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, Alexandre de Paula Pereira

Posted Date: 5 November 2024

doi: 10.20944/preprints202411.0339.v1

Keywords: Digital Transformation; Digital Technology; Risk; Risk Identification; Risk Classification

 doi:10.20944/preprints202411.0339.v1

Article

Information Security Risk Framework for Digital Transformation Technologies

Eduardo Stefani *,†, Ivanir Costa †, Marcos Antonio Gaspar †, Roberto de Souza Goes †, Rogério 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

* Correspondence: eduardo_stefani@uni9.edu.br

† These authors contributed equally to this work.

Abstract: The increasing impact of digital technologies on society, marked by rapid and disruptive changes, including more efficient and modern processes, is pushing companies to adopt digital solutions. However, companies have limited options, and they can rarely avoid being affected by the speed and challenges introduced by digital technologies. Researchers have observed that the cybersecurity risks associated with these technologies are not fully apparent, despite the advantages they bring. In this context, this study aims to uncover the associated risks of using Digital Transformation technologies, which may lead to outcomes that fall short of initial expectations. A systematic literature review was conducted as the research methodology, involving a search for scientific articles in bibliographic databases 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 questionnaire, thereby aligning the systematic literature review with market realities regarding the risks companies are exposed to when using digital technologies. As a contribution to both the industry and academia, this work offers a framework to support companies in their Digital Transformation journey, 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

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 that they are rarely able to shield themselves from the growing competition and challenges brought by digital technologies [4].

Digital Transformation (DT), as a process that encompasses the digitalization of companies, including products, services, and the creation of value through the implementation of various technologies [5], has resulted in a landscape of changes, which includes the evolution of information technologies, the 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

 doi:10.20944/preprints202411.0339.v1

agendas and emphasize the importance that digital technologies play in the current context, as they are faced with the need to use them as efficiently as possible [2], given that they are everywhere, 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, 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 will manage the increasing speed and risks imposed by new and disruptive technologies [6]. It 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 [16]. Risk can be understood as the possibility of an event having unexpected outcomes, the uncertainty of the unknown, or how its effects are perceived [17]. It is the probability of a variation from an expected result [18]. Additionally, companies are exposed to risks that may cause unexpected disruptions due to strikes, natural disasters, or supplier failures [19]. With an increase in complexity, DT has elevated this topic to a new level, with the introduction of systemic and structural risks [20].

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 academic worlds, but it remains a challenge to have a clear, precise, and unified definition of it [9]. A significant part of the difficulty in reaching an exact meaning for this topic is the fact that DT has a multidisciplinary perspective [21]. 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 [22].

In this perspective, the human component is an aspect of DT, both in terms of means and objectives [21]. The integrated use of these digital technologies changes the way individuals work and has the ultimate goal of improving the material conditions of society [22].

Based on interviews with executives, there is confusion in defining the term "digital," as it is something 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 been incorporated into this term.

The multidisciplinary perspective of DT takes society's point of view into account [16]. In this way, the opportunities that come with this revolution are important, but they 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 [23].

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

 doi:10.20944/preprints202411.0339.v1

2.2. Digital Transformation Technologies

The innovation behind DT is 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 [21], the evolutionary process that has occurred in recent decades, starting from informatics to the information society, paved the way for an event as impactful as DT [24].

As an example, it is possible to list some technologies, such as the IoT, cloud computing, big data, cyber-physical systems, virtual and augmented reality, and finally, AI [25]. This last one, in particular, poses some challenges, since its ultimate goal is the creation of an algorithm capable of solving problems and performing cognitive tasks as well as or better than humans [23].

The robotization of processes is a technology that deserves attention, and it does not replace AI or machine learning, but it is capable of performing automatic and repetitive tasks, such as data mining, for example [26].

Regarding cloud technology, other mechanisms, such as the IoT, store data and rely on the cloud to achieve the integration that DT has been providing, which permeates both citizens and companies [27].

As can be observed, the universe of available technologies is very broad, which is why a static definition of them would be somewhat incomplete. It is important to note that the technologies that cause concern today will, in a few years, be fully integrated into the lives of citizens and companies, thus no longer representing a threat. Likewise, the hypothetical risks associated with technologies like 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 [20].

2.3. Risks Associated with the Use of Digital Technologies

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 [21]. 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 risks associated with them.

Risk has always accompanied humanity, but in some way, it has been managed [16]. Regarding DT, it brings systemic and structural risks, such as economic security, which stems from the dependence on technologies from other countries, and the lack of foundational elements needed to build them [20]. The integration of this process with third-party technologies presents a source of danger [28]. This increases cybersecurity risks and their complexity, as a vulnerability 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 [16].

AI can bring risks and challenges that are difficult to calculate, which may cause unprecedented uncertainties [20]. In short, it is about the difficulty of clearly predicting the risks involved in the use of AI across various sectors of society. Drastic scenarios can be envisioned, such as the loss of control over military systems, but there are simpler horizons that include the challenge of establishing laws and regulations for the proper use of such technologies without becoming a risk.

DT has added a new layer of risk, which is cyber-related, and it can experience a cascade effect from a natural event, such as a disaster, which may trigger unexpected impacts on the infrastructure supporting digital technologies [28]. For example, a prolonged power outage can directly affect the continuity of data centers.

The possibility of a cascading effect 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 [29].

 doi:10.20944/preprints202411.0339.v1

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 [30].

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 [31]. Ports are an integral part of it due to a global supply chain that includes integration with transportation, energy, and telecommunications networks [32]. IoT and the management of a large amount of data available in the cloud create a significant dependency on critical infrastructure [32]. As the cloud hosts an increasing volume of data, including sensitive data, concerns about potential cyberattacks targeting this data also rise [27].

In this way, it is possible to observe that these examples cover industries of different natures, but there are common points, such as the pursuit of competitiveness and DT (the means through which they are working to achieve this goal). The 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 [28].

The intensive use of digital technologies can increase human risk and social vulnerability [33]. It involves recognizing that countries, companies, and citizens are not equal. According to these authors, 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 equal level at the starting point with more developed ones. This social vulnerability can marginalize entire regions and companies, making it very difficult for them to keep pace with the adoption of advanced technologies, thereby creating what is known as the digital divide [33].

Risk may exist in the process of concentration of digital platforms and the high investment in innovation that these industries require, such as cloud computing. 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 [34].

3. Systematic Literature Review

To allow a unbiased data collection in a situation where the results are unpredictable [35], this work is structured with a systematic literature review – conducted through searches in the bibliographic databases Web of Science and SCOPUS, which provide the theoretical foundation of the research, providing the state of the art on the risks that the use of DT technologies brings to companies. It is structured following the PRISMA method (Preferred Reporting Items for Systematic Review and Meta-Analysis) [36], 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 includes inclusion and exclusion criteria [37]. These criteria provide an objective way to determine whether the materials resulting from the searches are relevant to the central theme of the research and place the present study within ongoing discussions in the existing literature.

3.1. Searches in the Bibliographic Databases

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

Table 1. Search Expression.

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

 doi:10.20944/preprints202411.0339.v1

The search terms were adjusted to provide research involving DT with the risk of digital technologies; therefore, the term "risks" is mandatory. Words like privacy, breach, leakage, mitigation, and security expand the search, as they are related to risks. It's 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 mentioned databases, the inclusion and exclusion criteria were applied to the publications [37]. Table 2 presents the inclusion and exclusion criteria, along with comments.

Table 2. 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.

Two principles guided the literature review of 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 if the work met the established criteria;
- Data Collection with Evidence: as it was observed that the work met the established criteria, relevant data were captured, including notes to support important statements and elements.

Using the PRISMA method (Preferred Reporting Items for Systematic Review and Meta-Analysis) [36], the systematic literature review resulted in the sample presented in Figure 1.

3.3. PRISMA Method

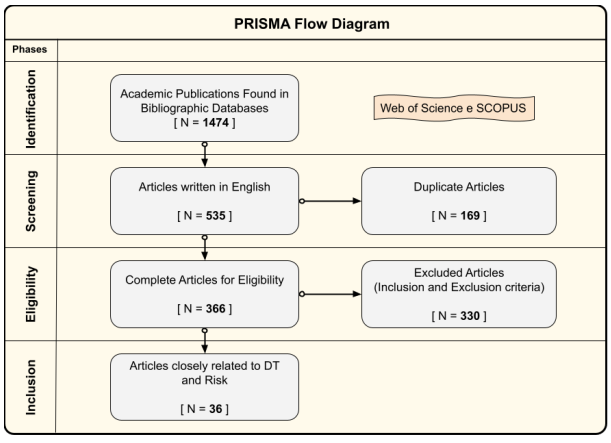

Figure 1. PRISMA Flow Diagram.

 doi:10.20944/preprints202411.0339.v1

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

4.1. Risks 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. It is known that these risks exist, but the literature review enabled the selection of risks connected to reality, which 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 [21].

The inclusion and exclusion criteria (Table 2) of the PRISMA method selected 36 (thirty-six) academic articles that are entirely related, meaning the research efforts are directly dedicated to risks of digital technologies. Twenty-one (21) risks were identified, which are associated with the use of digital technologies and can be observed in Table 3, listed and sorted by the number of occurrences, resulting in 36.

Table 3. 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

The risks, starting from the Identification column, are classified by letters ranging from "a" to "u," thus covering the 21 (twenty-one) risks observed in the systematic review, which will assist in the reading of Table 4, which relates the risks and their respective authors.

 doi:10.20944/preprints202411.0339.v1

Table 4. Authors x Risks.

Authors	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
[34]	✓																				
[38]	✓																				
[39]						✓															
[40]	✓																				
[41]	✓																				
[42]	✓																				
[43]					✓	✓															
[44]	✓			✓		✓	✓		✓				✓		✓	✓	✓	✓			
[45]														✓							
[46]		✓	✓																		
[47]	✓	✓				✓									✓						
[48]		✓																			
[49]	✓																				
[50]				✓																	
[23]	✓																				
[51]	✓																				
[52]		✓																			
[28]		✓																			
[32]			✓																		
[27]	✓			✓		✓		✓													
[7]	✓																				
[53]		✓																			
[54]											✓								✓		
[55]	✓			✓																	
[56]								✓			✓			✓						✓	✓
[57]	✓							✓		✓											
[58]	✓																				
[59]		✓	✓				✓		✓			✓									
[20]			✓	✓	✓																
[60]			✓																		
[61]	✓		✓		✓		✓		✓		✓	✓	✓								
[62]	✓			✓				✓		✓											
[63]	✓			✓																	
[64]			✓																		
[65]					✓																
[66]		✓	✓		✓		✓			✓											
Total	**18**	**8**	**8**	**7**	**5**	**5**	**4**	**4**	**3**	**3**	**3**	**2**	**2**	**2**	**2**	**1**	**1**	**1**	**1**	**1**	**1**

In light of the identified risks and to select the most relevant ones, a Curve ABC is applied since it is widely used in companies to classify information from various sources [67]. This tool is important because, among all the identified risks, some have a low number of occurrences in the reviewed articles, indicating that they are of low relevance. On the other hand, there are those that were frequently cited and deserve a more in-depth analysis. To differentiate them, the classification was done as follows: the most relevant items are categorized as A, those of medium importance are classified as B, and finally, those of low importance are classified as C. It is worth noting that the ABC classification concept is used in various applications both in professional and personal perspectives [68].

 doi:10.20944/preprints202411.0339.v1

One aspect of the ABC Curve that must be observed 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) [69]. 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 make up the A items, 17% the B items, and finally 9% the C items [69].

Table 5 presents the classification of the most cited risks, leading to a result of eight most relevant risks, classified as A, representing 70% of the total of eighty-two citations in the academic articles researched and selected.

Table 5. 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

4.2. Proposed Framework

Based on the selection criteria adopted and for the purposes of this work, the framework will be composed with the risks deemed most relevant and classified as such by the ABC Curve. Figure 2 graphically represents the proposed framework.

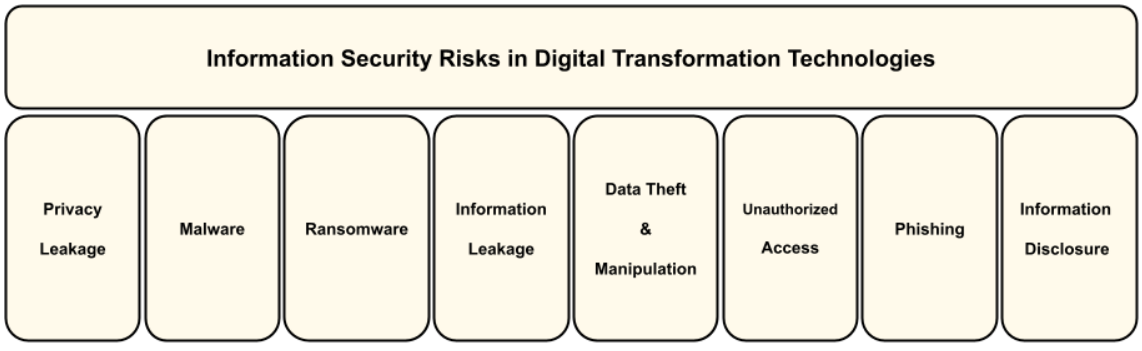

Figure 2. Proposed Framework - Graphical Representation.

 doi:10.20944/preprints202411.0339.v1

These are 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 smart devices used, the digital services consumed, or even the places visited, 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 the personalized and monetized services offered to people [57].
b. **Malware:** It is the main tool cybercriminals use to attack digital systems. It is a malicious computer program that includes viruses, worms, trojans, backdoors, and rootkits [53].
c. **Ransomware:** The connected world provides new opportunities for cybercriminals who collect personal data for fraudulent transactions or introduce ransomware – a malicious computer program that locks or encrypts devices, demanding money in exchange for the decryption key [64].
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 [20].
e. **Data Theft/Manipulation:** A user has sensitive data stored in a cloud solution consisting of multiple servers. An attacker may act to gain unauthorized access to their information, such as stealing data, destroying, or corrupting it in a way that renders it unusable by the user [70].
f. **Unauthorized Access:** In a bank account, only the account holder should access it, or a bank employee assisting the owner with specific transactions. No one else should have access. Once accessed by others, data confidentiality is compromised, which is irreversible [27].
g. **Phishing:** There are various definitions of the term phishing 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 use and context. It involves impersonating the recipient to achieve a desired action by the attacker [71], such as sending electronic messages to specific targets.
h. **Information Disclosure:** It is the joint action between platforms, providers, and consumers to reveal information about users, products, and services through a digital platform [72].

5. 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. These answers are valuable as they reflect the specialists' perceptions on the subject. It is worth noting that the risk framework was constructed from a systematic literature review, and the validation by specialists ensures the framework aligns with market realities, incorporating their insights on the risks associated with the use of digital technologies. This validation facilitates a mutual contribution between 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 the framework as a resource for companies navigating the digital transformation journey.

The questionnaire, which utilized a Likert scale, provided raw data enabling identification of the number of respondents selecting a specific scale for each statement, such as how many chose "Agree" or "Disagree." From this data, it is possible to determine the percentage of responses for each statement. With these numbers, the next step is to determine which responses indicate the framework's alignment with market realities. The research criterion assumed that "Agree" and "Strongly Agree" indicate this alignment; thus, these two scales are measured. This process yields two results that enable conditions for analysis. The simple average of each response was chosen, summing the percentages of each scale and calculating the simple average. When there is a set of raw data presented in tables or graphs, one sums the values and divides by the number of data points, defining a simple average [73].

 doi:10.20944/preprints202411.0339.v1

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

For each risk, graphs were generated with colors representing the number of respondents choosing one of the options for each statement related to the risk, which were converted into percentages 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 total agreement in percentage terms. These legends facilitate understanding by clearly relating the respondent count to the corresponding percentage of agreement. These graphs are presented for each of the risks discussed in this framework validation.

5.1. Privacy Leakage

As shown in Figure 3, 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.

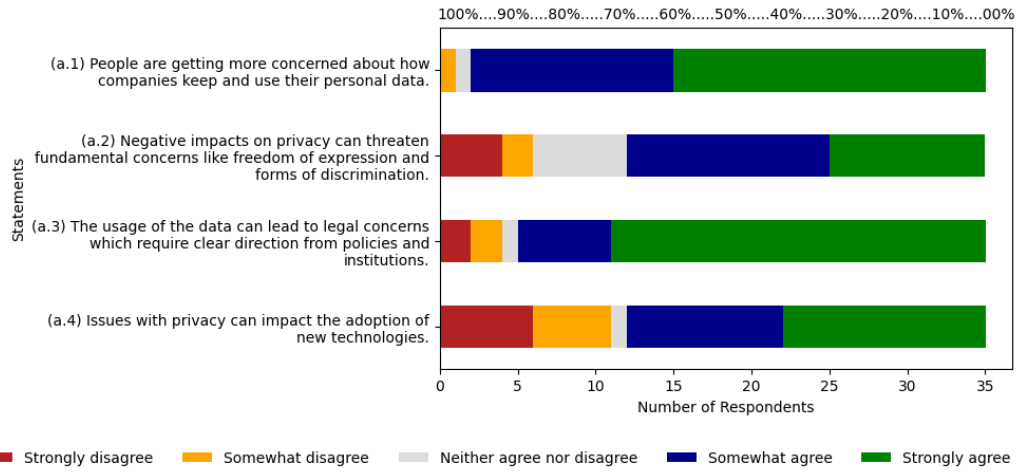

Figure 3. Likert Scale - Privacy Leakage.

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.

5.2. Malware

As shown in Figure 4, 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

 doi:10.20944/preprints202411.0339.v1

neutral present 6%, 14%, and 20% respectively. The agree scale has an average of 32%, along with an average of 38% for strongly agree.

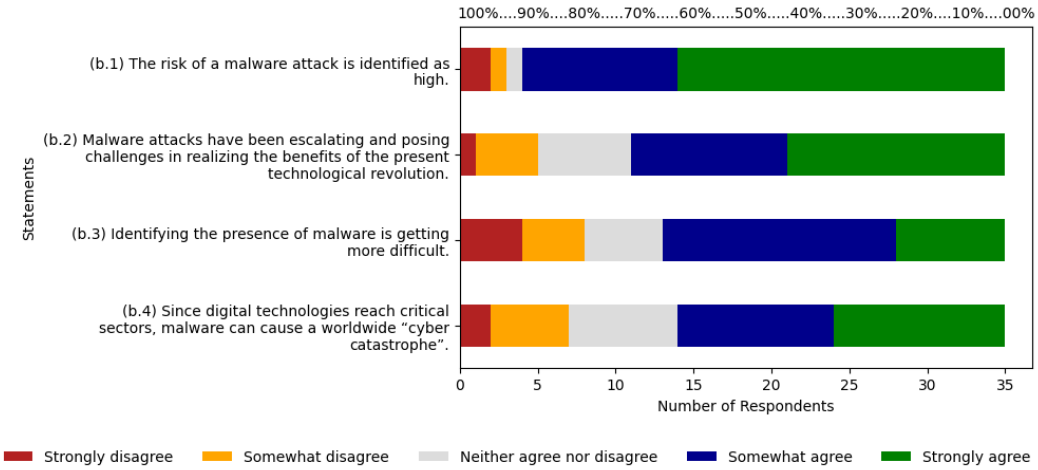

Figure 4. Likert Scale - Malware.

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, respondents indicate 70% agreement with the risk, also indicating it is a relevant risk.

5.3. Ransomware

According to Figure 5, 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.

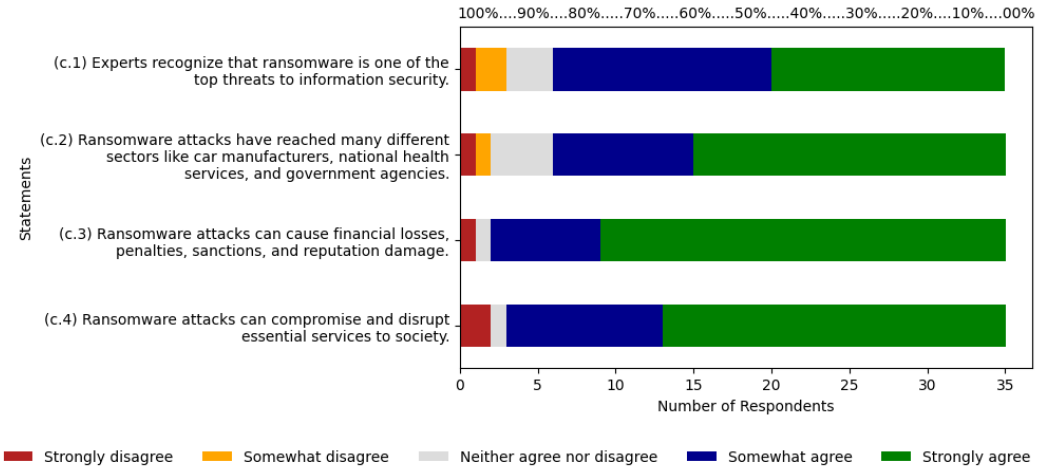

Figure 5. Likert Scale - Ransomware.

 doi:10.20944/preprints202411.0339.v1

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, respondents indicated 88% agreement with the risk, thus indicating it is a relevant risk.

5.4. Information Leakage

As shown in Figure 6, 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.

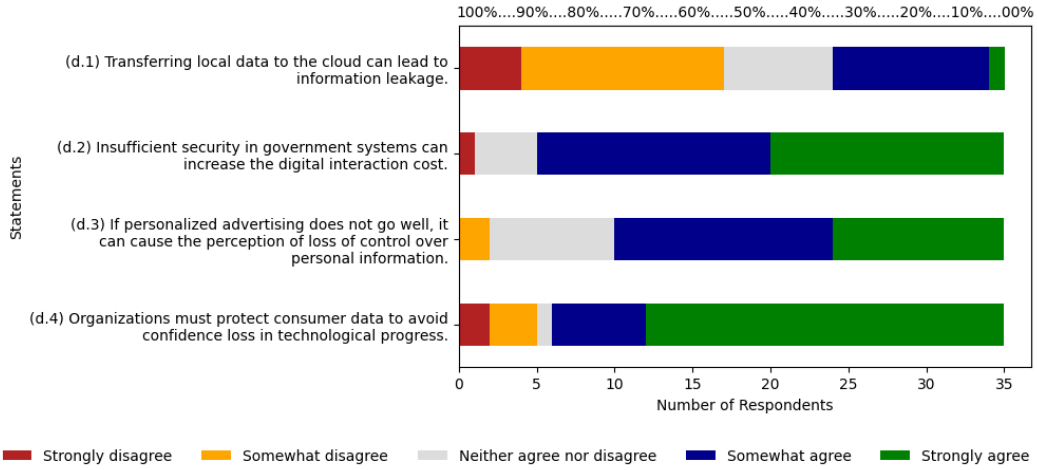

Figure 6. Likert Scale - Information Leakage.

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. It indicates the risk is not relevant for the specialists.

5.5. Data Theft/Manipulation

According to Figure 7, 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.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 November 2024 doi:10.20944/preprints202411.0339.v1

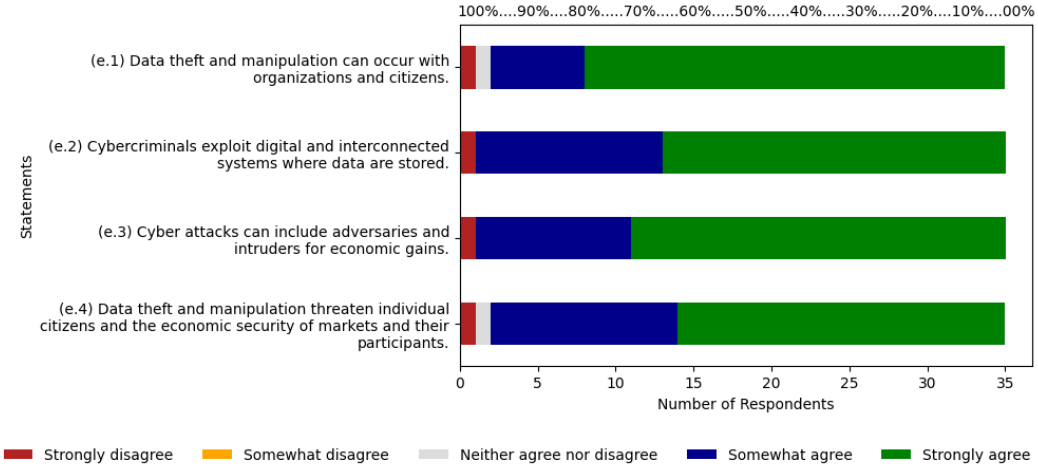

Figure 7. Likert Scale - Data Theft/Manipulation.

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, respondents indicated 96% agreement with the risk, thus indicating it is a relevant risk.

5.6. Unauthorized Access

As shown in Figure 8, 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.

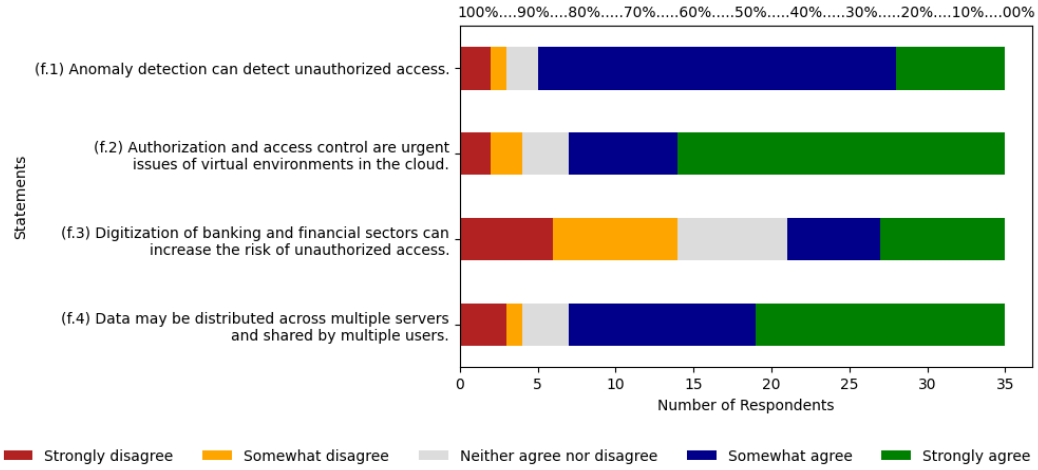

Figure 8. Likert Scale - Unauthorized Access.

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, respondents indicated 71% agreement with the risk, thus indicating it is a relevant risk.

 doi:10.20944/preprints202411.0339.v1

5.7. Phishing

According to Figure 9, 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.

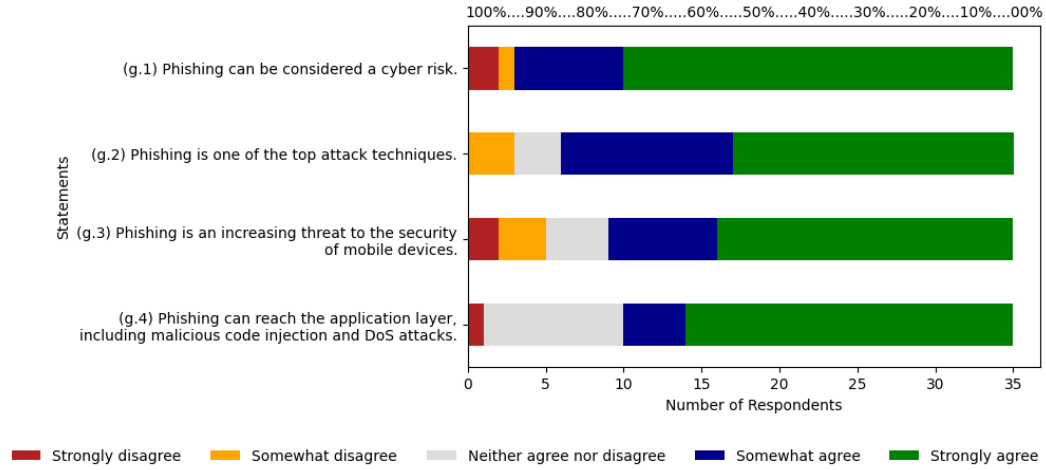

Figure 9. Likert Scale - Phishing.

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, respondents indicated 80% agreement with the risk, thus considering it is a relevant risk.

5.8. Information Disclosure

As shown in Figure 10, 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.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 November 2024 doi:10.20944/preprints202411.0339.v1

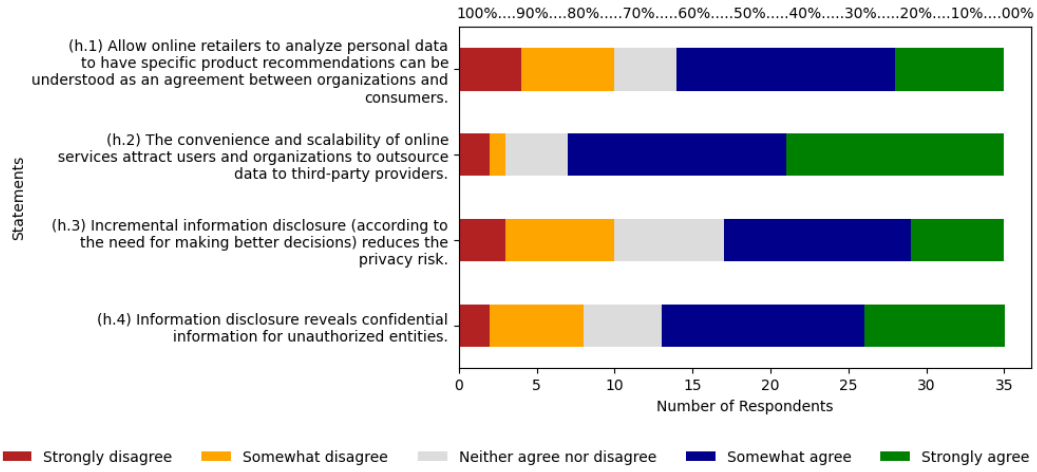

Figure 10. Likert Scale - Information Disclosure.

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. It means the specialists do not consider it as a relevant risk.

6. Conclusions

DT 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 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. Thus, tasks that were once performed physically are now predominantly digital.

In this way, more profit and competitive advantage are expected for companies, better prices and higher quality products and services for consumers, improved quality of life, and ultimately, work for people. There is hope in this, because with the use of technologies, the expectation is for more comfort, security, and free time for pleasurable activities. This is something that individuals seek with the use of technology, as they 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.

Even with these expectations, reality may show another face. Due to the rapid and disruptive change that DT is triggering, companies are unable to adapt. However, competitive advantage does not come unconditionally just from the use of technologies, and companies disappear from the market in a few years [74]. As a result, people become frustrated because they lose their jobs, and as consumers, they feel insecure due to privacy issues as they share their personal data with the remaining companies. Thus, risk replaces expectation. Consequently, citizens and companies 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, but to all disruptive changes that have occurred in the past. 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, which should be considered more carefully to get the most out of this great disruption.

It is important to emphasize that the risk is not trivial and has several dimensions. It is not only the risk of invasion of a company's servers or a domestic router. This risk exists but is already

 doi:10.20944/preprints202411.0339.v1

well-addressed by current tools. There are several models and tools that address risks in specific applications and equipment.

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

7. Contributions

This work offers three perspectives of contribution. The first is an immediate contribution to academia, expanding the theory on the risks associated with the use of digital technologies. The topic is not trivial because it 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 is to expand this field of study concerning the side effects of using digital technologies.

The second contribution is providing 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 in the future.

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

8. Limitations

This work, made possible through a systematic literature review, focuses on the risks of digital technologies and their effects on private companies. However, the work does not cover systemic, social, or human risks, nor those that impact the national security of countries. It also does not include public companies, governments, governmental bodies, non-governmental organizations, individual citizens, or even society as a whole.

9. Future Research

The future work that this research enables is to create a model for risk prioritization and mitigation using the proposed and evaluated framework as a starting point. The research can be expanded beyond private companies, including public companies or even governments, governmental bodies, or non-governmental organizations. This expansion of the research will support them on their DT journey, considering the risks in the context of governments and society. Additionally, it is suggested as future work to expand the research to cover risks of other types, such as social, human, and those impacting national security. This would extend the research beyond the risks of digital technologies and 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 future work suggestion is to revisit the risks of Information Leakage and Information Disclosure, as these presented some contradictions among the respondents in the field research.

Author Contributions: Conceptualization, E.C 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.

 doi:10.20944/preprints202411.0339.v1

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.

References

1. Bharadwaj, A.; El Sawy, O.A.; Pavlou, P.A.; Venkatraman, N. Digital Business Strategy: Toward a next Generation of Insights. MIS quarterly 2013, 471–482.
2. Schneider, S.; Kokshagina, O. Digital Transformation: What We Have Learned (Thus Far) and What Is Next. Creativity and Innovation Management 2020.
3. Fernandes, A.A.; Diniz, J.L.; Abreu, D., Vladimir Ferraz de Emiliano de Souza; H. Paiva Tonon, D.; Brito da Silva, E.; Costa, I.; Cardoso de Oliveira, J.; Alberto de Seixas, J.; Leão, L.; Carvalho Francisco, M.; et al. Governança Digital 4.0. 2019.
4. Al-Debei, M.M.; Avison, D. Developing a Unified Framework of the Business Model Concept. European journal of information systems 2010, 19, 359–376.
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); IEEE, 2021; pp. 159–166.
6. Vial, G. Understanding Digital Transformation: A Review and a Research Agenda. The Journal of Strategic Information Systems 2019, 28, 118–144.
7. El-Haddadeh, R. Digital Innovation Dynamics Influence on Organisational Adoption: The Case of Cloud Computing Services. Information Systems Frontiers 2020, 22, 985–999.
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. Journal of Management Studies 2021, 58, 1159–1197.
9. Morakanyane, R.; Grace, A.A.; O'Reilly, P. Conceptualizing Digital Transformation in Business Organizations: A Systematic Review of Literature. Bled eConference 2017, 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. Journal of Marketing 2016, 80, 146–172.
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. Journal of Interactive Marketing 2017, 40, 1–8.
12. Colbert, A.; Yee, N.; George, G. The Digital Workforce and the Workplace of the Future. 2016.
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), 2019; pp. 130–143.
14. Xia, F.; Liu, L.; Li, J.; Ma, J.; Vasilakos, A.V. Socially Aware Networking: A Survey. IEEE Systems Journal 2013, 9, 904–921.
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.
16. 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. Journal of the Knowledge Economy 2021, 1–24.
17. Lemos, F. On the Definition of Risk. Journal of risk management in financial institutions 2020, 13, 266–278.
18. Spekman, R.E.; Davis, E.W. Risky Business: Expanding the Discussion on Risk and the Extended Enterprise. International Journal of Physical Distribution & Logistics Management 2004.
19. Librantz, A.F.H.; Costa, I.; Spinola, M. de M.; de Oliveira Neto, G.C.; Zerbinatti, L. Risk Assessment in Software Supply Chains Using the Bayesian Method. International Journal of Production Research 2021, 59, 6758–6775.

 doi:10.20944/preprints202411.0339.v1

20. Gaivoronskaya, Y.V.; Mamychev, A.Y.; Petrova, D.A.; Rusanova, I.O. Typology of Risks and Threats Caused by Digitalization. Revista TURISMO: Estudos e Práticas 2020.
21. Hausberg, J.; Liere-Netheler, K.; Packmohr, S.; Pakura, S.; Vogelsang, K. Digital Transformation in Business Research: A Systematic Literature Review and Analysis. Proceedings of DRUID18 2018.
22. 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 Management 2020, 50, 136–160.
23. O'Leary, T.; Armfield, T. Adapting to the Digital Transformation. Alta. L. Rev. 2020, 58, 249.
24. de Araujo, R.F.; Oliveira, M.; others 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 em Revista 2017, 13.
25. 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); IEEE, 2016; pp. 407–410.
26. Siderska, J. Robotic Process Automation - a Driver of Digital Transformation? Engineering Management in Production and Services 2020, 12, 21–31.
27. Yang, P.; Xiong, N.; Ren, J. Data Security and Privacy Protection for Cloud Storage: A Survey. IEEE Access 2020, 8, 131723–131740.
28. Panda, A.; Bower, A. Cyber Security and the Disaster Resilience Framework. International Journal of Disaster Resilience in the Built Environment 2020.
29. HR3162 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001. 2001.
30. DHS The National Strategy to Secure Cyberspace 2003.
31. Owen, R.S. Infrastructures of Cyber Warfare. In Cyber warfare and cyber terrorism; IGI Global, 2007; pp. 35–41.
32. de la Peña Zarzuelo, I. Cybersecurity in Ports and Maritime Industry: Reasons for Raising Awareness on This Issue. Transport Policy 2021, 100, 1–4.
33. 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.
34. Nuccio, M.; Guerzoni, M. Big Data: Hell or Heaven? Digital Platforms and Market Power in the Data-Driven Economy. Competition and Change 2019, 23, 312–328.
35. Bryman, A. Integrating Quantitative and Qualitative Research: How Is It Done? Qualitative research 2006, 6, 97–113.
36. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G.; others Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. Int J Surg 2010, 8, 336–341.
37. Liao, Y.; Deschamps, F.; Loures, E. de F.R.; Ramos, L.F.P. Past, Present and Future of Industry 4.0 - a Systematic Literature Review and Research Agenda Proposal. International journal of production research 2017, 55, 3609–3629.
38. Riyana, S.; Natwichai, J. Privacy Preservation for Recommendation Databases. Service Oriented Computing and Applications 2018, 12, 259–273.
39. Vasil'ev, Y.S.; Zegzhda, D.P.; Poltavtseva, M.A. Problems of Security in Digital Production and Its Resistance to Cyber Threats. Automatic Control and Computer Sciences 2018, 52, 1090–1100.
40. 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. Interdisciplinary Description of Complex Systems: INDECS 2018, 16, 384–396.
41. Rossi, E.; Rubattino, C.; Viscusi, G. Big Data Use and Challenges: Insights from Two Internet-Mediated Surveys. Computers 2019, 8, 73.
42. 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.
43. Khanboubi, F.; Boulmakoul, A. Digital Transformation in the Banking Sector: Surveys Exploration and Analytics. International Journal of Information Systems and Change Management 2019, 11, 93–127.
44. Mendhurwar, S.; Mishra, R. Integration of Social and IoT Technologies: Architectural Framework for Digital Transformation and Cyber Security Challenges. Enterprise Information Systems 2021, 15, 565–584.

 doi:10.20944/preprints202411.0339.v1

45. Baghdasarin, D. MRO Cybersecurity SWOT. International Journal of Aviation, Aeronautics, and Aerospace 2019, 6, 9.
46. 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.
47. Shi, J.; Jin, L.; Li, J. The Integration of Azure Sphere and Azure Cloud Services for Internet of Things. Applied Sciences 2019, 9, 2746.
48. Alharbi, S.A. A Qualitative Study on Security Operations Centers in Saudi Arabia: Challenges and Research Directions. Journal of Theoretical and Applied Information Technology 2020, 98.
49. 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. Human Systems Management 2020, 1–17.
50. Park, S.-T.; Li, G.; Hong, J.-C. A Study on Smart Factory-Based Ambient Intelligence Context-Aware Intrusion Detection System Using Machine Learning. Journal of Ambient Intelligence and Humanized Computing 2020, 11, 1405–1412.
51. Puraite, A.; Zuzevičiūtė, V.; Bereikienė, D.; Skrypko, T.; Shmorgun, L. Algorithmic Governance in Public Sector: Is Digitization a Key to Effective Management. 2020.
52. Kabbas, A.; Alharthi, A.; Munshi, A. Artificial Intelligence Applications in Cybersecurity. International Journal of Computer Science and Network Security 2020, 20, 120–124.
53. 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. Computers & Electrical Engineering 2020, 88, 106825.
54. Oliveira, J.; Carvalho, G.; Cabral, B.; Bernardino, J. Failure Mode and Effect Analysis for Cyber-Physical Systems. Future Internet 2020, 12, 205.
55. Sestino, A.; Prete, M.I.; Piper, L.; Guido, G. Internet of Things and Big Data as Enablers for Business Digitalization Strategies. Technovation 2020, 102173.
56. Kavallieratos, G.; Katsikas, S. Managing Cyber Security Risks of the Cyber-Enabled Ship. Journal of Marine Science and Engineering 2020, 8, 768.
57. Bhattacharjee, K.; Chen, M.; Dasgupta, A. Privacy-Preserving Data Visualization: Reflections on the State of the Art and Research Opportunities. In Proceedings of the Computer Graphics Forum; Wiley Online Library, 2020; Vol. 39, pp. 675–692.
58. Elizaveta, G.; Tjasa, I. Regulatory Sandboxes (Experimental Legal) Regimes for Digital Innovations in Brics. BRICS Law Journal 2020, 7.
59. Tech, J.E.T. Security in the Age of Digital Disruption. Journal of Environmental Treatment Techniques 2020, 8, 259–261.
60. Bocayuva, M. Cybersecurity in the European Union Port Sector in Light of the Digital Transformation and the COVID-19 Pandemic. WMU Journal of Maritime Affairs 2021, 1–20.
61. Lee, I. Cybersecurity: Risk Management Framework and Investment Cost Analysis. Business Horizons 2021.
62. 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. Journal of Retailing 2021, 97, 133–149.
63. 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. The NISPAcee Journal of Public Administration and Policy 2021, 14, 61–86.
64. Chalyuk, Y.; Dovhanyk, N.; Kurbala, N.; Komarova, K.; Kovalchuk, N. The Digital Economy in a Global Environment. 2021.
65. Spivakovskyy, S.; Kochubei, O.; Shebanina, O.; Sokhatska, O.; Yaroshenko, I.; Nych, T.; others The Impact of Digital Transformation on the Economic Security of Ukraine. 2021.
66. 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 Management: An International Journal 2021.
67. Ballou, R.H. Logística Empresarial: Transportes, Administração de Materiais e Distribuição Física; Atlas, 1993;
68. Alvarenga, A.C.; Novaes, A.G.N. Logística Aplicada: Suprimento e Distribuição Física; Editora Blucher, 2000;

 doi:10.20944/preprints202411.0339.v1

69. Pacchini, A.P.T.; others O Grau de Prontidão Das Empresas Industriais Para Implantação Da Indústria 4.0: Um Estudo No Setor Automotivo Brasileiro. 2019.
70. Xing, L.; Levitin, G. Balancing Theft and Corruption Threats by Data Partition in Cloud System with Independent Server Protection. Reliability Engineering & System Safety 2017, 167, 248–254.
71. Alkhalil, Z.; Hewage, C.; Nawaf, L.; Khan, I. Phishing Attacks: Recent Comprehensive Study and a New Anatomy. Frontiers in Computer Science 2021, 3, 6.
72. Xu, X.; Zeng, S.; He, Y. The Impact of Information Disclosure on Consumer Purchase Behavior on Sharing Economy Platform Airbnb. International Journal of Production Economics 2021, 231, 107846.
73. Cazorla, I.M.; dos Santos Santana, E.R.; Utsumi, M.C. O Campo Conceitual Da Média Aritmética: Uma Primeira Aproximação Conceitual. Revista Eletrônica de Educação Matemática 2019, 14, 1–21.
74. Harari, Y.N. 21 Lessons for the 21st Century; Random House, 2018.