity is stronger for organizations with clearly separated capabilities, which is usually the case in German logistics.*

How the cybersecurity and innovation capability are integrated on an operational level influences the trade-off. In the early phases of an innovation, creative freedom, flexibility, and risk-taking are essential [33, 37]. However, an early consideration of cybersecurity measures is also necessary [45, 47]. This, in turn, could restrict the innovation capability. One solution could be to implement cybersecurity depending on the risks associated with an innovation, which has already been proposed for risk management in general [11]. A selective approach enables freedom and creativity in the ideation phase while ensuring risk-mitigating measures are implemented later. However, this is not standard practice [44], likely because of experience deficits and as time-consuming methods aggravate early risk assessments [32]. Due to the low status of innovation and cybersecurity, we assume this isn't the case in logistics companies either.

**P3c** – *Integration & collaboration: Tensions between cybersecurity and innovation capabilities are weakened by early integration & continuous cybersecurity risk management, not yet the norm in German logistics companies.*

## 3. Method

While a single paper certainly cannot simultaneously examine factors like regulation, culture, and structure in detail, other factors are not explicitly mentioned in our propositions, e.g., customers' pressures or technology. Rather than being exhaustive, the propositions are intended as a structure for our study. We aim to understand their relevance while allowing our experts to express divergent ideas. Reflecting the nature and low maturity of the research topic, we chose an inductive, grounded, theory development approach and selected semi-structured expert interviews as a data collection method. This qualitative approach will not enable us to verify or reject our propositions. The type of interview does, however, allow for in-depth, follow-up questions. As this requires a sound knowledge base [26], we conducted 18 preparatory discussions with representatives of digital transformation consultancies and companies operating in various industries. An interview guideline was then prepared to steer the interviews and prevent drifting into unrelated topics [42, 43]. This guideline has five parts: First, we started with an introduction to the topic, including definitions of digital innovation and cybersecurity, before asking the interview partner for professional background, current position, and a description of the company for which he/she works. Second, the interview revolved around the role of digital innovations for the organization, how they are used, and whether cybersecurity concerns are associated [7, 16, 52, 58, 60]. Third, our interviews focused on whether there is a trade-off between the two topics, asking for examples in which the integration worked particularly well or poorly [27, 44]. Fourth, we asked about the conflict from an organizational and operational perspective. Questions aimed at triggering and resolving factors, how and when cybersecurity is integrated into the innovation process, and the distribution of responsibilities in this process [5, 10, 11, 34, 44, 47, 49]. Fifth, concluding questions made sure all relevant points were addressed and tried to identify further interviewees. A pre-test with fellow researchers ensured all questions were understandable. We are happy to provide the interview guideline upon request.

For **data collection**, we looked for interview partners with experience in the subject area [42]. Thus, individuals involved in digital innovations in which cybersecurity has an impact were chosen. Examples of such individuals are managers of innovation projects/programs, departments with innovation focus (e.g., Head of IoT, Head of Digital), and digitalization or IT in general (e.g., Chief Information Officer (CIO), IT manager). Furthermore, to cover both perspectives, we talked to cybersecurity experts involved in the innovation process, e.g., as advisors to the roles above. Exemplary roles of these experts are Chief Information Security Officer (CISO) or IT security manager. Interview partners were acquired from the researchers' network, via LinkedIn or by directly contacting logistics

companies. Furthermore, we used a snowballing approach. A total of 14 experts from 12 companies were interviewed, with some respondents explicitly drawing on experience from former positions (see Table 1 for an overview). The number of people from the same companies was intentionally kept low to cover a broad spectrum. We deliberately chose mostly large companies that are likely to have more extensive resources, e.g., dedicated innovation and cybersecurity departments [30, 48].

**Table 1. Overview of interview partners**

| | | | Responsibility/ Expertise[1] | | | |
|---|---|---|---|---|---|---|
| **ID** | **Position** | **Company size** | **Logistics** | **Innovation** | **Cybersecurity** | **Date and duration** |
| 1 | CEO; former Vice President of Asset Digitization | <50; ~30.000 | + | + | - | 27th Apr 20, 35 min |
| 2 | Head of Digital Transformation / BPM | ~40.000 | + | + | = | 29th Apr 20, 47 min |
| 3 | Technology Expert; Client Project Lead | ~450.000; ~30.000 | = | + | = | 28th Apr 20, 23 min |
| 4 | Head of Digital Air Freight | ~75.000 | + | + | - | 07th May 20, 27 min |
| 5 | Business Consultant (IS) | ~10.000 | + | + | - | 07th May 20, 26 min |
| 6 | Head of Innovation Strategy | ~325.000 | + | + | - | 06th May 20, 14 min |
| 7 | Head of Digital Security | ~4.500 | + | - | + | 08th May 20, 31 min |
| 8 | CEO | <50 | = | = | + | 14th May 20, 43 min |
| 9 | Head of IT & Project Mgmt. | ~7.500 | + | + | = | 14th May 20, 28 min |
| 10 | Head of IoT | ~75.000 | + | + | = | 14th May 20, 27 min |
| 11 | CIO | ~5.000 | + | + | = | 20th May 20, 38 min |
| 12 | Director Logistics, Strategy, and Business Development | ~6.500 | + | + | = | 12th Jun 20, 18 min |
| 13 | Associated Partner Cybersecurity | ~150 | = | - | + | 19th May 20, 32 min |
| 14 | Head of Information Security Mgmt. | ~40.000 | + | - | + | 09th Jun 20, 39 min |

1: Expertise levels: +: Expert knowledge; =: Average knowledge; -: No knowledge; rated by authors based on information like years of work experience from interview partner introduction and additional sources (e.g., LinkedIn profile, Google search results)

**Table 2. Topic areas incl. examples (Excerpt)**

| **Topic area** | **Example** |
|---|---|
| Importance of innovation | "Of course, it has an enormous significance, and has also become more and more important in recent years. […] What is changing, of course, are the accompanying digital processes" (I9) |
| Innovation pressure | "We don't have pressure to innovate; we have a desire to innovate, that's a big difference." (I12)<br>"Absolutely. Honestly, I think this industry has rested on its laurels for too long." (I13) |
| Importance of cybersecurity | "We are known for […] tested, working solutions […], both in terms of logistics, but also in terms of digital products. […] The expectation […] is that the whole product is very secure." (I10) |
| Logistics-specific threats | "On the one hand [...] [we have] a large network with many […] companies [...] On the other hand, there is always the question: How critical is the data for the customer?" (I9) |
| Tensions in general | "You don't have […] a direct business value if you have a particularly secure product." (I3)<br>"My hypothesis would be, […] that in a large company with regulations that have to be adhered to, this falls foul and has an influence on speed or perhaps even on the degree of innovation" (I2) |
| Temporal tensions | "Supposedly, things would move faster without cybersecurity." (I11)<br>"The trade-off that I think is happening here is between speed, so to speak how quickly you are able to offer something on and market, and absolute security." (I13) |
| Functional tensions | "[Innovation] pressure means that a lot of things are proposed that cannot be operated in a compliant manner, that cannot even be put into operation with a clear conscience." (I11)<br>Salespeople go to business stakeholders, […] brochures are distributed, and […] desires arise." (I11) |
| Economical tensions | "If I realize: 'Oops, I'll have to do a lot of re-development now, because it doesn't work the way I imagined.', then, of course, […] [cybersecurity creates additional] costs." (I14) |

| | |
|---|---|
| | "Of course, you can also go too far with cybersecurity. If you aim for a high level of cybersecurity, it must then also be maintained, and you will always need the personnel for this." (I8) |
| Integration/ Collaboration | "It depends on the project, but often these challengers […] are brought in selectively as experts." (I6) "If you often do projects like this, then of course you know when you can cleverly involve the lady in advance. […] It's always stupid if I only involve the security officer at the end of the chain." (I2) |
| (Cybersecurity) risk management in innovations | "If you require the smallest prototype to fulfill the full set of rules, then that will destroy everything. […] What we need is an appropriate approach. There are two variants. The first is the textbook approach [...] Variant two [...] I call the sandbox process." (I11) |

The interviews were conducted by telephone between 27th April and 12th June 2020. All conversations were held in German, using the interviewee's language and considering his/ her area of expertise to ensure a fluent conversation [42]. The interview partners agreed with the recording and the subsequent transcription. An attempt was made to keep the interview to around 30 minutes, as time limitations represent a central problem of expert interviews [43].

The **data analysis** was conducted according to Meuser & Nagel (1991), which is a standard for German-language studies [55]. This approach is meant to be adapted to research needs, which we did, e.g., during data preparation [42, 55]. As content-completeness was our objective, we decided to create verbatim transcripts, leaving out repetitions and fillers. The sentence structure was smoothed to improve readability. During this step, no interpretation was made, and nothing related to the research topic was left out. We did, however, not transcribe small talk. Following criticism of the initially suggested paraphrasing [55], this step was omitted. Instead, headlines were assigned to segments of each transcript using the coding function of the qualitative data analysis software MAXQDA. Data evaluation followed the steps: thematic comparison, conceptualization, and theoretical generalization [55]. During the thematic comparison, headings were clustered into topic areas to present and compare the experts' statements. The level of abstraction was further increased during conceptualization, e.g., by replacing non-scientific terms and substantiating the statements with literature. Finally, during theoretical generalization, existing theories were applied, and new theories were established. In total, about 500 segments were aggregated in 22 topic areas (see Table 2 for an excerpt).

## 4. Findings

### 4.1. Tension Recognition

Concerning the logistics industry, **digital innovation** and cybersecurity are classified as highly relevant capabilities (I1-I14). However, the industry is considered price-driven, conservative, risk-averse, and less innovative (I1-I3). Most interviewees do not feel an intense pressure to innovate (e.g., I2; I5; I12), and almost all focus on incremental innovations with small risks and cost (I1-I3; I9; I11). Pursuing digital disruptions is not seen as necessary (I2; I9). Consequently, there is an unwillingness to take risks to reach higher innovation outputs. This is, however, not true for every logistics company. Specific sectors or companies, especially start-ups (I8), are highly innovative. The interviews suggest that these either feel pressure to gain market share or have long-term strategies that force them to drive innovations (I4; I8; I12). These firms are assumed to be more strongly affected by tensions between the two capabilities. They might prioritize innovation and neglect cybersecurity for time, cost, or functional reasons (I4; I6; I8; I13).

Most companies either view **cybersecurity** as a requirement when implementing innovations or do not perceive it as a limiting factor as innovation speed is not as crucial as in other industries (I1; I3; I7; I10). The risk of creating insecure innovations is therefore considered to be low. Not every expert agrees that the supply chain of logistics firms is particularly vulnerable, as the data is often not considered interesting for attackers (I9; I14). Regulations play a significant role in prioritizing cybersecurity as they force companies to fulfill specific standards no matter the cost. Companies affected by them are mainly in the sector of critical infrastructures (I11). Such regulations can have a notable effect on the innovativeness as well as the attitude towards risk and thus cybersecurity of firms. One expert noted, for example, that without them, companies might ignore cybersecurity standards for cost and time savings at the cost of public safety (I13). However, some examples show that even without regulations, companies strive to implement high security standards. These firms view cybersecurity as a competitive advantage. They advertise their services as "best-in-class security" and thereby create value for their customers (I10; I11)

In general, innovation and cybersecurity experts' opinions on whether there is a **trade-off** between their capabilities differ. While innovators consider cybersecurity as hindering, cybersecurity professionals underline the necessity of their topic and do not perceive a trade-off (I1-I4; I6-I13). Nonetheless, all parties

describe tensions or conflicts between cybersecurity and innovation capabilities. These tensions can be categorized as: temporal, economical, functional.

The *temporal tension* arises when companies or teams strive for a high innovation speed (a low time-to-market) while cybersecurity activities require additional time (I2; I8; I13). In practice, additional steps include the preparation of risk estimates, as well as the creation, implementation, and review of security concepts (I2; I3; I14). The experts note that the subsequent implementation of these activities has an even higher chance of leading to delays (I7; I10; I11). Late discovery of insufficient cybersecurity leads to additional steps, such as re-works or further quality inspections (I7; I11).

The *economic tension* results from the motivation to keep the costs of an innovation low despite additional investments to implement cybersecurity (I2; I8). These costs arise from personnel resources (e.g., involvement of experts), know-how (e.g., sourcing of external consulting), purchase prices (e.g., higher prices of secure devices), and additional functionality (e.g., implementation of security features) (I1-I3; I8; I13). The experts highlight the importance of cost-benefit analysis (I11; I14). Some interviewees mentioned that large companies have more resources at their disposal and have more room to maneuver (I8; I13).

The *functional tension* is found when (parts of) an idea cannot be implemented because of its cybersecurity risks. The requirements for quality standards in cybersecurity make specific solutions fall out of scope (I2; I11). That means an innovation is either a) not secure enough from the beginning or b) the implementation of cybersecurity features is infeasible because it restricts the user experience or usability (I7; I11).

## 4.2. Tension salience & resolution

Concerning tension salience and resolution, triggering and resolving factors are often closely related. In many cases, the lack of a particular feature represents a trigger, while establishing said feature can resolve the tensions (see Figure 1).

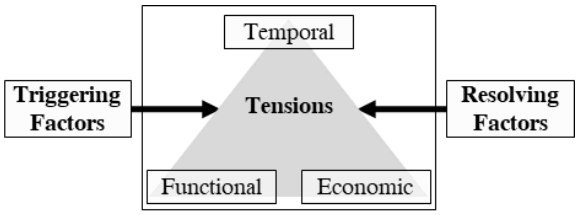


**Figure 1. Relationship between tensions, triggering and resolving factors**

Our interviewees agree that the extent to which the tensions are perceived mainly depends on the **organizational culture**. Risk-averse, rather exploiting organizations often anchor cybersecurity in the company through audit cycles and regulations (e.g., mandatory risk-analysis or cybersecurity testing). Cybersecurity is then considered a secondary condition or must-have feature for innovation (e.g., I7; I10). One expert highlights this by saying: “an innovation without cybersecurity is not considered an innovation” (I10). Such companies usually do not perceive a trade-off, as innovation is not pursued at the expense of cybersecurity. However, if managers ignore the internal policies regarding cybersecurity, the innovation process slows down notably. Costs do then increase as re-works, re-verifications, or even project delays occur (I7; I11). The bypassing of cybersecurity rules is especially documented when managers were uninformed or under pressure to meet innovation goals (I7; I10; I11). This leaves innovators with the impression that cybersecurity policies hinder their projects (I7; I11). Innovating, explorative organizations like start-ups are more willing to take risks to gain competitive advantages (I4; I8; I12). They implement less overhead to increase innovative freedom, accelerate time-to-market, and decrease costs (I8). Furthermore, even known risks might be accepted if the potential return is high enough. This usually results in more flexibility and more responsibility for the project lead, as they have to prioritize cybersecurity activities within their project and have fewer guidelines to follow (I8; I12). In this context, cybersecurity awareness is named as a countermeasure (I1; I7; I8)

According to the interviewees, the **organizational structure** influences the balance between cybersecurity and innovation. In large companies, different departments with conflicting interests usually provide the capabilities (I1-I3; I5; I7; I9; I14). While innovations are driven by various business units, the cybersecurity capability is often located in the IT department (I1; I2; I5; I7; I9; I14). However, those responsible for innovation (e.g., project managers, product owners) are usually also liable for ensuring cybersecurity (I10; I12; I14). For such situations, an alignment of team interests at the management level was mentioned (I5). Small firms, in contrast, often only have one Chief Digital Officer (CDO), Chief Technology Officer (CTO), or CIO responsible for both innovation and cybersecurity. This is caused by resource restrictions of small and medium enterprises (SMEs). According to our interviewees, this company structure leads to flexibility and speed at the cost of control orientation. (I8; I9; I13).

The **integration and collaboration** of cybersecurity and innovation capabilities are crucial in reducing tensions (I1-I3; I7; I10; I11; I14). If both collaborate closely and cybersecurity is integrated at an early project stage, this leads to a high cybersecurity maturity, in turn (I1; I2; I10; I11; I14). It can, however,

also make innovation teams perceive cybersecurity experts as "preventers" (I7; I11), attributed to a lack of creative freedom during or shortly after the "ideation phase" (I3; I6; I12). However, both parties are not opposed to this collaboration, especially if the innovation teams have essential competencies and sufficient cybersecurity awareness (I5; I10; I14). Management encouraging and promoting the integration and establishing cybersecurity experts as part of the innovation team are named success factors (I1; I5). These additional skills and resources require investments in training, recruiting new employees, or contracting externals (I1, I7; I8). The collaboration is, however, said not to be very common in practice (I1; I7; I10; I14). While our interview partners provide examples in which early, intensive collaboration has led to successful innovation projects (I1; I11; I14), the departments work separately in most cases and only collaborate selectively in the form of consulting services or audit cycles (I3; I6; I8; I14). Consequently, innovations might be developed that do not fulfill the desired cybersecurity standards (I7; I10; I11).

Furthermore, especially if no cyber breach has occurred before, managers tend to believe that investments in cybersecurity are useless (I8; I13). Cyber threats are perceived as an "invisible risk", against which complete protection is impossible (I8; I9; I11; I14). This is attributed to the assessment of risk representing a significant challenge for companies, especially before or at project start (I1; I8). The lack of knowledge or historical data often leads to their under-estimation (I8; I11). Correct assessments require specialist knowledge and are time- and resource-intensive. This can, in practice, lead to them being skipped (I7; I8). Furthermore, risk assessors might be biased, e.g., to accelerate their own innovation project, requiring control mechanisms to ensure correct results (I8). Our interviewees point out that it is crucial to also consider the business value of an innovation, as most companies would accept higher risks for higher returns (I4; I8; I9; I13; I14). Finally, these assessments must be repeated during the innovation process, as the cybersecurity risks or business value might change (I3). To counteract some of these points, it might make sense to involve externals (I8). If some precautions are considered, cybersecurity risk management can, according to our interviewees, be suitable to fine-tune the integration into the innovation process (I8; I11). Such assessments can then help determine the scope of cybersecurity: if cyber risks are high, the integration of cybersecurity is increased. If they are low, innovators get more freedom, and projects are accelerated (I11; I12; I14). This does not necessarily mean that an innovation with higher risks is subject to more security measures than an innovation with lower risks. If cybersecurity costs and the potential business value of an innovation are disproportionate, a residual risk can be accepted (I8; I11; I12 I14). Such an approach was reported to be already applied in practice sometimes (I12; I14).

## 5. Discussion

Regarding the first two research questions and propositions (P1 and P2), the literature points to a conflict between innovation and cybersecurity capabilities [5, 11, 33, 49]. However, only a minority of the interviewees perceive a trade-off between the two. In line with research, the German logistics sector was considered not to be very innovative. This could be because logistics providers do not fear displacement by radical innovations. There is a focus on incremental process innovations to increase efficiency or reduce costs [58]. Consequently, digital innovation capability is currently not seen as a decisive factor in competition. Controversial to the findings of Nelson and Madnick [44], the majority of logistics companies can thus be classified as "beginners" or "secure conservatives". The low relevance that the former attribute to the two capabilities could explain that no or only a weak trade-off is perceived. Conservative firms with a high risk-aversion attribute a higher priority to cybersecurity [14]. This could lead to a conscious reduction in innovation ability as cybersecurity is regarded as indispensable or considered a secondary condition in innovations. Such companies could potentially be significantly more innovative if tensions between innovation and cybersecurity capabilities were lower. These temporal, economic, or functional tensions are described by all interviewees. While only a few studies research such tensions in the context of innovation and cybersecurity [2, 44, 50], various studies deal with them in either the innovation or cybersecurity context [1, 10, 33, 59].

Regarding the third research question, our interviewees highlighted several triggering and resolving factors to address these tensions.

The conservative attitude and cybersecurity consciousness, which is deeply anchored in the organizational culture (P3a), is, for example, influenced by the fact that many logistics companies are under competitive pressure, deal with goods of high criticality or operate critical infrastructure [56]. However, the idea that the increasing pressure to perform can lead to a greater willingness to take risks in decision-making among managers [39] cannot be uniformly transferred to our interviews. Most of the interview partners did not feel under pressure to innovate. Those that did feared their competitors' agility and speed of innovation, especially that of start-ups. It was, however, recognized that it is under this innovation pressure that rash decisions are made. At the same time, a balance of both

topics at the management level was said to lead to higher performance. This reflects the results presented in our background [10, 41]. Factors like increased regulation often lead to a control-oriented culture that positively influences cybersecurity [15].

Concerning the organizational structure (P3b), overcoming the separation between innovation and cybersecurity capabilities by promoting collaboration through the management and establishing cybersecurity experts as part of the innovation team were mentioned. Finding the balance between exploitation and exploration was considered a question of organizational culture rather than its structure [6, 21]. This might be explained by the fact that only two interviewees felt their organization had separated explorative and exploitative units. Presumably, the gap between explorative and exploitative capabilities could therefore not be observed as an essential field of tension.

Regarding the integration and cooperation of the two capabilities (P3c), our interviewees agreed with findings that recognized the need for early consideration of cybersecurity [45, 47], e.g., through the integration of cybersecurity experts. This can prevent the innovation process from being slowed or even shut down because cybersecurity is not sufficiently considered. In line with research on innovation management, the negative perception of the cybersecurity capability this might cause was attributed to a lack of creative freedom in the "ideation phase" [11]. Cybersecurity risk management was mentioned as essential to counteract the underestimation of cyber risks and enable a risk-oriented integration. As proposed in the literature [32], assessing cyber risks before the project start was deemed challenging. It requires specialist knowledge and is time- and resource-intensive, which can lead to it being skipped. This is confirmed by research indicating that due to a lack of experience, companies tend to take a “wait-and-see approach” [29], underinvest in cybersecurity [27, 28], or accept risks [23].

From our understanding, this study makes **contributions** from both a theoretical and practical perspective. From a theoretical standpoint, we add to the relatively scarce body of research around the trade-off between digital innovation(s) and cybersecurity. We identified three different types of tensions, as well as a set of triggering and resolving factors. While taking the logistics industry as an example, our methodology and most of our findings are potentially relevant for other industries. In particular, the theoretical background, our propositions, and the interview guideline are easily adaptable and could thus be re-used. From a practical standpoint, our findings provide organizations with a list of triggering and resolving factors to be considered when trying to find a balance between digital innovation and cybersecurity capabilities. We are convinced that they are relevant, not only to logistics organizations.

We are aware that our study has certain **limitations**. Because existing research on the trade-off is limited, we chose a broad study design to ensure that all relevant aspects are captured. Despite this broad design, a study cannot simultaneously cover all perspectives like organizational ambidexterity and IT governance. We did, furthermore, decide not to consider technology-specific influencing factors. Additionally, our study is limited to the logistics industry. Since the German logistics sector is a comparatively risk-averse and innovation-weak industry, it can be assumed that the observed tensions will be more potent in other industries. In addition, the number of interviews and the choice of interview partners also represent limitations. With 14 experts, the sample size of our study is relatively small. We tried to select interview partners carefully, e.g., from different organizations and both perspectives of the trade-off. However, they might not represent the entire spectrum of the industry. Furthermore, the selected interviewees might be biased. As all interview partners were German, for example, our findings might show a cultural bias. Digital innovation, cybersecurity, and the logistics industry are developing quickly, and the fact that our interviews were conducted about 12 months ago might represent another limitation. Regarding data analysis, we tried to mitigate any bias amongst the researchers and increase credibility and validity through member checking.

## 6. Conclusion and Outlook

The role of both digital innovation and cybersecurity in the logistics industry is increasing. Due to its systemic relevance, the industry is an interesting target for hackers, and it is crucial not to introduce vulnerabilities when rushing to introduce digital innovations. While a tension between digital innovation and cybersecurity has already been identified [50], we believe that research of this tension, its recognition, salience, and resolution is in its infancy. We do therefore think that our paper is of high relevance and novelty.

Nevertheless, **further research** is required. There are additional perspectives from which the digital innovation-cybersecurity trade-off could be analyzed. Interesting examples are organizational ambidexterity theory, a socio-technical perspective on digital innovation management, IT governance in general, and the interplay of structural and normative IT governance mechanisms in specific. While it would certainly be interesting to confirm our results in other industries, e.g., selected based on digital innovation and cybersecurity characteristics, our findings must be specified and verified. From our perspective, it would

make sense to conduct focus studies on selected aspects of our findings. We do, for example, consider organizational structures and the integration of the capabilities on an operational level to be of particular interest. Furthermore, we would recommend analyzing how strongly the different factors influence the three types of tensions. Besides, the impact of different technologies should be researched. Finally, the development of approaches to balance innovation and cybersecurity capabilities seems promising. These could put cybersecurity risk management at the heart of the innovation process. This would enable organizations to fine-tune the integration and limit the tensions found.

## References


[1] Andriopoulos, C., and M.W. Lewis, "Exploitation-exploration tensions and organizational ambidexterity: Managing paradoxes of innovation", *Organization Science 20*(4), 2009, pp. 696–717.

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

[3] Barczak, A., I. Dembińska, and Ł. Marzantowicz, "Analysis of the Risk Impact of Implementing Digital Innovations for Logistics Management", *Processes 7*(11), 2019, pp. 815.

[4] Barreto, L., A. Amaral, and T. Pereira, "Industry 4.0 implications in logistics: an overview", *Procedia Manufacturing 13*, 2017, pp. 1245–1252.

[5] Berglund, H., "Risk Conception and Risk Management in Corporate Innovation: Lessons From Two Swedish Cases", *International Journal of Innovation Management 11*(04), 2007, pp. 497–513.

[6] Birkinshaw, J., and C. Gibson, "Building Ambidexterity into an Organization", *MIT Sloan Management Review 45*(4), 2004, pp. 47–55.

[7] Bitkom e.V., *Digitalisierung der Logistik*, Berlin, 2019.

[8] BlueVoyant, *Supply Chain Disruptions and Cyber Security in the Logistics Industry 2021*, 2021.

[9] 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.

[10] Borgelt, K., and I. Falk, "The leadership/management conundrum: Innovation or risk management?", *Leadership and Organization Development Journal 28*(2), 2007, pp. 122–136.

[11] Bowers, J., and A. Khorakian, "Integrating risk management in the innovation project", *European Journal of Innovation Management 17*(1), 2014, pp. 25–40.

[12] 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.

[13] Chan, C.M.L., S.Y. Teoh, A. Yeow, and G. Pan, "Agility in responding to disruptive digital innovation: Case study of an SME", *Information Systems Journal 29*(2), 2019, pp. 436–455.

[14] Chang, S.E., and C.B. Ho, "Organizational factors to the effectiveness of implementing information security management", *Industrial Management and Data Systems 106*(3), 2006, pp. 345–361.

[15] Chang, S.E., and C.S. Lin, "Exploring organizational culture for information security management", *Industrial Management and Data Systems 107*(3), 2007, pp. 438–458.

[16] Chen, Y., and D. Hua, "Do Innovators Concern Less about Security and Value New Technologies More? A Case of Mobile Commerce", *Journal of Information Technology Management 25*, 2014, pp. 13–16.

[17] Chernyakov, M., and M. Chernyakova, "Technological Risks of the Digital Economy", *Journal of Corporate Finance Research 12*(4), 2018, pp. 99–109.

[18] Chronopoulos, M., E. Panaousis, and J. Grossklags, "An Options Approach to Cybersecurity Investment", *IEEE Access 6*, 2018, pp. 12175–12186.

[19] Ciriello, R.F., A. Richter, and G. Schwabe, "Digital Innovation", *Business & Information Systems Engineering 60*(6), 2018, pp. 563–569.

[20] CISOMAG, "Mailto Ransomware Hits Toll Group, Deliveries Across Australia Affected", *Cisomag News*, 2020. https://www.cisomag.com/mailto-ransomware-hits-toll-group-deliveries-across-australia-affected/

[21] Duncan, R., "The ambidextrous organization: Designing dual structures for innovation", In R.H. Killmann, L.R. Pondy and D. Sleven, eds., *The Management of Organization*. New York: North Holland., 1976, 167–188.

[22] Elahi, E., "Risk management: The next source of competitive advantage", *Foresight 15*(2), 2013, pp. 117–131.

[23] Fan, Y., and M. Stevenson, "A review of supply chain risk management: definition, theory, and research agenda", *International Journal of Physical Distribution & Logistics Management 48*(3), 2018, pp. 205–230.

[24] Gellman, A.J., "Barriers To Innovation in the Railroad Industry", *Transportation Journal 25*(4), 1986, pp. 4–11.

[25] Georgsdottir, A.S., and I. Getz, "How Flexibility Facilitates Innovation and Ways to Manage it in Organizations", *Creativity and Innovation Management 13*(3), 2004, pp. 166–175.

[26] Gläser, J., and G. Laudel, *Experteninterviews und qualitative Inhaltsanalyse: als Instrumente rekonstruierender Untersuchungen*, VS Verlag für Sozialwissenschaften, Wiesbaden, 2009.

[27] Gordon, L.A., M. Loeb, and W. Lucyshyn, "Information Security Expenditures and Real Options: A Wait-and-See Approach", *Computer Security Journal 19*, 2003.

[28] 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.

[29] Gordon, L.A., M.P. Loeb, and T. Sohail, "A framework for using insurance for cyber-risk management", *Communications of the ACM 46*(3), 2003, pp. 81–85.

[30] Grawe, S.J., "Logistics innovation: A literature-based conceptual framework", *The International Journal of*

*Logistics Management 20*(3), 2009, pp. 360–377.
[31] Hsiao, W.H., and T.S. Chang, "Exploring the opportunity of digital voice assistants in the logistics and transportation industry", *Journal of Enterprise Information Management 32*(6), 2019, pp. 1034–1050.
[32] Hutchinson, D., H. Maddern, and J. Wells, "An agile it security model for project risk assessment", *Proceedings of the 9th Australian Information Security Management Conference*, 2011, pp. 111–123.
[33] Isaksen, S.G., and G. Ekvall, "Managing for Innovation: The Two Faces of Tension in Creative Climates", *Creativity and Innovation Management 19*(2), 2010, pp. 73–88.
[34] 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.
[35] Jeyaraj, A., and A.H. Zadeh, "Exploration and Exploitation in Organizational Cybersecurity", *Journal of Computer Information Systems*, 2021.
[36] Khansa, L., and D. Liginlal, "The influence of regulations on innovation in information security", *13th Americas Conference on Information Systems, AMCIS 2007*, 2007, pp. 449–460.
[37] Lawson, B., and D. Samson, "Developing Innovation Capability in Organisations: a Dynamic Capabilities Approach", *International Journal of Innovation Management 05*(03), 2001, pp. 377–400.
[38] Li, D., and X. Wang, "Dynamic supply chain decisions based on networked sensor data: an application in the chilled food retail chain", *International Journal of Production Research 55*(17), 2017, pp. 5127–5141.
[39] March, J.G., and Z. Shapira, "Managerial perspectives on risk and risk taking: The Definition of Risk", *Management Science 33*(11), 1987, pp. 1404–1418.
[40] Martin, N., C. Matt, C. Niebel, and K. Blind, "How Data Protection Regulation Affects Startup Innovation", *Information Systems Frontiers 21*(6), 2019, pp. 1307–1324.
[41] McFadzean, E., J.N. Ezingeard, and D. Birchall, "Perception of risk and the strategic impact of existing IT on information security strategy at board level", *Online Information Review 31*(5), 2007, pp. 622–660.
[42] Meuser, M., and U. Nagel, "ExpertInneninterviews - vielfach erprobt, wenig bedacht: ein Beitrag zur qualitativen Methodendiskussion", In D. Garz and K. Kraimer, eds., *Qualitativ-empirische Sozialforschung: Konzepte, Methoden, Analysen*. Westdeutscher Verlag, Opladen, 1991, 441–471.
[43] Myers, M.D., and M. Newman, "The qualitative interview in IS research: Examining the craft", *Information and Organization 17*(1), 2007, pp. 2–26.
[44] Nelson, N., and S. Madnick, "Studying the Tension Between Digital Innovation and Cybersecurity", *23rd Americas Conference on Information Systems*, 2017.
[45] 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.
[46] du Plessis, M., "The role of knowledge management in innovation", *Journal of Knowledge Management 11*(4), 2007, pp. 20–29.
[47] Presley, S.S., J.P. Landry, and J. Shropshire, "Cybersecurity threats in the context of project meta-phases", *24th Americas Conference on Information Systems, AMCIS 2018*, 2018, pp. 1–10.
[48] Richey, R.G., S.E. Genchev, and P.J. Daugherty, "The role of resource commitment and innovation in reverse logistics performance", *International Journal of Physical Distribution and Logistics Management 35*(4), 2005, pp. 233–257.
[49] Rosenbusch, N., J. Brinckmann, and A. Bausch, "Is innovation always beneficial? A meta-analysis of the relationship between innovation and performance in SMEs", *Journal of Business Venturing 26*(4), 2011, pp. 441–457.
[50] Schinagl, S., S. Khapova, and A. Shahim, "Tensions that Hinder the Implementation of Digital Security Governance", In A. Jøsang, L. Futcher and J. Hagen, eds., *ICT Systems Security and Privacy Protection*. Springer International Publishing, 2021, 430–445.
[51] Schöne, B., and P. Schmitz, "Hacker übernehmen Raffinerien und Hochregallager", *Security Insider*, 2019. https://www.security-insider.de/hacker-uebernehmen-raffinerien-und-hochregallager-a-822092/
[52] Sollins, K.R., "IoT big data security and privacy versus innovation", *IEEE Internet of Things Journal 6*(2), 2019, pp. 1628–1635.
[53] Von Solms, R., and J. Van Niekerk, "From information security to cyber security", *Computers & Security 38*, 2013, pp. 97–102.
[54] The Open Group, *TOGAF® Version 9.1*, van Haren Publishing, 2011.
[55] Ullrich, P., "Das explorative ExpertInneninterview: Modifikationen und konkrete Umsetzung der Auswertung von ExpertInneninterviews nach Meuser/Nagel", In T. Teubl, ed., *Die Transformation des Politischen: Analysen, Deutungen und Perspektiven*. Dietz, Berlin, 2006, 100–109.
[56] Urciuoli, L., T. Männistö, J. Hintsa, and T. Khan, "Supply Chain Cyber Security – Potential Threats", *Information & Security: An International Journal 29*, 2013, pp. 51–68.
[57] Vasiu, I., and L. Vasiu, "Cybersecurity as an Essential Sustainable Economic Development Factor", *European Journal of Sustainable Development 7*(4), 2018.
[58] Wagner, S.M., "Innovation Management in the German Transportation Industry", *Journal of Business Logistics 29*(2), 2008, pp. 215–231.
[59] Weimer, M., and L. Marin, "The role of law in managing the tension between risk and innovation: Introduction to the special issue on regulating new and emerging technologies", *European Journal of Risk Regulation 7*(3), 2016, pp. 469–474.
[60] World Economic Forum; Accenture, "Digital Transformation of Industries: Digital Consumption", (January), 2016, pp. 34.