systems

MDPI

Article

Information Security Risk Framework for Digital Transformation Technologies

Eduardo Stefani *,†, Ivanir Costa †, Marcos Antonio Gaspar †, Roberto de Souza Goes †, Rogerio Carlos Monteiro †, Breno Ribeiro Petrili † and Alexandre de Paula Pereira †

Information Technology and Knowledge Management Graduate School (PPGI), University Nove de Julho, São Paulo 03155-000, Brazil; ivanirc@uni9.pro.br (I.C.); marcos.antonio@uni9.pro.br (M.A.G.); roberto.goes@uni9.edu.br (R.d.S.G.); rogeriomonteiro@uni9.edu.br (R.C.M.); breno.petrili@uni9.edu.br (B.R.P.); alexandrepereira@uni9.edu.br (A.d.P.P.)

* Correspondence: eduardo_stefani@uni9.edu.br

† These authors contributed equally to this work.

Abstract: The increasing impact of digital technologies on society is marked by rapid and disruptive changes, including more efficient and modern processes, and is pushing companies to adopt digital solutions. However, companies have limited options, and can rarely avoid being affected by the speed and challenges introduced by digital technologies. Researchers have observed that, despite the advantages they bring, the cybersecurity risks associated with these technologies are not fully apparent. In this context, the present study aims to uncover the risks associated with using digital transformation technologies, which may lead to outcomes that fall short of initial expectations. As the research methodology, a systematic literature review was conducted involving a search for scientific articles in bibliographic databases in order to identify, organize, and classify these risks. This review offered visibility into the risks companies face when adopting digital technologies and provided a framework that highlights the most relevant risks. IT specialists validated these risks through a consistent questionnaire followed by application of the Cronbach's alpha coefficient applied, aligning our systematic literature review with market realities regarding the risks that companies are exposed to when using digital technologies. As a contribution to both industry and academia, this work offers a framework that can support companies in their digital transformation journey by helping them to recognize and manage the cybersecurity risks associated with digital technologies. Future studies could expand on this framework by developing a model for risk prioritization and mitigation.

Keywords: digital transformation; digital technology; risk; risk identification; risk classification; Cronbach's alpha

check for updates

Academic Editor: Gandolfo Dominici

Received: 31 October 2024
Revised: 17 December 2024
Accepted: 30 December 2024
Published: 6 January 2025

Citation: Stefani, E.; Costa, I.; Gaspar, M.A.; Goes, R.d.S.; Monteiro, R.C.; Petrili, B.R.; Pereira, A.d.P. Information Security Risk Framework for Digital Transformation Technologies. *Systems* **2025**, *13*, 37. https://doi.org/10.3390/systems13010037

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Digital technologies, which represent the combination and connectivity of a dispersed volume of information, communication, and computing technologies [1], have begun to have an increasing impact on people's lives, businesses, and companies [2]. Their evolution has resulted in business models based on digital platforms, which has affected how companies are structured and how their management is conducted [3]. This includes changes in companies' behavior, pushing them in ways such that they are rarely able to shield themselves from the growing competition and challenges brought about by digital technologies [4].

Digital transformation (DT) is a process that encompasses the digitalization of companies, including products, services, and the creation of value through the implementation of various

technologies [5], and has resulted in a landscape of changes such as the evolution of information technologies, pursuit of efficient processes, and modernization [6]. DT has become a critical component for the success and survival of companies, as it allows for the identification and creation of opportunities to strengthen their competitive advantages [7].

Although this topic has been of growing interest to both academia and the market [8], a unified understanding of what DT is and what it means is still lacking [9]. According to the literature, it can be defined as a process that enhances a specific entity, triggering many changes through information, computing, communication, and connectivity [6]. DT can also be understood as an organizational change triggered by the diffusion of digital technologies [8].

Digital technologies are transforming the way companies and markets interact [10,11]. As these technologies become present in all areas, companies are assigning executives to lead their digital agendas and emphasize the importance that digital technologies play in the current context. Companies are also faced with the need to use these technologies efficiently as possible [2], given that they are widespread and playing an increasingly important role in people's lives [12]. Digital technologies are used to enhance the performance and capabilities of a user, system, or process [13]. They are employed to enable connectivity between components as well as to search for information, transform, and store data. In the context of the mutual integration and optimization of digital technologies, this makes the production, processing, and customization of products simpler and more convenient [14].

Among the technologies that impact the DT process, the Internet of Things (IoT), big data and analytics, artificial intelligence (AI), cloud computing, cyber–physical systems, and 3D printing are the most relevant today [15]. There is no specific and static set of DT technologies; they vary according to a company business and the technological availability at a given historical moment or specific location.

The challenge is how companies manage the increasing speed and risks imposed by new and disruptive technologies [6], as traditional business models are rapidly losing their competitiveness and being replaced by innovative models that drive and embrace digital transformation [16].

This also involves considering the effect that the use of digital technologies has on society, which is facing a viral disruption that challenges the notion of prosperity at any cost as well as the foundations of trust in institutions and a better future [17].

Risk can be understood as the possibility of an event having unexpected outcomes, the uncertainty of the unknown, or how its effects are perceived [18]. It is the probability of a variation from an expected result [19]. Additionally, companies are exposed to risks that may cause unexpected disruptions due to strikes, natural disasters, or supplier failures [20]. By increasing complexity, DT has elevated this topic to a new level, bringing with it the introduction of systemic and structural risks [21].

This research highlights the fact that no sector or area of companies is exempt from the effects of DT, which has become a response to the pressures of the digital economy, earning the status of a strategic priority [22].

Several facts corroborate this sense of urgency regarding the risks associated with the use of DT technologies. By around 2025, the data generated by IoT devices is expected to reach approximately 73 zettabytes, up from 18 zettabytes in 2019, with a large portion of these data coming from video. Industrial IoT applications will represent a significant share of these data [23].

Modern privacy laws will cover 75% of the global population, and by 2025 60% of companies will use some form of security risk criteria as a determinant for conducting business with third parties. Furthermore, by the end of 2025, there will be a 30% increase in nations enacting legislation to regulate payments related to ransomware attacks [24].

Thus, the development and validation of an information security risk framework, including the identification and classification of risks inherent to DT technologies, is a relevant factor for companies and the objective of this work. It is also worth noting that the world is witnessing a transition from an industrial society to an information society, with technologies imposing challenges that require effective and high-quality solutions [21].

2. Research Background

This section presents the theoretical platform supporting the development of this work, outlining the concepts related to digital transformation, its technologies, and the risks associated with the use of them.

2.1. Digital Transformation (DT)

DT has become a focus of attention in both the corporate and worlds, but it remains challenging to provide a clear, precise, and unified definition [9]. A significant part of the difficulty in reaching an exact meaning for this topic is the fact that DT has a multidisciplinary perspective [25]. An important characteristic of DT is the integrated use of technologies that reach and impact internal processes within companies and have the particularity of affecting societies and people [26].

In this perspective, the human component is an aspect of DT in terms of both means and objectives [25]. The integrated use of these digital technologies changes the way individuals work, and has the ultimate goal of improving the material conditions of society [26].

Based on interviews with executives, there is confusion in defining the term "digital" because it is something that is quite saturated and can have various meanings [2]. Furthermore, according to these authors, although there are definitions that emphasize technology itself, transformative aspects, strategies, and business models have also been incorporated into this term.

The multidisciplinary perspective of DT takes society's point of view into account [17]. In this way, the opportunities that come with this revolution are important, but are accompanied by risks that directly affect people. DT is described as the use of technologies to radically improve companies and rethink how they utilize this resource, as well as people and processes, to change business performance [27].

In light of the concepts and definitions presented above, it is evident that DT does not have a unified meaning. Perspectives differ according to the authors and their fields of study, but all are able to formulate their own definition for this phenomenon that is revolutionizing societies.

2.2. Digital Transformation Technologies

The innovation behind DT has been identified as the combination of information, computing, communication, and connectivity technologies [1,6]. As many of the technologies directly linked to DT are not new [25], the evolutionary process that has occurred in recent decades, starting from informatics to the information society, has paved the way for an event as impactful as DT [28].

As an example, it is possible to list some of the implicated technologies, such as the IoT, cloud computing, big data, cyber–physical systems, virtual and augmented reality, and AI [29]. AI in particular, poses challenges, as its ultimate goal is the creation of an algorithm capable of solving problems and performing cognitive tasks equally well or better than humans [27].

The roboticization of processes is another technology that deserves attention; it does not replace AI or machine learning, but is capable of performing automatic and repetitive tasks such as data mining [30].

Regarding cloud technology, other mechanisms such as the IoT store data and rely on the cloud to achieve the integration promised by DT, which permeates both citizens and companies [31].

As can be observed, the universe of available technologies is very broad, which is why a static definition would be somewhat incomplete. It is important to note that the technologies that cause concern today will be fully integrated into the lives of citizens and companies within a few years, and no longer represent a threat. Likewise, the hypothetical risks associated with technologies such as AI, which may present potential threats to humanity in the coming years, are similar to the innovations and risks of past technologies that are now fully integrated into society [21].

2.3. Risks Associated with the Use of Digital Technologies

Digital technologies have become a requirement for companies to gain competitive advantages [7]. On the other hand, despite the gains from DT, researchers are beginning to discuss the negative effects of digitalization [25]. In this context, the effort here is to relate the use of digital technologies to the inherent risks of this process. Although the benefits are significant, it is impossible to ignore the associated risks.

Risk has always accompanied humanity, necessitating some way of managing it [17]. Regarding DT, it brings systemic and structural risks, for instance, to economic security stemming from dependence on technologies from other countries and the lack of foundational elements needed to build them [21]. The integration of this process with third-party technologies presents a source of danger [32]. This increases cybersecurity risks and their complexity, as a vulnerabilities may be linked precisely to an external element; this type of dependency was identified by the European Parliament in 2019. Today, the world is globalized, with societies deeply integrated. In this scenario, technologies add a level of speed that imposes a significant challenge, as it is necessary to improve people's conditions and reinforce expectations for a better future [17].

AI can bring with it risks and challenges that are difficult to calculate, which may cause unprecedented uncertainties [21]. In short, this involves the difficulty of clearly predicting the risks involved in the use of AI across various sectors of society. While drastic scenarios can be envisioned, such as the loss of control over military systems, there are also simpler horizons that include the challenge of establishing laws and regulations for the proper use of such technologies without creating risk.

DT has added a new layer of cyber-related risk which can experience a cascade effect from natural events such as disasters, which may trigger unexpected impacts on the infrastructure supporting digital technologies [32]. For example, a prolonged power outage can directly affect the continuity of data centers.

The possibility of cascading effects introduces a term previously reserved for the literature on cyberwarfare and cyberterrorism. This term refers to critical infrastructure, which represents systems and assets that can be either physical or virtual. If they are destroyed or compromised, they can cause a debilitating impact on national security, economic security, public health, or all of these combined [33]. It is important to highlight that cyberspace is part of critical infrastructure, which can be defined as the computers, servers, routers, and cables that enable its functioning [34].

It is possible to list some items that provide a more domestic dimension of critical infrastructure, such as energy, food, transportation, the banking system, and communication [35]. Ports are an integral part of this infrastructure due to a global supply chain that includes integration with transportation, energy, and telecommunications networks [36]. IoT and the management of the large amount of data available in the cloud create significant dependence on critical infrastructure [36]. As the cloud hosts an increasing volume of data,

including sensitive data, concerns about potential cyberattacks targeting these data are also rising [31].

In this way, it is possible to observe that while the above examples cover industries of different natures, they include common points such as the pursuit of competitiveness and DT, the latter being the means through which companies are working to achieve this goal. Risk arises when sensitive areas affected by DT experience an unexpected event, which could be a disaster or even a human action intended to cause harm [32].

The intensive use of digital technologies can increase human risk and social vulnerability [37]. This involves recognizing that countries, companies, and citizens are not equal. According to [37], not all human beings are connected to the internet, as this depends on telecommunications infrastructure, income, and the location. This results in digital inequalities or different forms of equality. This perspective is relevant for citizens and companies in less developed regions, which face pressure to adopt and implement DT but are not on an equal level with more developed ones at the starting point. This social vulnerability can marginalize entire regions or companies, making it very difficult for them to keep pace with the adoption of advanced technologies, thereby creating what is known as a digital divide [37].

Risk may exist in the process of concentrating digital platforms and the high investment in innovation, such as in cloud computing, that these industries require. However, only companies that reach a certain level of market power are able to afford the significant investment needed for the innovation of digital platforms. This market power and concentration can hinder the entry of new participants and ultimately harm the entire system [38].

3. Systematic Literature Review

To allow for unbiased data collection in a situation where the results are unpredictable [39], this work is structured in the manner of a systematic literature review conducted through searches in the bibliographic databases Web of Science and SCOPUS. These searches provide the theoretical foundation of our research, consisting of the state-of-the-art on the risks that use of DT technologies brings to companies. It is structured following the PRISMA (Preferred Reporting Items for Systematic Review and Meta-Analysis) method [40], which divides the research process into the following steps: identification, screening, eligibility, and inclusion. To ensure that all analyzed material is consistent and minimizes subjective perspectives, the eligibility step include inclusion and exclusion criteria [41]. These criteria provide an objective way of determining whether the materials resulting from the searches are relevant to the central theme of the research, and situate the present study within ongoing discussions in the existing literature.

3.1. Searches in the Bibliographic Databases

A systematic literature review was conducted by searching for scientific publications in the Web of Science and SCOPUS bibliographic databases. Table 1 presents the terms used in the search expression.

Table 1. Search expression.

Expression
"digital transformation" AND (risk* OR privacy OR breach* OR leak* OR mitigati* OR security)

The search terms were adjusted to provide research involving DT along with the risk of digital technologies; therefore, the term "risks" is mandatory. Words such as privacy, breach, leakage, mitigation, and security expand the search, as they are related to risks.

It is worth noting that the term "digital technologies" does not appear in the expression, as it was observed that searching for DT automatically includes the concept of digital technologies.

3.2. Inclusion and Exclusion Criteria

Based on the raw results obtained with the search expression in the aforementioned databases, the inclusion and exclusion criteria were applied to the publications [41]. Table A1 in the Appendix A presents the inclusion and exclusion criteria along with comments.

Two principles guided the literature review in this study:

- Objective review: Each collected work was reviewed to determine its inclusion or exclusion. The abstract and keywords were initially analyzed to objectively verify whether the work met the established criteria.
- Data collection with evidence: When a work met the established criteria, relevant data were captured, including notes to support important statements and elements.

3.3. PRISMA Method

Our systematic literature review using the PRISMA method resulted in the sample presented in Figure 1.

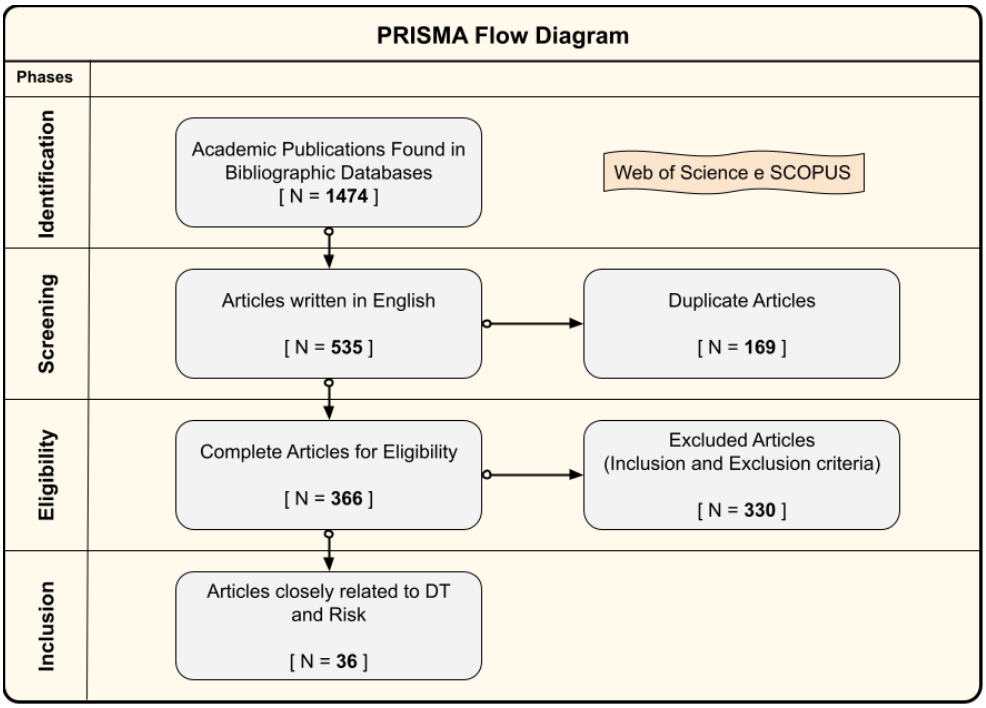

Figure 1. PRISMA flow diagram.

4. Results

This work is exploratory and qualitative, as it validates the risks involved in the use of digital technologies in companies through a systematic literature review which supports the creation of a framework. A questionnaire was applied as a research instrument for data collection. The quantitative perspective of this work is the validation of the framework through the Likert scale in the questionnaire. The Table A5 presents the Likert scale answered by all respondents.

The result of this work is the construction of a validated risk framework inherent to the use of digital technologies. This can enable companies to implement protection and cybersecurity strategies.

4.1. Risk Identification

The systematic literature review undertaken in the course of this work allowed for the identification of risks associated with the use of digital technologies. While it is known that these risks exist, our literature review enabled the selection of risks connected to reality. Such risks are also a concern for other researchers, who, although optimistic about the ongoing technological revolution, are beginning to pay attention to the negative effects of this rapid change [25].

The inclusion and exclusion criteria (Table A1) of the PRISMA method selected 36 (thirty-six) academic articles that were entirely related, meaning that the research efforts could be directly dedicated to risks of digital technologies. Twenty-one (21) risks were identified as being associated with the use of digital technologies, which can be found listed and sorted by number of occurrences in Table A2 of the appendices.

The risks, starting from the Identification column, are classified by letters ranging from "a" to "u," covering the 21 (twenty-one) risks observed in the systematic review. This classification assists in the reading of Table A3, which relates the risks and their respective authors.

In light of the identified risks, and to select the most relevant ones, a Curve ABC was applied, which is widely used in companies to classify information from various sources [42]. This tool is important because some of the identified risks have a low number of occurrences in the reviewed articles, indicating that they are of low relevance; on the other hand, others are frequently cited and deserve a more in-depth analysis. To differentiate these, the classification was as follows: the most relevant items were categorized as A, those of medium importance as B, and finally those of low importance as C. It is worth noting that the ABC classification concept is used in various applications involving both professional and personal perspectives [43].

One important aspect of the ABC curve is that the percentages for classification do not follow a fixed mathematical rule for all cases, with different cutoff values for each categorization range (A, B, and C) [44]. Additionally, given this lack of uniformity and the absence of references on the topic in the literature, the following classification criterion was used: 70% of the citations made up the A items, 17% made up the B items, and finally 9% made up the C items [44].

Table A4 presents the classification of the most cited risks, leading to a result in which the eight most relevant risks, classified as A, represented 70% of the 82 (eighty-two) total citations in the academic articles researched and selected for this review.

4.2. Top Eight Critical Risks

The following were found to be the most relevant information security risks arising from the use of digital transformation technologies:

a. **Privacy Leakage:** The preservation of privacy has become an antithesis to the idea of a digital era. Whether through the use of smart devices, consumption of digital services, or even visiting different places, data on users' activities, habits, and preferences are being collected on an unprecedented scale. However, privacy is a fundamental human right, and is also considered a side-effect of various personalized and monetized services offered to people [45].

b. **Malware:** This is the main tool used by cybercriminals to attack digital systems. Malware consists of malicious computer programs such as viruses, worms, trojans, backdoors, and rootkits [46].

c. **Ransomware:** The connected world provides new opportunities for cybercriminals to collect personal data for fraudulent transactions or to introduce ransomware, the latter consisting of malicious computer programs that lock or encrypt devices. Cybercriminals can use ransomware to demand money in exchange for the decryption key [47].

d. **Information Leakage:** This refers to the uncontrolled dissemination of information outside a company, beyond physical or territorial boundaries, or outside a circle of people who have access to the information [21].
e. **Data Theft/Manipulation:** When a user stores sensitive data stored in a cloud solution consisting of multiple servers, an attacker may act to gain unauthorized access to their information, such as by stealing, destroying, or corrupting it in a way that renders it unusable by the user [48].
f. **Unauthorized Access:** In a bank account, only the account holder or a bank employee assisting the owner with specific transactions should access it; no one else should have access. When such information is accessed by others, data confidentiality is irreversibly compromised [31].
g. **Phishing:** Various definitions of the term "phishing" have been proposed and discussed by specialists, researchers, and institutions. Although no definitive meaning exists due to its constant evolution, this term has been defined in various ways depending on usage and context. In general, it involves an attacker impersonating a recipient in order to achieve a desired action [49], such as by sending electronic messages to specific targets.
h. **Information Disclosure:** This consists of joint action between platforms, providers, and consumers to reveal information about users, products, and services through a digital platform [50].

5. Proposed Framework

Based on the selection criteria adopted for the purposes of this work, the framework is composed of the risks deemed to be most relevant and classified as such by the ABC curve. Figure 2 presents the proposed framework.

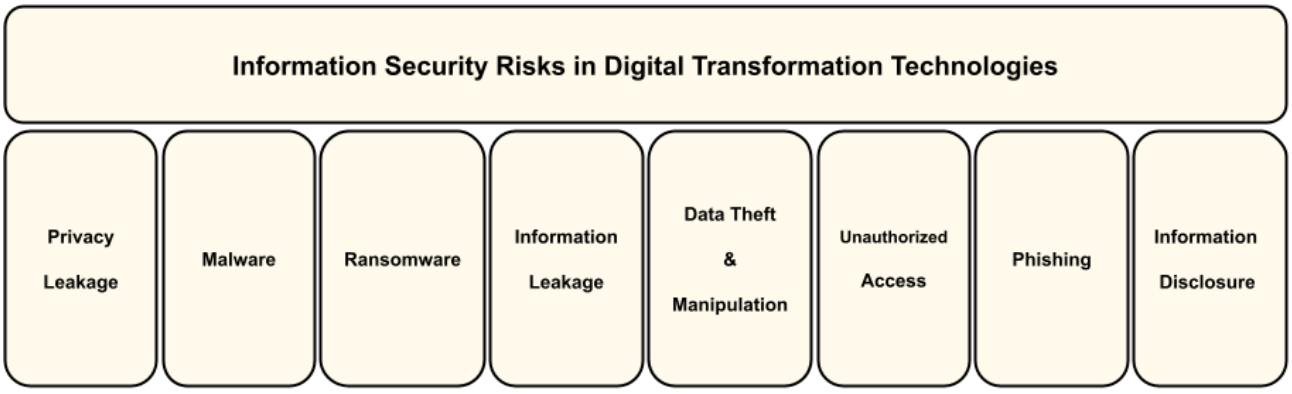

Figure 2. Graphical representation of the proposed framework.

6. Framework Validation

This section presents a review of the responses to each statement in the questionnaire and validates the risk framework based on the results from the Likert scale. Appendix C provides details of the responses along with charts illustrating each respondent's choices. These answers are valuable, as they reflect the specialists' perceptions of the subject. It is worth noting that the risk framework was constructed from a systematic literature review. Validation by specialists ensures the framework aligns with market realities by incorporating their insights on the risks associated with the use of digital technologies. This validation facilitates a mutual contribution from both academia and the market. On one hand, academia contributes through a systematic literature review that identifies and classifies the most relevant risks; on the other, market specialists offer insights into the

applicability of these risks within real-world business contexts, validating our framework as a resource for companies navigating the digital transformation journey.

While the systematic literature review enables the construction of a framework based on the risks identified in the selected articles, the questionnaire serves as a key instrument to validate the risks inherent in the use of digital technologies in DT. A study on competitiveness developed a questionnaire that incorporates dimensions and statements to measure the maturity level based on responses ranging from nonexistent to fully present maturity [51]. Similarly, the questionnaire in this research addresses the eight (8) risks identified in the literature review, with four statements for each risk.

The questionnaire went through two phases. The first was a pilot phase aimed at validation and approval based on the feedback of IT specialists regarding the risks, statements, and Likert scale. The final questionnaire was then made available to thirty-five (35) IT specialists, who evaluated each statement using the Likert scale and provided their perceptions of the risks.

The IT specialists came from the areas of research and development, product development, IT services, engineering, and global support and sales, and their positions included CEO, VP, Head of IT, IT Manager, IT Director, Researcher, IT Architect, and Solution Engineer. It is important to highlight they brought perspectives from different countries, including Brazil, Argentina, the United States of America, India, the Czech Republic, Switzerland and Portugal.

The questionnaire provided raw data enabling us to identify the number of respondents who selected a specific scale for each statement, such as how many chose "Agree" or "Disagree." From these data, it was possible to determine the percentage of responses for each statement. After obtaining these numbers, the next step was to determine which responses indicated the framework's alignment with market realities. The research criterion assumed that "Agree" and "Strongly Agree" indicated this alignment; thus, these two scales were measured. This process yielded two results enabling conditions for analysis. The simple average of each response was chosen, summing the percentages of each scale and calculating the simple average. When there was a set of raw data presented in tables or graphs, we summed the values and divided by the number of data points to define a simple average [52].

Additionally, the Cronbach's alpha coefficient was applied to the questionnaire results to verify their consistency. This coefficient serves as an estimator of test reliability, and is particularly well-suited for single applications of a test, such as within cross-sectional research designs. For a test comprising a number of items, Cronbach's alpha operates under the assumption that all items function as equivalent test units, then estimates the reliability of the complete test by conceptually extending the properties of a single unit across the items. This approach is analogous to the split-halves reliability method, in which the correlation between two halves of a test is used to infer the reliability of the entire instrument [53].

Table A6 in the appendices presents the results, with a Cronbach's alpha of 0.918. Further details about the results can be found in Tables A7 and A8. This is an excellent result; according to Table A7 and the appendices, the results indicate that the questionnaire is both robust and consistent, thereby corroborating the reliability of the statistical perspective of this research.

There are two averages, as the same operation was performed for "Agree" and "Strongly Agree." With these two averages, it can be assumed that the final average for validation is the sum of the averages of these two scales. According to criterion used in this work, if the final average (the result of adding the two averages) is above 70%, then the risk is considered relevant by the specialists.

Graphs were generated for each risk, with colors representing the number of respondents choosing one of the options for each statement related to the risk. These were then converted to percentages in order to calculate the averages for quantitative discussion. It is important

to note that the graphs include a bottom legend indicating the number of respondents and a top legend that displays the total agreement in percentage terms. These legends facilitate understanding by clearly relating the respondent count to the corresponding percentage of agreement. Graphs are presented for each of the risks discussed in this framework validation.

7. Discussion

This section presents an analysis and thoughts on the comments made by the IT specialists we consulted regarding the risks outlined in the questionnaire. We included an open-ended question that allowed them to share their insights on the topic based on their experience in the IT field. The following discussion is divided by each risk for clarity and ease of reading.

7.1. Privacy Leakage

Privacy has gained prominence with the advancement of data protection laws, but there are differing views on its impact on technology adoption. Some respondents highlighted the issue that concerns about privacy are limited, arising only when data are misused, while others argued that although regulations mandate the proper use of data, they do not hinder the adoption of new technologies. Additionally, some emphasized that processes are undervalued compared to technologies when it comes to ensuring privacy. Cases such as Cambridge Analytica and Facebook were cited as examples of the use of personal data to manipulate collective behaviors. Lastly, it was observed that the rapid adoption of new technologies often occurs prior to fully understanding their impacts on privacy, a situation worsened by the fast pace of technological innovation compared to regulatory developments.

7.2. Malware

Malware was addressed as a risk that transcends information security, bringing implications for governments and companies, especially in contexts involving importing equipment with embedded software. Respondents highlighted different perspectives, including malware as a tactical weapon in conflicts and competitions, the possibility of cyber catastrophes due to system integration, and the decentralization of systems, which despite reducing risks may be countered by increased integration. Additionally, they emphasized the importance of human training and security processes, although increasingly autonomous and integrated systems heighten the challenges. These scenarios explore strategic uses of malware and reveal vulnerabilities that expand global risks.

7.3. Ransomware

Ransomware attacks have gained prominence due to media coverage after affecting companies and government agencies. These attacks have impacts that go beyond information security, including anonymity in financial transactions and the use of cryptocurrencies. Respondents highlighted that in addition to financial damage, these can attacks generate social effects (as in the case of the ransomware attack targeting Brazil's Ministry of Health [54]), compromise the reputation and trust in companies, and impact their market position. This particular attack occurred during a critical moment when the nation was already deeply affected by the COVID-19 pandemic. When health systems are compromised, the population faces direct consequences. This serves as a clear example of how such attacks can jeopardize national security and escalate to other layers of a country's infrastructure. The vulnerability of the public sector compared to the private sector is identified as a risk to system integration, potentially leading to cyber catastrophes due to the lack of uniformity in investments and prevention among interdependent parties.

7.4. Information Leakage

The topic of information leaks is discussed, differentiating it from privacy invasion and highlighting causes such as poor practices and negligence. Respondents offer varied perspectives, with some pointing to tolerance of improper data usage in exchange for technological benefits and others emphasizing the importance of data protection legislation and technological lag in the public sector. Data security in cloud and on-premises environments was also analyzed, considering the complexity and responsibilities of each model. Additionally, the impact of AI on personalization and potential leaks was debated, along with the challenges faced by small businesses in implementing security policies. The central idea underscores that in addition to technology, well-executed processes are crucial to minimizing risks.

7.5. Data Theft/Manipulation

The respondents highlighted that data theft and manipulation are primarily motivated by economic gain, considering the legitimate value of data as a determining factor for attacks (according to Respondents 3, 14, and 30). This perspective reinforces the need to prioritize information security, with more robust layers for critical data. Respondent 4 observed that group data have greater strategic impact, especially in contexts such as elections, as they can be used to predict collective behaviors. Respondent 10 pointed out that data available on the internet make theft unnecessary, highlighting the connection with data leaks. Finally, Respondent 23 mentioned the vulnerability of internet-connected devices due to security flaws in embedded software, which can be exploited by cybercriminals.

7.6. Unauthorized Access

According to the respondents, unauthorized access, is strongly associated with the human factor and social engineering, which can simulate normal behaviors, making detection challenging even with investments in prevention technologies. Respondent 26 pointed out that a significant portion of access occurs internally within companies, while Respondent 30 highlighted the importance of training and awareness to strengthen information security. Respondent 27 mentioned Brazilian banks as a reference in access control, despite their continued investments in new technologies, a point that was corroborated by Respondent 16, who emphasized the efficiency of controls in the financial sector even with digitalization and the use of cloud computing. Finally, Respondent 3 underscored that unauthorized access is an old practice and that the human aspect is crucial to its success, including the use of social engineering techniques to access sensitive data and infrastructures.

7.7. Phishing

Phishing attacks are widely used by criminals and exploit user vulnerabilities, which many respondents noted are often considered the weakest link in security. These attacks serve as an entry point for more robust threats such as malware and ransomware, and are carried out not only through email but also via mobile device messages, messaging apps, and social media. Strategies include fake profiles and deceptive advertisements. Additionally, phishing exploits the social vulnerability of specific groups, such as beneficiaries of assistance programs or government campaigns. Despite this, training and random tests have increased awareness and reduced the effectiveness of such attacks, although even experienced users still struggle to identify malicious messages.

7.8. Information Disclosure

Information disclosure involves the conscious sharing of data by users, but presents risks when this information is misused. While Respondent 3 warned that disclosure agreements may benefit some but not all, and that confidentiality does not guarantee

security, Respondent 7 expressed the belief the practice is not harmful so long as it adheres to data protection laws. On the other hand, Respondent 8 highlighted discomfort with targeted advertising based on recent searches, emphasizing the need for transparency in complex privacy agreements. Respondent 16 pointed out that consumer preferences and behaviors are exploited without full consent to serve in collective profile analysis. Meanwhile, Respondent 25 did not oppose the use of data for product suggestions, but criticized the effectiveness and ease of manipulation of personal data and cookies.

8. Guidelines for Implementing the Risk Framework

The objective is to help companies assess their current state in terms of risk management and to enable strategies for reducing and mitigating risks in the event of security incidents. The guidelines presented here are an adaptation of the Sendai Framework for Disaster Risk Reduction 2015–2030 [55] developed by the United Nations Office for Disaster Risk Reduction. This framework addresses perspectives such as disaster risk management, governance, the private sector, and risk identification and assessment, providing support for developing strategies based on identified and classified risks.

It is important to highlight that the guidelines for implementing the risk framework encompass all the risks identified and classified in this study. This comprehensive coverage is made possible by the broad scope of the guidelines, which direct companies on how risks can be effectively managed. The guidelines extend to suppliers, partners, and customers, facilitating adherence to a wide range of digital technologies that involve the risks discussed in this study.

8.1. Guideline 1: Understanding Risk Identification and Classification

To strengthen risk management, it is crucial to promote the collection, analysis, management, and use of relevant data on identified risks and to ensure its dissemination while considering the needs of various user categories and systems. Encouraging the use of statistical data on security events is essential for assessing the risk of new occurrences, including dimensions such as vulnerability, capacity, and exposure of people and systems as well as their potential impacts on suppliers, partners, and customers. Regularly developing and disseminating risk information to decision-makers, such as risk maps and exposure levels in accessible formats for stakeholders, is another key element. Additionally, assessing, recording, and sharing losses from security events can enhance the understanding of their impacts on suppliers, partners, and customers in the context of exposure to vulnerabilities.

Ensuring real-time access to reliable data is fundamental to improving tools for collecting, analyzing, and disseminating such data. Moreover, fostering the exchange of experiences among suppliers, partners, and customers is vital for sharing lessons learned, best practices, and training resources for risk management. Leveraging existing education and training mechanisms can further facilitate this exchange. Strengthening dialogue and cooperation between the business and scientific communities, stakeholders, and decision-makers also supports more effective risk management actions.

Finally, it is important to enhance technical expertise in order to consolidate existing knowledge while promoting long-term investment in innovation and technology. Incorporating risk management knowledge into both formal and informal education is essential as a way of covering such different areas as event prevention, mitigation, preparation, response, recovery, and rehabilitation. This integration helps stakeholders to build a robust foundation for effectively and sustainably managing risks.

8.2. Guideline 2: Strengthening Risk Management

To ensure efficient risk management, it is essential to adopt and implement clear strategies and plans with well-defined objectives, measurable indicators, and established

deadlines. Additionally, a comprehensive assessment of the technical, financial, administrative, and managerial capacities of stakeholders is necessary in order to prepare them to address risks at all levels. It is equally important to encourage the creation of mechanisms that ensure compliance with laws and regulations, especially regarding data protection, in order to promote a targeted approach to risk management.

Periodic monitoring and evaluation of plans should be reinforced by appropriate mechanisms, with transparent reports and internal discussions about the effectiveness of actions. To this end, it is crucial to assign clear responsibilities to stakeholders and establish collaborative consultation and decision-making processes. Encouraging coordination among suppliers, partners, and clients as well as promoting quality standards and initiatives such as certifications and awards are all strategies that help engage the business and scientific communities, fostering an integrated and sustainable approach to risk management.

8.3. Guidance 3: Investing in Risk Reduction

To implement effective risk reduction strategies, it is essential to allocate financial and logistical resources comprehensively across all areas of the company, ensuring adequate support for these initiatives. Additionally, it is necessary to develop risk transfer mechanisms such as insurance and risk-sharing partnerships, which provide financial protection for suppliers, partners, and customers. At the same time, strengthening investments in critical facilities and systems is crucial to their preservation as well as for mitigating vulnerabilities.

Another priority is to promote preparedness for security events by integrating risk reduction measures with financial and legal aspects. The risk management perspective should be shared and integrated among all stakeholders, including suppliers, partners, and customers, thereby consolidating a collaborative and comprehensive approach to mitigating organizational risks.

9. Conclusions

The digital transformation is undeniably one of the most impactful events occurring today. It is the result of a gradual technological evolution which started with the information technology revolution that took place between the 1980s and 1990s, and has quickly reached its current stage with the massive use of technology by both citizens and companies. It is not a choice that can be made according to a lifestyle, but rather a basic requirement for performing daily tasks such as shopping, studying, managing bank accounts, watching movies, and chatting with friends. Today, tasks that were once performed physically are now predominantly digital.

In this way, the expectation is more profit and competitive advantage for companies, better prices and higher quality products and services for consumers, and improved quality of life and work for people. There is hope that because with the use of technologies, there will be more comfort, security, and free time for pleasurable activities. This is something that individuals seek with the use of technology, as they can outsource repetitive or dangerous tasks to machines, creating conditions for tasks that add more value, whether in terms of leisure or education. This fuels the expectation of a better future.

Despite these expectations, however, reality may show another face. Due to the rapid and disruptive change that the digital transformation is triggering, companies may be unable to adapt. Competitive advantage does not come unconditionally just from the use of technologies, and companies may disappear from the market in a few years [56]. As a result, people can become frustrated. They may lose their jobs; as consumers, they may feel insecure due to privacy issues as they share their personal data with the remaining companies. Thus, risk replaces expectation. Consequently, citizens and companies can feel threatened by this revolution that was supposed to bring optimism.

According to the results of the present work, what happens is the underestimation of a fundamental element in the occurrence of a revolution. This is not exclusive to DT, and applies to all disruptive changes that have occurred in the past; rather, it is about underestimating the risk, that is, the threat, that a modification entails. This is the danger that DT brings to both citizens and companies, and should be considered more carefully in order to obtain the most out of this great disruption.

It is important to emphasize that the risk is not trivial and that it has several dimensions. The risks are not simply ones such as invasion of a company's servers or a domestic router, which exist but are already well addressed by current tools. There are already many models and tools that address risks in specific applications and equipment.

Our systematic literature review allowed the construction of a risk framework, which was validated by IT market experts through a questionnaire. The resulting framework delivers support for companies in their DT journey, and enables mechanisms by which risks can be prioritized and mitigated by companies.

10. Contributions

The contributions of this work offer three perspectives. The first is an immediate contribution to academia, expanding the theory on the risks associated with the use of digital technologies. This topic is not trivial and easily transcends the boundaries of research, as the risks span various areas of knowledge. Although contradictions may arise during their identification and classification, the academic contribution of this paper is to expand the field of study concerning the side-effects of using digital technologies. By identifying and prioritizing risks, our framework further strengthens existing approaches by providing enhanced visibility on the associated risks incurred throughout the DT journey.

The second contribution of this paper is a systematic literature review that presents the academic state of the art on the topic of risks and technologies. This contribution offers a snapshot of the topic that can be compared with other studies and at different points in time.

The third contribution is a tool which can be applied by companies to support them on their DT journey, including all the references and foundations to help them identify and classify the associated risks. The goal is to recognize risks so that they can be reduced and even prevented. This is the most significant contribution of the entire work, enabling the use of digital technologies without resulting in losses due to the risks discussed in this paper.

The proposed framework enables small companies with limited budgets to implement IT security policies tailored to the identified risks. This is highly beneficial, as our framework brings much-needed visibility to a critical and sensitive topic for small businesses.

11. Limitations

In the same way as other research on risk, the present study has some limitations. The first identifiable limitation is that although our identification of risks was based on a consistent literature review along with validation by IT specialists, it did not include empirical application in real companies; in other words, it is fundamentally theoretical and has not yet had practical application in organizations. A second limitation that can be identified is that the consultation was exclusively with market specialists, meaning that the research lacks the perspective of public companies or government agencies. Thus, our results do not cover a national dimension that could contribute to the national security of countries. The third limitation pertains to the sample size, as our consultation included only 35 respondents. Finally, it should also be noted that average citizens were not consulted to gain insight into their concerns, as the research focused essentially on specialists from private companies.

12. Future Research

The future work that this research enables involves the creation of a model for risk prioritization and mitigation using the proposed and evaluated framework as a starting point. This research could be expanded beyond private companies to include public companies, governments, governmental bodies, or non-governmental organizations. This expansion of the research would help to support these organizations on their DT journey by considering the risks in the context of governments and society. Additionally, a suggested future work is to expand the current research to cover risks of other types, such as social, human, and national security risks. This would extend the current research beyond the risks of digital technologies to encompass their effects on society or the critical infrastructure of countries. The topic of risk is broad, and can be explored from various perspectives in future studies. Another suggestion for future work is to revisit the topics of information leakage and information disclosure, as these presented some contradictions among the respondents in our field research.

Author Contributions: Conceptualization, E.S. and I.C.; searches, E.S.; data curation, E.S. and I.C.; formal analysis, E.S. and I.C.; funding acquisition, I.C.; investigation, E.S. and I.C.; methodology, M.A.G.; project administration, I.C.; resources, I.C.; supervision, R.C.M.; validation, B.R.P.; writing—original draft preparation, E.S.; writing—review and editing, E.S., R.d.S.G., and A.d.P.P. All authors have read and agreed to the published version of the manuscript.

Funding: This study was supported in Brazil by CAPES—Coordination of Personnel Improvement for Higher Education: Code 001. Researchers working on this study have scholarships from Univesity Nove de Julho.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Data are contained within the article.

Acknowledgments: The work described in this document was carried out as part of the research projects of Ivanir Costa, Marcos Antonio Gaspar, and Eduardo Stefani from the Master's and Doctoral Program at University Nove de Julho.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

Table A1. Inclusion and exclusion criteria, with comments.

I/E	Criteria	Comments
E	SER (Search Engine Reason)	The paper has only its title, abstract, and keywords in English but not its full-text.
E	WF (Without Full-Text)	A paper without full text to be assessed.
E	NR (Non-Related)	NR-1: The paper is not an academic article.; NR-2: The definition of risk is not related to DT.
I	LR (Loosely Related.)	LR-1: Risk and DT are used as examples.; LR-2: Risk and DT are used to future research.; LR-3: Risk and DT are used as expressions; LR-4: Risk and DT are presented as keywords.
I	PR (Partially related)	PR-1: Risk and DT are used as challenges or trends.; PR-2: Risk and DT are among the topics reviewed or discussed.
I	CR (Closely related)	The research efforts are explicitly dedicated to Risk and DT.

Table A2. Identified risks.

Identification	Risk	Occurrences
a	Privacy Leakage	18
b	Malware	8
c	Ransomware	8
d	Information Leakage	7
e	Data Theft/Manipulation	5
f	Unauthorized Access	5
g	Phishing	4
h	Information Disclosure	4
i	Denial of Services	3
j	Data Breach	3
k	Spoofing	3
l	Spyware	2
m	Virus	2
n	Tampering	2
o	Sniffing	2
p	Worms	1
q	Bombs	1
r	Trojans	1
s	MitM attacks	1
t	Repudiation	1
u	Elevation Privileges	1

Table A3. Authors by identified risks.

Authors	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
[38]	✓																				
[57]	✓																				
[58]						✓															
[59]	✓																				
[60]	✓																				
[61]	✓																				
[62]					✓	✓															
[63]	✓			✓		✓	✓		✓				✓		✓	✓	✓	✓			
[64]														✓							
[65]		✓	✓																		
[66]	✓	✓				✓									✓						
[67]		✓																			
[68]	✓																				
[69]				✓																	
[27]	✓																				
[70]	✓																				
[71]		✓																			
[32]		✓																			
[36]			✓																		
[31]	✓			✓		✓		✓													
[7]	✓																				

Table A3. *Cont.*

Authors	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
[46]		✓																			
[72]											✓								✓		
[73]	✓			✓																	
[74]								✓			✓			✓						✓	✓
[45]	✓							✓		✓											
[75]	✓																				
[76]		✓	✓				✓		✓			✓									
[21]			✓	✓	✓																
[77]			✓																		
[78]	✓		✓		✓		✓		✓		✓	✓	✓								
[79]	✓			✓				✓		✓											
[80]	✓			✓																	
[47]			✓																		
[81]					✓																
[82]		✓	✓		✓		✓			✓											
Total	**18**	**8**	**8**	**7**	**5**	**5**	**4**	**4**	**3**	**3**	**3**	**2**	**2**	**2**	**2**	**1**	**1**	**1**	**1**	**1**	**1**

Appendix B

Table A4. Indication of relevant risks using the ABC curve.

Risk ID	# Citations	% Citations	% Total	ABC	Description
a	18	21.43%	21.43%	A	Privacy Leakage
b	8	9.52%	30.95%	A	Malware
c	8	9.52%	40.48%	A	Ransomware
d	7	8.33%	48.81%	A	Information Leakage
e	5	5.95%	54.76%	A	Data Theft/Manipulation
f	5	5.95%	60.71%	A	Unauthorized Access
g	4	4.76%	65.48%	A	Phishing
h	4	4.76%	70.24%	A	Information Disclosure
i	3	3.57%	73.81%	B	Denial of Service
j	3	3.57%	77.38%	B	Data Breach
k	3	3.57%	80.95%	B	Spoofing
l	2	2.38%	83.33%	B	Spyware
m	2	2.38%	85.71%	B	Virus
n	2	2.38%	88.10%	B	Tampering
o	2	2.38%	90.48%	C	Sniffing
p	1	1.19%	91.67%	C	Worms
q	1	1.19%	92.86%	C	Bombs
r	1	1.19%	94.05%	C	Trojans
s	1	1.19%	95.24%	C	MitM attacks
t	1	1.19%	96.43%	C	Repudiation
u	1	1.19%	97.62%	C	Elevation Privileges

Appendix C

Table A5. Likert scale answers from the respondents.

Respondent	(a.1)	(a.2)	(a.3)	(a.4)	(b.1)	(b.2)	(b.3)	(b.4)	(c.1)	(c.2)	(c.3)	(c.4)	(d.1)	(d.2)	(d.3)	(d.4)	(e.1)	(e.2)	(e.3)	(e.4)	(f.1)	(f.2)	(f.3)	(f.4)	(g.1)	(g.2)	(g.3)	(g.4)	(h.1)	(h.2)	(h.3)	(h.4)
1	4	4	5	5	4	5	3	5	5	4	4	5	1	4	3	5	4	4	5	5	4	4	2	5	5	5	5	4	4	5	5	3
2	5	5	5	1	5	4	5	4	4	5	4	1	3	4	4	1	5	5	5	5	4	5	2	5	5	4	4	5	1	5	1	5
3	5	5	5	5	5	5	4	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5	3	5	5	5	5	5	4	5	5	5
4	4	4	3	3	4	5	4	5	5	5	5	5	2	5	3	5	5	5	5	5	4	5	3	4	5	5	5	5	5	3	4	5
5	5	4	5	1	5	3	1	4	3	4	5	5	1	4	3	5	5	4	4	3	4	1	1	4	4	3	4	3	3	5	5	5
6	3	4	2	2	5	4	3	4	4	5	5	4	3	4	3	5	5	5	4	4	3	5	3	5	5	4	3	5	4	4	3	4
7	5	5	5	4	5	2	4	4	5	5	5	5	2	5	4	4	5	5	5	5	5	4	3	5	5	5	5	3	5	4	2	1
8	4	5	5	5	4	5	4	5	4	5	5	5	3	5	5	5	5	5	5	5	4	5	4	5	5	4	4	3	1	1	3	5
9	5	5	5	4	5	4	4	4	4	3	5	5	2	4	5	4	4	4	4	4	4	3	5	3	4	4	5	5	4	5	4	4
10	5	4	5	4	1	2	1	1	4	4	5	5	2	4	4	4	5	4	4	4	4	2	2	4	4	5	5	5	4	4	4	2
11	4	3	5	1	3	3	4	3	4	5	5	5	3	4	4	5	5	4	5	5	5	5	3	1	5	4	5	3	2	3	1	4
12	4	3	5	4	4	4	4	3	4	4	3	4	2	3	3	4	4	4	4	4	4	4	3	4	4	3	3	3	2	4	3	3
13	4	4	4	4	5	5	5	5	5	5	5	5	4	4	4	5	4	5	5	4	4	4	5	4	1	2	1	5	4	4	4	4
14	4	4	4	5	5	5	5	5	5	5	5	5	2	4	5	5	5	4	5	4	2	5	5	4	5	5	5	5	4	5	2	2
15	4	5	4	5	4	2	3	2	4	3	5	4	3	4	2	5	4	5	4	5	4	4	4	5	2	2	2	3	4	5	1	2
16	4	1	5	2	4	3	2	2	4	5	5	5	2	4	4	5	5	4	4	4	4	5	2	4	4	4	5	4	2	4	2	4
17	5	5	5	5	5	4	4	5	3	3	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	4
18	5	1	1	1	4	3	2	2	2	2	4	4	2	4	2	5	5	4	5	5	4	5	1	4	5	5	3	3	5	5	3	2
19	5	4	5	4	5	4	5	3	4	5	5	5	4	4	4	5	5	5	5	4	4	4	5	4	5	5	4	5	4	5	5	4
20	5	3	4	4	5	5	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	5	5	4	5	5	5	5	4	4	4	4
21	5	5	5	4	5	4	4	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	4	5	4
22	2	4	5	4	5	5	5	4	4	4	4	5	4	5	5	5	5	5	5	5	4	5	5	5	5	4	5	5	2	4	4	4
23	5	1	5	1	5	5	1	3	5	5	5	3	4	3	5	5	5	5	5	5	5	5	1	1	5	5	3	5	2	5	4	5
24	5	3	4	4	5	3	2	5	5	5	5	5	2	5	3	2	5	5	5	5	5	5	4	5	5	5	5	5	4	4	4	4
25	4	5	5	2	5	4	2	2	2	5	5	5	2	5	4	2	5	5	5	5	4	2	2	5	5	4	2	5	1	4	2	3
26	5	4	5	5	5	5	3	3	5	5	5	4	3	3	4	4	5	5	5	5	3	3	2	5	5	5	5	5	1	1	3	5
27	4	3	4	5	2	4	4	2	5	4	5	5	1	4	4	5	5	5	5	4	1	5	4	2	5	5	4	5	2	4	2	4
28	5	4	5	2	5	5	4	5	5	5	5	4	3	5	5	5	5	5	5	5	4	4	1	5	5	5	5	5	4	2	5	5
29	5	2	5	5	5	5	5	4	5	5	5	5	4	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5	4	4
30	5	3	5	2	4	2	4	3	5	5	5	5	1	4	4	5	5	4	5	4	5	5	3	4	5	4	5	4	3	3	2	3
31	5	4	5	5	5	5	5	4	5	5	5	5	2	5	4	3	5	5	4	5	4	5	2	4	5	5	5	5	3	5	2	2
32	4	5	2	5	5	5	4	4	4	4	4	4	4	5	3	5	3	4	5	4	4	3	1	3	4	4	4	4	4	4	4	5
33	5	4	5	5	4	4	4	5	4	4	5	5	2	5	5	5	5	5	4	5	4	5	2	5	5	4	4	3	5	5	3	2
34	4	2	5	5	4	3	3	3	3	3	5	4	4	3	4	1	5	5	5	5	4	5	4	3	4	3	2	3	5	5	4	3
35	5	1	1	1	1	1	1	1	1	1	1	1	2	1	3	2	1	1	1	1	1	1	1	1	1	2	1	1	3	3	3	1

Appendix C.1. Privacy Leakage

As shown in Figure A1, for statement (a.1), 94% of respondents answered between agree and strongly agree, with 37% and 57% respectively. Neutral and disagree responses account for 6%, with 3% each. There were no responses for strongly disagree. Statement (a.2) shows 66% of responses between agree and strongly agree. The remaining 34% include responses for strongly disagree, disagree, and neutral, with 11%, 6%, and 17% respectively. Statement (a.3) shows 6%, 6%, 3%, 17%, and 69% for strongly disagree, disagree, neutral, agree, and strongly agree. Statement (a.4) has the highest proportion of responses for strongly disagree and disagree, totaling 31%, with 17% and 14% each. Neutral accounts for 3%, while agree and strongly agree make up 66%, with 29% and 37% respectively. The agree scale has an average of 30%, along with an average of 48% for strongly agree.

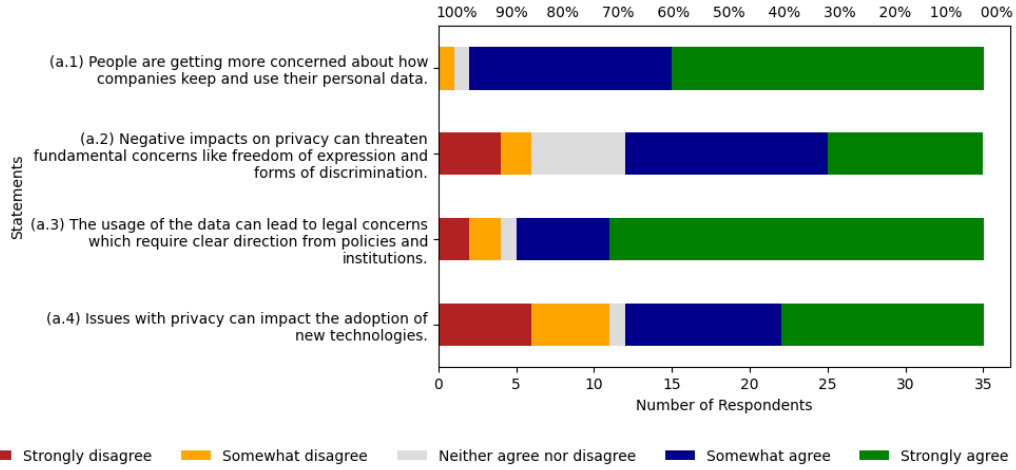

Figure A1. Likert scale for privacy leakage.

The sum of the two averages results is 78%. In the ABC curve, the risk was classified as relevant with 21.43% of citations, and on the Likert scale, respondents indicate 78% agreement with the risk, thereby indicating it is a relevant risk.

Appendix C.2. Malware

As shown in Figure A2, for statement (b.1), 89% of respondents fall between agree and strongly agree, with 29% and 60% respectively. Strongly disagree, disagree, and neutral together make up 11%, with 6%, 3%, and 3% each. For statement (b.2), 69% chose agree and strongly agree, with 29% and 40% respectively. 17% selected neutral, and 14% fell between strongly disagree and disagree, with 3% and 11% each. Statement (b.3) totals 63% for agree and strongly agree, with 43% and 20% each. 14% selected neutral, while 11% chose strongly disagree and 11% disagree. For statement (b.4), 60% selected agree and strongly agree, with 29% and 31% respectively. Strongly disagree, disagree, and neutral present 6%, 14%, and 20% respectively. The agree scale has an average of 32%, along with an average of 38% for strongly agree.

The sum of these two averages results in 70%. In the ABC curve, the risk was classified as relevant with 9.52% of citations, and on the Likert scale the respondents indicate 70% agreement with the risk, indicating that it is a relevant risk.

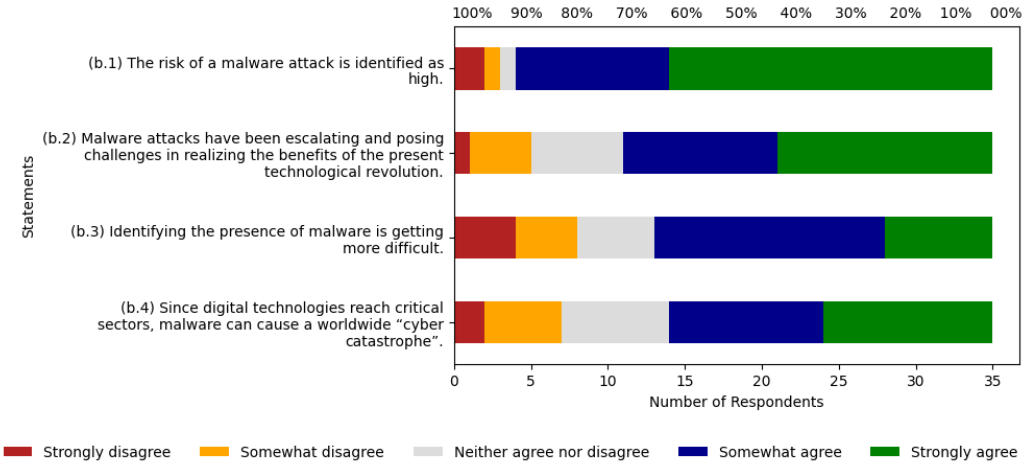

Figure A2. Likert scale for malware.

Appendix C.3. Ransomware

According to Figure A3, statement (c.1) shows that 83% of respondents are between agree and strongly agree, with 40% and 43% respectively. Strongly disagree, disagree, and neutral total 17%, with 3%, 6%, and 9% each. Statement (c.2) shows similar results, with 83% choosing agree and strongly agree, at 26% and 57% each. Strongly disagree, disagree, and neutral total 17%, with 3%, 3%, and 11% each. Statement (c.3) resulted in 94% of respondents between agree and strongly agree, with 20% and 74% each. Strongly disagree and neutral responses combined are 6%, with 3% each, and there were no responses for disagree. Statement (c.4) shows 91% of respondents between agree and strongly agree, with 29% and 63% each. Strongly disagree and neutral account for 6% and 3% respectively. The agree scale has an average of 29%, along with an average of 59% for strongly agree.

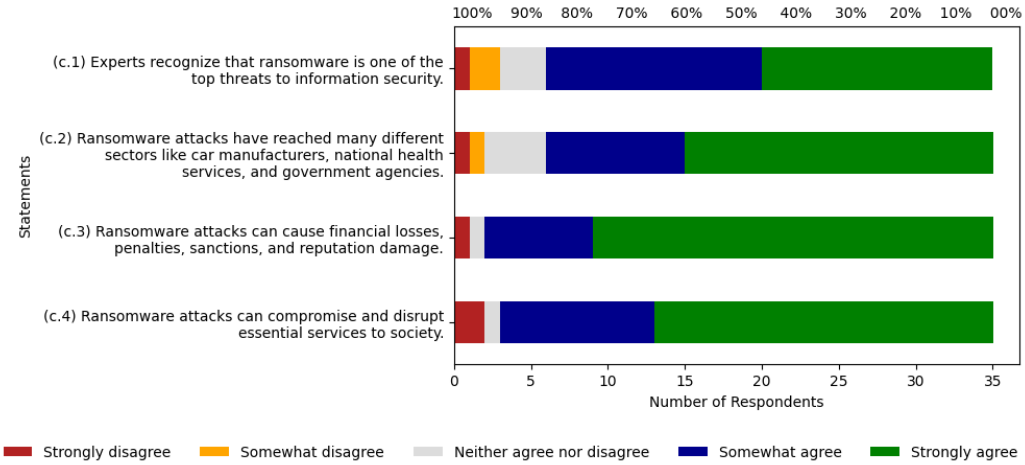

Figure A3. Likert scale for ransomware.

The sum of these two averages results is 88%. In the ABC curve, the risk was classified as relevant with 9.52% of citations, and on the Likert scale the respondents indicated 88% agreement with the risk, indicating that it is a relevant risk.

Appendix C.4. Information Leakage

As shown in Figure A4, for statement (d.1), 31% of respondents are between agree and strongly agree, with 29% and 3% each. Strongly disagree, disagree, and neutral responses account for 69% of respondents, with 11%, 37%, and 20% respectively. Statement (d.2) shows 86% of respondents between agree and strongly disagree. Strongly disagree and

neutral responses account for 14% of respondents, with 3% and 11% each. For statement (d.3), 71% of respondents are between agree and strongly agree, with 40% and 31% each. Disagree and neutral total 29%, with 6% and 23% respectively. Statement (d.4) shows 83% of respondents between agree and strongly agree, with 40% and 31% each. Strongly disagree, disagree, and neutral responses make up 17%, with 6%, 9%, and 3% each. The agree scale has an average of 32%, along with an average of 36% for strongly agree.

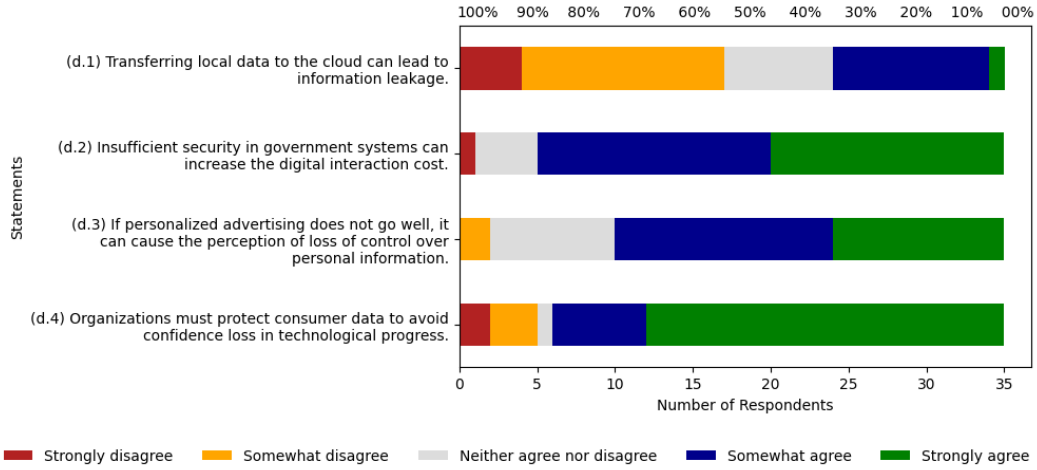

Figure A4. Likert scale for information leakage.

The sum of these two averages results is 68%. In the ABC curve, the risk was classified as relevant with 8.33% of citations, and on the Likert scale, respondents indicated 68% agreement with the risk. This risk falls below the 70% threshold for risk relevance eligibility, which indicates that the risk is not relevant for the specialists.

Appendix C.5. Data Theft/Manipulation

According to Figure A5, for statement (e.1), 94% of respondents fall between agree and strongly agree, with 17% and 77% respectively. Strongly disagree and neutral account for 6%, with 3% each. Statement (e.2) shows 97% of respondents between agree and strongly agree, with 34% and 63% each. Strongly disagree makes up 3% of responses. Statement (e.3) totals 97% for agree and strongly agree, with 29% and 69% respectively. Strongly disagree accounts for 3% of responses. Statement (e.4) has 94% between agree and strongly agree, with 34% and 60% respectively. Strongly disagree and neutral together make up 6%, with 3% each. The agree scale has an average of 29%, along with an average of 67% for strongly agree.

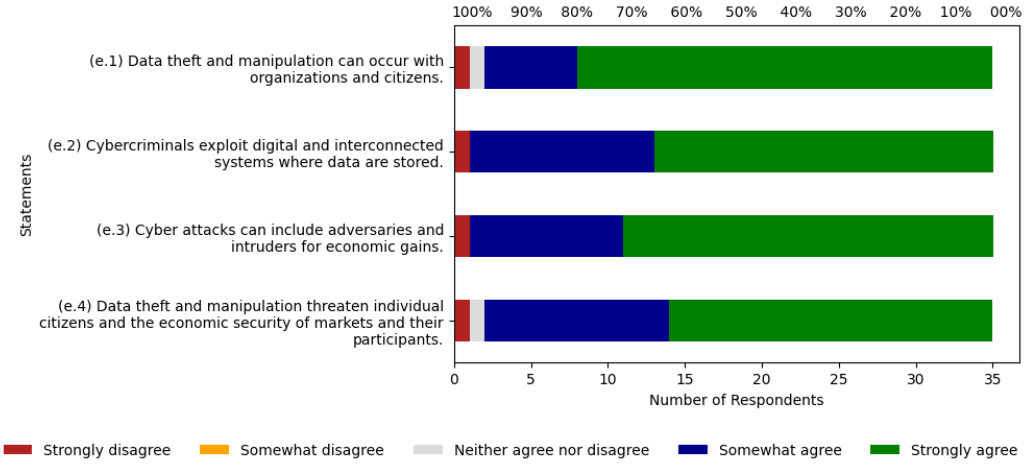

Figure A5. Likert scale for data theft/manipulation.

The sum of these two averages results is 96%. In the ABC curve, the risk was classified as relevant with 5.95% of citations, and on the Likert scale the respondents indicated 96% agreement with the risk, indicating that it is a relevant risk.

Appendix C.6. Unauthorized Access

As shown in Figure A6, statement (f.1) has 86% of respondents between agree and strongly agree, with 66% and 20% each. Strongly disagree, disagree, and neutral responses make up 14%, with 6%, 3%, and 6% respectively. Statement (f.2) has 80% between agree and strongly agree, with 20% and 60% each. Strongly disagree, disagree, and neutral responses total 20%, with 6%, 6%, and 9% each. Statement (f.3) shows 40% between agree and strongly agree, with 17% and 23% each. Strongly disagree, disagree, and neutral responses total 60%, with 17%, 23%, and 20% each. Finally, statement (f.4) shows 80% of respondents between agree and strongly agree, with 34% and 46% respectively. Strongly disagree, disagree, and neutral responses account for 20%, with 9%, 3%, and 9% each. The agree scale has an average of 34%, along with an average of 37% for strongly agree.

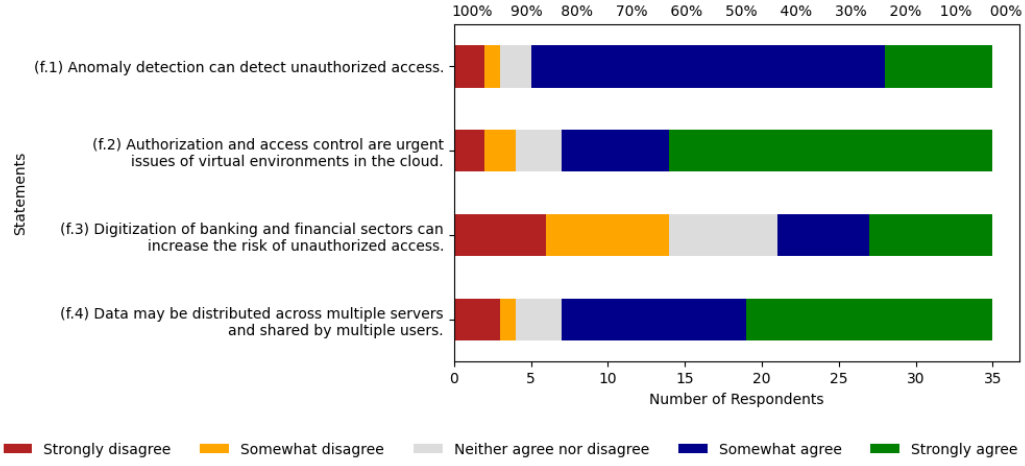

Figure A6. Likert scale for unauthorized access.

The sum of these two averages results is 71%. In the ABC curve, the risk was classified as relevant with 5.95% of citations, and on the Likert scale the respondents indicated 71% agreement with the risk, indicating that it is a relevant risk.

Appendix C.7. Phishing

According to Figure A7, statement (g.1) shows 91% of respondents between agree and strongly agree, with 20% and 71% each. Strongly disagree and disagree total 9%, with 6% and 3% respectively. Statement (g.2) has 82% between agree and strongly agree, with 31% and 51% each. Disagree and neutral account for 18%, with 9% each. Statement (g.3) shows 74% of respondents between agree and strongly agree, with 20% and 54% each. Strongly disagree, disagree, and neutral total 26%, with 6%, 9%, and 11% respectively. Finally, statement (g.4) has 71% between agree and strongly agree, with 11% and 60% respectively. Strongly disagree and neutral account for 29% of respondents, with 3% and 26% each. The agree scale has an average of 21%, along with an average of 59% for strongly agree.

The sum of these two averages results is 80%. In the ABC curve, the risk was classified as relevant with 4.76% of citations, and on the Likert scale the respondents indicated 80% agreement with the risk, considering it is a relevant risk.

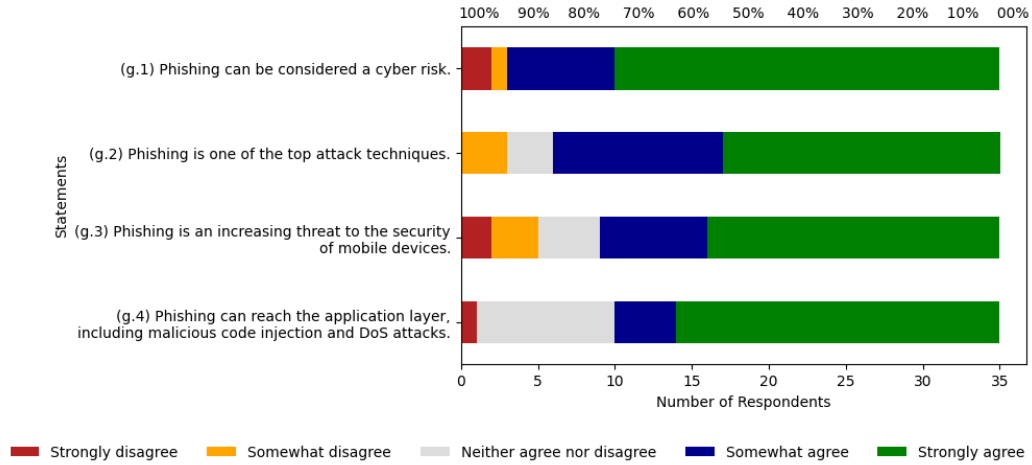

Figure A7. Likert scale phishing.

Appendix C.8. Information Disclosure

As shown in Figure A8, statement (h.1) has 60% of respondents between agree and strongly agree, with 40% and 20% respectively. Strongly disagree, disagree, and neutral responses total 40%, with 11%, 17%, and 11% each. Statement (h.2) shows 80% of respondents between agree and strongly agree, with 40% each. Strongly disagree, disagree, and neutral responses make up 20%, with 6%, 3%, and 11% respectively. Statement (h.3) has 51% of respondents between agree and strongly agree, with 34% and 17% each. Strongly disagree, disagree, and neutral total 49%, with 9%, 20%, and 20% each. Finally, statement (h.4) has 63% of respondents between agree and strongly agree, with 37% and 26% respectively. Strongly disagree, disagree, and neutral responses account for 37%, with 6%, 17%, and 14% each. The agree scale has an average of 38%, along with an average of 26% for strongly agree.

The sum of these two averages results is 64%. In the ABC curve, the risk was classified as relevant with 4.76% of citations, and on the Likert scale respondents indicated 64% agreement with the theme. This risk falls below the 70% threshold for risk relevance eligibility, which means the specialists do not consider it as a relevant risk.

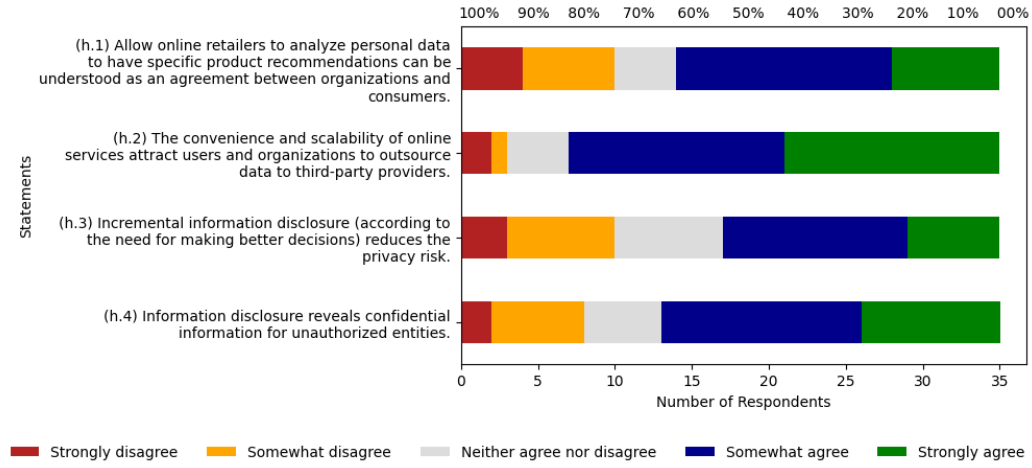

Figure A8. Likert scale information disclosure.

Appendix D

Table A6. Reliability statistics for Cronbach's alpha coefficient.

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N Items
0.918	0.925	32

Table A7. Summary item statistics.

	Mean	Minimum	Maximum	Range	Max/Min	Variance	N Items
Item Means	4.038	2.743	4.657	1.914	1.698	0.233	32
Item Variances	1.198	0.492	2.373	1.881	4.819	0.199	32

Table A8. Cronbach's alpha coefficient [83].

Cronbach's Alpha	Strenght
<0.00	Poor
0.00–0.20	Slight
0.21–0.40	Fair
0.41–0.60	Moderate
0.61–0.80	Substantial
0.81–1.00	Almost Perfect

References

1. Bharadwaj, A.; El Sawy, O.A.; Pavlou, P.A.; Venkatraman, N. Digital Business Strategy: Toward a next Generation of Insights. *MIS Q.* **2013**, *37*, 471–482. [CrossRef]
2. Schneider, S.; Kokshagina, O. Digital Transformation: What We Have Learned (Thus Far) and What Is Next. *Creat. Innov. Manag.* **2021**, *30*, 384–411. [CrossRef]
3. Fernandes, A.A.; Diniz, J.L.; Abreu, D.; de Souza, V.F.d.E.; Paiva Tonon, D.H.; Brito da Silva, E.; Costa, I.; Cardoso de Oliveira, J.; Alberto de Seixas, J.; Leão, L.; et al. *Governança Digital 4.0*; BRASPORT: La Chaux-de-Fonds, Switzerland, 2019.
4. Al-Debei, M.M.; Avison, D. Developing a Unified Framework of the Business Model Concept. *Eur. J. Inf. Syst.* **2010**, *19*, 359–376. [CrossRef]
5. Schnasse, F.; Menzefricke, J.S.; Dumitrescu, R. Identification of Socio-Technical Risks and Their Correlations in the Context of Digital Transformation for the Manufacturing Sector. In Proceedings of the 2021 IEEE 8th International Conference on Industrial Engineering and Applications (ICIEA), Virtual, 23–26 April 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 159–166.
6. Vial, G. Understanding Digital Transformation: A Review and a Research Agenda. *J. Strateg. Inf. Syst.* **2019**, *28*, 118–144. [CrossRef]
7. El-Haddadeh, R. Digital Innovation Dynamics Influence on Organisational Adoption: The Case of Cloud Computing Services. *Inf. Syst. Front.* **2020**, *22*, 985–999. [CrossRef]
8. Hanelt, A.; Bohnsack, R.; Marz, D.; Antunes Marante, C. A Systematic Review of the Literature on Digital Transformation: Insights and Implications for Strategy and Organizational Change. *J. Manag. Stud.* **2021**, *58*, 1159–1197. [CrossRef]
9. Morakanyane, R.; Grace, A.A.; O'Reilly, P. Conceptualizing Digital Transformation in Business Organizations: A Systematic Review of Literature. In Proceedings of the Bled eConference 2017, Bled, Slovenia, 18–21 June 2017; p. 21.
10. Lamberton, C.; Stephen, A.T. A Thematic Exploration of Digital, Social Media, and Mobile Marketing: Research Evolution from 2000 to 2015 and an Agenda for Future Inquiry. *J. Mark.* **2016**, *80*, 146–172. [CrossRef]
11. Verhoef, P.C.; Stephen, A.T.; Kannan, P.; Luo, X.; Abhishek, V.; Andrews, M.; Bart, Y.; Datta, H.; Fong, N.; Hoffman, D.L.; et al. Consumer Connectivity in a Complex, Technology-Enabled, and Mobile-Oriented World with Smart Products. *J. Interact. Mark.* **2017**, *40*, 1–8. [CrossRef]
12. Colbert, A.; Yee, N.; George, G. The Digital Workforce and the Workplace of the Future. *Acad. Manag. J.* **2016**, *59*, 731–739. [CrossRef]
13. Guilbaud, P.; Hayes, M.; Hamed, D. Use of Enabling Technology to Enhance Self-Efficacy Beliefs and Social Capital Dispositions: Integrating ArcGIS in an Upper Level Business Course. In Proceedings of the Global Learn, Association for the Advancement of Computing in Education (AACE), New Orleans, LO, USA, 4–7 November 2019; pp. 130–143.
14. Xia, F.; Liu, L.; Li, J.; Ma, J.; Vasilakos, A.V. Socially Aware Networking: A Survey. *IEEE Syst. J.* **2013**, *9*, 904–921. [CrossRef]
15. Costa, I.; Riccotta, R.; Montini, P.; Stefani, E.; de Souza Goes, R.; Gaspar, M.A.; Martins, F.S.; Fernandes, A.A.; Machado, C.; Loçano, R.; et al. The Degree of Contribution of Digital Transformation Technology on Company Sustainability Areas. *Sustainability* **2022**, *14*, 462. [CrossRef]
16. Slavković, M.; Pavlović, K.; Mamula Nikolić, T.; Vučenović, T.; Bugarčić, M. Impact of Digital Capabilities on Digital Transformation: The Mediating Role of Digital Citizenship. *Systems* **2023**, *11*, 172. [CrossRef]

17. Carayannis, E.G.; Christodoulou, K.; Christodoulou, P.; Chatzichristofis, S.A.; Zinonos, Z. Known Unknowns in an Era of Technological and Viral Disruptions-Implications for Theory, Policy, and Practice. *J. Knowl. Econ.* **2021**, *13*, 1–24. [CrossRef]
18. Lemos, F. On the Definition of Risk. *J. Risk Manag. Financ. Inst.* **2020**, *13*, 266–278. [CrossRef]
19. Spekman, R.E.; Davis, E.W. Risky Business: Expanding the Discussion on Risk and the Extended Enterprise. *Int. J. Phys. Distrib. Logist. Manag.* **2004**, *34*, 414–433. [CrossRef]
20. Librantz, A.F.H.; Costa, I.; Spinola, M.d.M.; de Oliveira Neto, G.C.; Zerbinatti, L. Risk Assessment in Software Supply Chains Using the Bayesian Method. *Int. J. Prod. Res.* **2021**, *59*, 6758–6775. [CrossRef]
21. Gaivoronskaya, Y.V.; Mamychev, A.Y.; Petrova, D.A.; Rusanova, I.O. Typology of Risks and Threats Caused by Digitalization. *Rev. Tur. Estud. Práticas* **2020**, *5*, 1–12.
22. Hess, T.; Matt, C.; Benlian, A.; Wiesböck, F. Options for Formulating a Digital Transformation Strategy. *MIS Q. Exec.* **2016**, *15*, 123.
23. Future of Industry Ecosystems: Shared Data and Insights. IDC Blog—Blogs.Idc.Com. Available online: https://blogs.idc.com/2021/01/06/future-of-industry-ecosystems-shared-data-and-insights (accessed on 8 December 2024).
24. Gartner. The Top 8 Cybersecurity Predictions for 2021–2022. Available online: https://www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022-1 (accessed on 3 February 2022).
25. Hausberg, J.; Liere-Netheler, K.; Packmohr, S.; Pakura, S.; Vogelsang, K. Digital Transformation in Business Research: A Systematic Literature Review and Analysis. In Proceedings of the DRUID18, Copenhagen, Denmark, 11–13 June 2018.
26. Urbinati, A.; Chiaroni, D.; Chiesa, V.; Frattini, F. The Role of Digital Technologies in Open Innovation Processes: An Exploratory Multiple Case Study Analysis. *R&D Manag.* **2020**, *50*, 136–160.
27. O'Leary, T.; Armfield, T. Adapting to the Digital Transformation. *Alta. Law Rev.* **2020**, *58*, 249. [CrossRef]
28. de Araujo, R.F.; Oliveira, M. Da Informática à Tecnologia Da Informação: Dependência, Reserva de Mercado e Suas Implicações Político-Econômicas From Informatics to Information Technology: Dependence, Market Reserve and Its Political and Economic Implications. *LIINC Rev.* **2017**, *13*, 401–415. [CrossRef]
29. Cheng, G.-J.; Liu, L.-T.; Qiang, X.-J.; Liu, Y. Industry 4.0 Development and Application of Intelligent Manufacturing. In Proceedings of the 2016 International Conference on Information System and Artificial Intelligence (ISAI), Hong Kong, China, 24–26 June 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 407–410.
30. Siderska, J. Robotic Process Automation—A Driver of Digital Transformation? *Eng. Manag. Prod. Serv.* **2020**, *12*, 21–31. [CrossRef]
31. Yang, P.; Xiong, N.; Ren, J. Data Security and Privacy Protection for Cloud Storage: A Survey. *IEEE Access* **2020**, *8*, 131723–131740. [CrossRef]
32. Panda, A.; Bower, A. Cyber Security and the Disaster Resilience Framework. *Int. J. Disaster Resil. Built Environ.* **2020**, *11*, 507–518. [CrossRef]
33. Act, P. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. *Public Law* **2001**, *107*, 56.
34. Luker, M.A. The National Strategy to Secure Cyberspace. *Educ. Rev.* **2003**, *38*, 60.
35. Owen, R.S. Infrastructures of Cyber Warfare. In *Cyber Warfare and Cyber Terrorism*; IGI Global: Hershey, PA, USA, 2007; pp. 35–41. [CrossRef]
36. de la Peña Zarzuelo, I. Cybersecurity in Ports and Maritime Industry: Reasons for Raising Awareness on This Issue. *Transp. Policy* **2021**, *100*, 1–4. [CrossRef]
37. Fekete, A.; Rhyner, J. Sustainable Digital Transformation of Disaster Risk-Integrating New Types of Digital Social Vulnerability and Interdependencies with Critical Infrastructure. *Sustainability* **2020**, *12*, 9324. [CrossRef]
38. Nuccio, M.; Guerzoni, M. Big Data: Hell or Heaven? Digital Platforms and Market Power in the Data-Driven Economy. *Compet. Change* **2019**, *23*, 312–328. [CrossRef]
39. Bryman, A. Integrating Quantitative and Qualitative Research: How Is It Done? *Qual. Res.* **2006**, *6*, 97–113. [CrossRef]
40. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G.; Prisma Group. Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *Int. J. Surg.* **2010**, *8*, 336–341. [CrossRef] [PubMed]
41. Liao, Y.; Deschamps, F.; Loures, E.d.F.R.; Ramos, L.F.P. Past, Present and Future of Industry 4.0—A Systematic Literature Review and Research Agenda Proposal. *Int. J. Prod. Res.* **2017**, *55*, 3609–3629. [CrossRef]
42. Ballou, R.H. *Logística Empresarial: Transportes, Administração de Materiais e Distribuição Física*; Atlas: Sao Paulo, Brazil, 1993.
43. Alvarenga, A.C.; Novaes, A.G.N. *Logística Aplicada: Suprimento e Distribuição Física*; Editora Blucher: Sao Paulo, Brazil, 2000.
44. Pacchini, A.P.T. O Grau de Prontidão das Empresas Industriais Para Implantação da Indústria 4.0: Um Estudo No Setor Automotivo Brasileiro. Universidade Jove de Julho. Available online: https://bibliotecatede.uninove.br/handle/tede/2220#preview-link0 (accessed on 10 July 2024).
45. Bhattacharjee, K.; Chen, M.; Dasgupta, A. Privacy-Preserving Data Visualization: Reflections on the State of the Art and Research Opportunities. *Proc. Comput. Graph. Forum* **2020**, *39*, 675–692. [CrossRef]
46. Fard, S.M.H.; Karimimpour, H.; Dehghantanha, A.; Jahromi, A.N.; Srivastava, G. Ensemble Sparse Representation-Based Cyber Threat Hunting for Security of Smart Cities. *Comput. Electr. Eng.* **2020**, *88*, 106825. [CrossRef]

47. Chalyuk, Y.; Dovhanyk, N.; Kurbala, N.; Komarova, K.; Kovalchuk, N. The Digital Economy in a Global Environment. *AD ALTA J. Interdiscip. Res.* **2021**, *17*, 143–148.
48. Xing, L.; Levitin, G. Balancing Theft and Corruption Threats by Data Partition in Cloud System with Independent Server Protection. *Reliab. Eng. Syst. Saf.* **2017**, *167*, 248–254. [CrossRef]
49. Alkhalil, Z.; Hewage, C.; Nawaf, L.; Khan, I. Phishing Attacks: Recent Comprehensive Study and a New Anatomy. *Front. Comput. Sci.* **2021**, *3*, 6. [CrossRef]
50. Xu, X.; Zeng, S.; He, Y. The Impact of Information Disclosure on Consumer Purchase Behavior on Sharing Economy Platform Airbnb. *Int. J. Prod. Econ.* **2021**, *231*, 107846. [CrossRef]
51. Lucato, W.C.; Júnior, M.V.; Vanalle, R.M.; Salles, J.A.A. Model to Measure the Degree of Competitiveness for Auto Parts Manufacturing Companies. *Int. J. Prod. Res.* **2012**, *50*, 5508–5522. [CrossRef]
52. Cazorla, I.M.; dos Santos Santana, E.R.; Utsumi, M.C. O Campo Conceitual Da Média Aritmética: Uma Primeira Aproximação Conceitual. *Rev. Eletrônica Educ. Matemática* **2019**, *14*, 1–21. [CrossRef]
53. Forero, C.G. Cronbachâ€™s Alpha. In *Encyclopedia of Quality of Life and Well-Being Research*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 1505–1507.
54. Rosal Santos, I.M.; Guimarães, A.L. Vazamento Em Ministério: Instituições Públicas Sabem Lidar Com Dados Sensíveis? *Consultor Jurídico*. Available online: https://www.conjur.com.br/2021-dez-17/opiniao-instituicoes-publicas-sabem-lidar-dados-sensiveis (accessed on 8 December 2024).
55. Sendai, J. Sendai Framework for Disaster Risk Reduction 2015–2030. In Proceedings of the UN World Conference on Disaster Risk Reduction 2015, Sendai, Japan, 14–18 March 2015; pp. 1–32.
56. Harari, Y.N. *21 Lessons for the 21st Century*; Random House: New York, NY, USA, 2018.
57. Riyana, S.; Natwichai, J. Privacy Preservation for Recommendation Databases. *Serv. Oriented Comput. Appl.* **2018**, *12*, 259–273. [CrossRef]
58. Vasil'ev, Y.S.; Zegzhda, D.P.; Poltavtseva, M.A. Problems of Security in Digital Production and Its Resistance to Cyber Threats. *Autom. Control. Comput. Sci.* **2018**, *52*, 1090–1100. [CrossRef]
59. Tokody, D.; Albini, A.; Ady, L.; Rajnai, Z.; Pongrácz, F. Safety and Security through the Design of Autonomous Intelligent Vehicle Systems and Intelligent Infrastructure in the Smart City. *Interdiscip. Descr. Complex Syst. INDECS* **2018**, *16*, 384–396. [CrossRef]
60. Rossi, E.; Rubattino, C.; Viscusi, G. Big Data Use and Challenges: Insights from Two Internet-Mediated Surveys. *Computers* **2019**, *8*, 73. [CrossRef]
61. Birkel, H.S.; Veile, J.W.; Müller, J.M.; Hartmann, E.; Voigt, K.-I. Development of a Risk Framework for Industry 4.0 in the Context of Sustainability for Established Manufacturers. *Sustainability* **2019**, *11*, 384. [CrossRef]
62. Khanboubi, F.; Boulmakoul, A. Digital Transformation in the Banking Sector: Surveys Exploration and Analytics. *Int. J. Inf. Syst. Chang. Manag.* **2019**, *11*, 93–127. [CrossRef]
63. Mendhurwar, S.; Mishra, R. Integration of Social and IoT Technologies: Architectural Framework for Digital Transformation and Cyber Security Challenges. *Enterp. Inf. Syst.* **2021**, *15*, 565–584. [CrossRef]
64. Baghdasarin, D. MRO Cybersecurity SWOT. *Int. J. Aviat. Aeronaut. Aerosp.* **2019**, *6*, 9. [CrossRef]
65. Eckhart, M.; Brenner, B.; Ekelhart, A.; Weippl, E.R. Quantitative Security Risk Assessment for Industrial Control Systems: Research Opportunities and Challenges. *J. Internet Serv. Inf. Secur.* **2019**, *9*, 52–73.
66. Shi, J.; Jin, L.; Li, J. The Integration of Azure Sphere and Azure Cloud Services for Internet of Things. *Appl. Sci.* **2019**, *9*, 2746. [CrossRef]
67. Alharbi, S.A. A Qualitative Study on Security Operations Centers in Saudi Arabia: Challenges and Research Directions. *J. Theor. Appl. Inf. Technol.* **2020**, *98*, 3972–3982
68. Popescu, S.; Santa, R.; Teleaba, F.; Ilesan, H. A Structured Framework for Identifying Risks Sources Related to Human Resources in a 4.0 Working Environment Perspective. *Hum. Syst. Manag.* **2020**, *39*, 511–527. [CrossRef]
69. Park, S.-T.; Li, G.; Hong, J.-C. A Study on Smart Factory-Based Ambient Intelligence Context-Aware Intrusion Detection System Using Machine Learning. *J. Ambient. Intell. Humaniz. Comput.* **2020**, *11*, 1405–1412. [CrossRef]
70. Puraite, A.; Zuzevičiūtė, V.; Bereikienė, D.; Skrypko, T.; Shmorgun, L. Algorithmic Governance in Public Sector: Is Digitization a Key to Effective Management. *Indep. J. Manag. Prod.* **2020**, *11*, 9.
71. Kabbas, A.; Alharthi, A.; Munshi, A. Artificial Intelligence Applications in Cybersecurity. *Int. J. Comput. Sci. Netw. Secur.* **2020**, *20*, 120–124.
72. Oliveira, J.; Carvalho, G.; Cabral, B.; Bernardino, J. Failure Mode and Effect Analysis for Cyber-Physical Systems. *Future Internet* **2020**, *12*, 205. [CrossRef]
73. Sestino, A.; Prete, M.I.; Piper, L.; Guido, G. Internet of Things and Big Data as Enablers for Business Digitalization Strategies. *Technovation* **2020**, *98*, 102173. [CrossRef]
74. Kavallieratos, G.; Katsikas, S. Managing Cyber Security Risks of the Cyber-Enabled Ship. *J. Mar. Sci. Eng.* **2020**, *8*, 768. [CrossRef]

75. Elizaveta, G.; Tjasa, I. Regulatory Sandboxes (Experimental Legal) Regimes for Digital Innovations in Brics. *BRICS Law J.* **2020**, *7*, 10–36.
76. JET Tech. Security in the Age of Digital Disruption. *J. Environ. Treat. Tech.* **2020**, *8*, 259–261.
77. Bocayuva, M. Cybersecurity in the European Union Port Sector in Light of the Digital Transformation and the COVID-19 Pandemic. *WMU J. Marit. Aff.* **2021**, *20*, 1–20. [CrossRef]
78. Lee, I. Cybersecurity: Risk Management Framework and Investment Cost Analysis. *Bus. Horizons* **2021**, *64*, 659–671. [CrossRef]
79. Krafft, M.; Kumar, V.; Harmeling, C.; Singh, S.; Zhu, T.; Chen, J.; Duncan, T.; Fortin, W.; Rosa, E. Insight Is Power: Understanding the Terms of the Consumer-Firm Data Exchange. *J. Retail.* **2021**, *97*, 133–149. [CrossRef]
80. Dobrolyubova, E. Measuring Outcomes of Digital Transformation in Public Administration: Literature Review and Possible Steps Forward. Network of Institutes and Schools of Public Administration in Central and Eastern Europe. *NISPAcee J. Public Adm. Policy* **2021**, *14*, 61–86.
81. Spivakovskyy, S.; Kochubei, O.; Shebanina, O.; Sokhatska, O.; Yaroshenko, I.; Nych, T. The Impact of Digital Transformation on the Economic Security of Ukraine. *Stud. Appl. Econ.* **2021**, *39*, 10. [CrossRef]
82. Creazza, A.; Colicchia, C.; Spiezia, S.; Dallari, F. Who Cares? Supply Chain Managers' Perceptions Regarding Cyber Supply Chain Risk Management in the Digital Transformation Era. *Supply Chain. Manag. Int. J.* **2021**, *27*, 30–53. [CrossRef]
83. Landis, R.J. The Measurement of Observer Agreements for Categorical Data. *Biometrice* **1977**, *33*, 159–174. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.