THE DIGITAL DEFICIT OF THE NIS2 DIRECTIVE: REGULATORY TENSIONS THAT HINDER THE MANAGEMENT OF DIGITAL SECURITY RISKS

Raymond Bierens, Abbas Shahim and Svetlana Khapova

School of Business and Economics, Vrije Universiteit Amsterdam, De Boelelaan 1105, Amsterdam, The Netherlands

ABSTRACT

In 2024, the NIS2 Directive came into effect in Europe introducing specific measures, reporting obligations and personal liabilities to mitigate risks for societal digital disruption. We conducted an inductive study and interviewed 29 CISO's and IT or C-level executives from large, NIS2 affected, organizations in The Netherlands and validated the outcomes with 300^{+} cybersecurity professionals through various workshops. Our study reveals interrelated tensions in organizational behavior driven by the regulatory changes. It stimulates more compliance behavior amongst organizations and their suppliers which is being reinforced by its accountability and liability clauses. However, our study confirms that considerable residual risks remain due to the dynamic nature of technology, shifting security risks up the supply chain, and dependencies on global technology companies. Government is perceived as challenged in their ability to govern while being a critical factor to succesfullly transforming compliance behavior into digital security risk management to reduce residual risks.

KEYWORDS

NIS2 Directive, Policy, Organizational Risk, Personal Risk, Liability, Technology, Information Security, Cyber Security, Digital Risk, Risk Management

1. INTRODUCTION

Society's digital transformation introduces unprecedented digital security risks [1] due to its fast pace [2] and dynamic nature [3], that compels governments to respond [4]. Acting as coordinators and policy-setters [5], they must define clear roles, responsibilities and key processes for data management [6] and supply chains [7], particularly protecting national security and critical infrastructure [8]. Through digital transformation, organizations evolve into socio-technical ecosystems [9, 10], with interdependencies often extending beyond borders, drawing governments into the risk management process [11]. For multinational entities, these interdependencies add regulatory complexities to existing challenges in digital interdependence and information security[12].

To ensure organizations across Europe take the recommended "appropriate and proportionate technical and organizational measures", the European Parliament and Council agreed on July 6th, 2016, on Directive 2016/1148 [13] known as the first NIS Directive (or NIS1).As the first horizontal legislation undertaken at EU level for the protection of network and information systems across the Union [14], the NIS1 closely aligns with the digital security risk perspective

David C. Wyld et al. (Eds): COMIT, AISO, CRBL, WIMNET, EDUPT– 2025
pp. 01-20, 2025. CS & IT - CSCP 2025 DOI: 10.5121/csit.2025.151201

by defining its scope in article 4 as “any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data”.

A relevant risk of limited consistency and unnecessary complexity for all stakeholders emerged during the NIS1 implementation. The European Commission subsequently ordered an extensive study on the NIS1 in 2019 [15] whichout lined three main problem drivers: insufficient investment (due to many organizations being out of scope), inconsistent treatment of covered entities across EU Member States, and limited information-sharing and operational cooperation. The NIS1 was consequently deemed insufficient to reach a higher level of cyber resilience across EU Member States. On December 14th 2022, the European Parliament and Council therefore agreed on the update of the Directive 2022/2555 [16] on measures for a high common level of cybersecurity across the Union, also known as the NIS2 Directive or NIS2).

The NIS2 focusses on the actual execution of risk management on national, organizational, and even personal level. Compared to NIS1, more sectors and organizations were brought into scope [17, 18]. Roles for governments and organizations were also more specifically defined by prescribing measures focused on the reconnaissance phase of a cyberattack [19].Many operators, previously exempt by the NIS1 Directive, may now face new compliance challenges when operating in Europe. Companies that were already subject to NIS1 should also reassess their stance in order to limit their legal risks in the region[20]. In the Netherlands, the NIS2 will apply to between 10.600 and 11.600 organizations [21], while the NIS1 applied to an estimated 10% of that total.

From a behavior management perspective on security risk management, it is interesting that specific prescribed measures were deemed necessary to define what constitutes “appropriate and proportionate technical, operational and organizational measures to manage the risks”, as found by Michels & Walden [22] after researching the NIS1 effectiveness. From a digital risk perspective, it is also of interest that the term “operational” was added to the previous definition in the NIS1. To ensure every organization complies with these measures, new organizational and personal liabilities were also introduced under the NIS2.

Managing digital security risks requires people and technology from multiple public and private organizations (and possibly multiple countries) to work seamlessly together [23].The NIS2 additions, specifications and liabilities all seem to suggest that its primary focus is the risk management behavior of directors within and across EU Member States. However, while cognitive and cultural biases shape information security perceptions and behaviors [24], there is a gap in the literature on the relationship between directors and information security strategy [25].This is particularly relevant for the NIS2 which needs to be translated into local law by each individual EU Member State since it intertwines with national security which is outside of the governance mandate of the European Council [26].

Our inductive study prompts us to address the research gap within the “digital security risk management behavior” phenomenon. To accomplish this, we collected data via 29 interviews with Directors, Chief Information Officers (CIOs) and IT Directors, working in large organizations in the Netherlands. To some, the NIS1 already applies, while the NIS2 will apply to all once it becomes local law. Our understanding is that, although there is a “need to change” for security risk management behavior within society’s most critical organizations, there are tensions that hinder the implementation of new regulation to create higher levels of cyber resilience. These tensions are mainly determined by the digital context. We consolidated our research findings to a data structure based on the Gioia methodology [27], as shown in
Figure1, 2 and 3. To explain the data, we draw from management and organization theories that help describe the theoretical tensions presented in this paper.

This paper continues with a brief overview of related research. Then, after explaining our methods, we provide an in-depth analysis of our empirical findings describing three tensions. As our aim is to build theory, each tension includes a brief theoretical background. Next, we explain the theoretical tensions that exist in the digital security risk management implementation phenomenon. After citing supportive qualitative research to demonstrate the applicability of the identified tensions and their interrelatedness, the study concludes with a discussion of the implications of our findings and suggestions for future research that these findings present.

2. RELATED RESEARCH: DIGITAL SECURITY RISK MANAGEMENT

Research has steadily progressed from focusing on information security (confidentiality, integrity, availability) toward broader cybersecurity risk management, but is still at its infancy when it comes to digital security risk management [28, 29]. Digital security risk - encompassing IT, OT, and IoT - remains in an even more nascent stage[30].However, NIS2 defines "Network and Information Systems" as "any device or group of interconnected or related devices"[16], aligning with OECD's digital security risk definition[31].Additionally, "electronic communications network" is now defined in Article 2, point (1), of Directive (EU) 2018/1972, instead of point (a) of Article 2 of Directive 2002/21/EC[1] resulting in the added phrase "whether or not based on a permanent infrastructure or centralised administration capacity" which brings (cloud) outsourcing into the picture as well.

This raised the question how the risk management behavior of organizations is changing because of the new (or updated) regulatory frameworks like the NIS2? In this study, we bridge this gap and provide emprical insights on implementation tensions of risk management through regulatory frameworks. This can provide important insights for both researchers and practitioners, helping them to become aware of possible tensions in security risk management as well of coping strategies and practices to tackle these tensions. We believe that by providing this research lens on tensions we gradually help to build knowledge that offers a deeper understanding of the digital security risk management phenomenon.

3. METHODOLOGY

We applied a qualitative research approach to inductively develop the tensions in digital security risk management implementation. This approach is in line with the principles of an iterative approach to qualitative research – in particular, grounded theory. Concerning this inductive research approach, it may seem contradictory that we offer a brief overview of the relevant literature in each of the tensions presented in the findings section. Although we draw from different management theories to clarify and explain the tensions, as our vantage point we used a grounded theory approach to identify the tensions from our interview data, without being aware of the theories yet. To analyze our data, we applied the Gioia methodology, which comprises three different levels of abstraction and is tailored to inductive inquiry[27]. We began by openly coding, grouping, and classifying the individual descriptions that our informants provided as 'interview samples' to perform a first-order analysis. Our next step was to perform a second-order analysis by comparing these categories and examining the patterns that emerged. This analysis provided the basis on which we developed our third-order theoretical propositions e.g.

[1] *'electronic communications network' means transmission systems, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;*

the tensions. We created a data structure for each tension as described in the findings section below, as shown in
Figure1, 2 and 3.

3.1. Data Collection

The first author collected qualitative data in four stages between July 2023 and May 2025. In the first stage, from July 2023until May 2023,two different approaches were discussed with experts to independently collect the data, while awaiting the release of the NIS2 Directive on December 14th, 2022. In the second stage from June 2023 until November 2023 (6 months), 29 interviews were conducted. The interviews were conducted mainly face-to-face or in-person, were tape-recorded, and were fully transcribed. In total, the data sample includes 17 different companies as sometimes both the CISO and the C-level executives were independently interviewed. All semi-structured interviews were held in Dutch and between 35 and 60 min (an average of approximately 48 min).To build trust and to allow a higher probability of uncovering rich data, we ensured all interviewees' anonymity in the data analysis. Additionally, we strived for transparency, so the transcripts were sent back to the participants for review. If corrections to the transcript were suggested, they were primarily related to the use of popular language about the company, their boss or information about sensitive cases. This did not impact the data's richness as we are more interested in understanding the abstract level of security risk management tensions within the organizations. In the third stage, from January 2024 till June 2024, the outcomes were presented in three workshops to 265 cybersecurity professionals to discuss the tensions observed. In the final stage the outcomes were presented to 43 Dutch governmental officials who are responsible for the NIS2 implementation and translation into local legislation.

3.2. Research Context

Our empirical data are collected from large organizations in the Netherlands. The timing of the interviews and validation workshops is of particular importance since the Dutch Government did not release the local translation of the NIS2 (called the CyberBeveiligingsWet, short: CBW) until June 2024 which provided the researchers more insight into the risk management behavior of the informants due to the interbellum of the NIS2 being released while awaiting the local CBW.

Of the 17 organizations interviewed, 5 were already designated Critical National Infrastructure (CNI) representing three sectors: energy, (national) transportation and (national) healthcare. The sector wastewater was at the time of interview not appointed as CNI but has been so after the interviews were held. The NIS2 introduced two additional classifications on top of the existing CNI: essential and important organizations. It also expands the target organizations of the existing CNI sectors (energy, transportation, healthcare, and wastewater) and adds government as new essential sector. Table 1 shows both situations for the interviewed organizations per Dutch sector, before and after the implementation of the NIS2 takes place.

Table 1. Distribution of interviewed organizations before and after the NIS2 implementation,

Sector	**Under NIS1**			**Under NIS2**		
	CNI	**No Status**	**Total**	**CNI & Essential**	**Essential**	**Total**
Wastewater	2		**2**	2		**2**
Energy	2		**2**	2		**2**
Local Government		5	**5**		5	**5**
Transportation	2	2	**4**	4		**4**
Healthcare	1	3	**4**		4	**4**

Sector	Under NIS1			Under NIS2		
	CNI	No Status	Total	CNI & Essential	Essential	Total
Grand Total	**5**	**12**	**17**	**8**	**5**	**17**

In particular, the Netherlands is an interesting research context for this study. On the one hand, the Netherlands are ranked eighth in the World Digital Competitiveness Index[2]and has consistently been in the top 10 since 2020. On the other hand, the Netherlands is not a frontrunner in cybersecurity[3]. In this context, we expect to find rich data on implementation tensions in Dutch organizations. Additionally, we focus on large organizations with high risk profiles to society that with rapid digital transformation taking place in their sectors and organizations. This context makes it more likely for organizations to truly cope with digital security risk.

3.3. Research Process

We increased the analytical rigor by dividing our investigation into four subsequent research phases. In the first phase, two different approaches were discussed with experts to identify the organizations that would qualify to participate in the study. The first approach was a technology-driven selection based upon organizations that were using (or considering) asset management solutions to identify the scope of their security risks. However, since at the time of this research, asset management solutions are unable to identify assets as OT, IoT or IT, uncertainty appeared on the feasibility of the current solution to cover all the assets as mandated by the NIS2. Therefore, a second, risk-driven approach was chosen where 19 client organizations of a Dutch consulting firm were invited to participate with 13 accepting the invitation. The remaining 4 organizations were identified during the interviews held with the initial 13 and were not clients. After the initial introduction, the consulting firm has not been involved in the further identification of the interviewees at each organization or the outcome of each interview.Table 2 shows the roles for each of the informants that were interviewed in this stage. In the third stage, the outcomes were presented in various workshops to discuss the tensions observed. The first was with a group of 220 cybersecurity professionals which included several informants, the second was with 5 people from an advisory council to the Dutch Government and a third workshop with a 40 people representation from a Dutch Community on Cyberwarfare. The research was concluded in May 2025 with a final workshop with 43 governmental policy makers from the Dutch government who are responsible fordrafting the CBW from the NIS2. Due to the requested confidentiality, none of the workshops were recorded or transcribed but served to provide additional insights related to the tensions defined in this study.

Table 2. Informants interviewed in stage 2 of the study.

Sector	Director / GM	CISO / Security Advisor	IT Executive	Total
Wastewater	1	2	1	**4**
Energy	1	1	1	**3**
Local Government	3	6	1	**10**
Transportation	2	4	1	**7**
Healthcare	0	4	1	**5**
Grand Total	**7**	**17**	**5**	**29**

It was not until the end of our analysis and discussing the data that we could clearly identify the empirical story of the digital security risk management phenomenon and the theoretical tensions

[2]https://imd.widen.net/s/xvhldkrrkw/20241111-wcc-digital-report-2024-wipfound at https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/
[3]https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

that occur in relation to the implementation phase. This is where the role of the second and third authors contributed to the collaborative team as they adopted an outsider's perspective—a devil's advocate whose role was to critique interpretations [27].

4. FINDINGS

In our findings section, we present the theoretical tensions that were found in the data on the digital security risk management phenomenon. These tensions exist due to the increase of risks in the digital domain that 'forces' governments into pushing organizations to adopt their security approaches accordingly and quickly. The theoretical tensions reveal and explain why organizations have difficulties implementing digital security risk approaches. Sometimes these tensions even reveal that, due to a paradoxical situation, the organization will not achieve the desired digital security, with considerable residual risks remaining. We refer to informant quotes with the aim to carefully present our evidence of data-to-theory connections and show how data are aligned with the data structure, as shown in Figures1, 2 and 3. Anonymized interview identifiers are used to code direct quotes (Organization Number – Informant Number).

4.1. Tension 1: Compliance Management vs Risk Management

The first identified tension is related to a debate in the literature between compliance management and security risk management. As organisations increasingly need to comply with various laws and regulations, they have to verify the adequacy and effectiveness of their security controls through internal and external audits [32].A long-held assumption in literature is that managing compliance equals the management of digital security risks because auditable controls are seen as an effective way to influence the decision-making process through accountability and assurance [33]. The two theoretical constructs are therefore generally described as being "congruent" to one another. However, recent studies have challenged the congruent compliance-risk-management assumption and have shown it is more likely to be incongruent. For instance, documenting an organisation's current state is often difficult due to the complexity of its technological landscape, the complex regulatory and organisational environment, and the frequent changes to both [34, 35]. In real-world risk evaluation scenarios, it is difficult for analysts to determine the complex relationships among security controls [36]. We use this theoretical background to understand how the NIS2 may affect the management of risks within an organization.

4.1.1. Congruent View Between Compliance and Digital Security Risk Management

Compliance can be seen as a motivating factor in achieving better cybersecurity and staying vigilant in cybersecurity operations since regulations might guide and force the organization to improve [37]. Most of the informants find value in using sectoral compliance frameworks such as the NEN7510 (healthcare) and BIO[4] (local government, wastewater) that are often derived from international frameworks like ISO27001. Due to its focus on IT Security Risk Management, the wastewater sector created an additional, sector-specific, security risk framework to cover OT security risks called CSIR which is derived from the IEC62443 standard. Both BIO and CSIR were co-created by government and organizations within the sector, while the NEN7510 was drafted in collaboration between healthcare organizations and its industry. Many informants confirm research by Folorunso [38] where compliance to standards and regulations is seen as the goal instead of security:

"[…] In the end our strategy is to become NEN7510 compliant first" (15-25),
"[…] Our policy is to comply with BIO and CSIR" (11-18), and

[4]*Baseline for Information Security*

"[…] If we are compliant with BIO, we don't have to be very afraid for the NIS2" (04-06).

Though compliance to standards, best practices, and regulatory requirements can help reduce cyber risks, it does not guarantee that an organization will have strong cybersecurity [39]. Even worse, it may think (or even "stretch things") to appear compliant (and secure) to save costs – without much actual regard for security [33]. Some informants demonstrate awareness of this fact andadmit they have become victim to a checkbox-mentality [38]:

"[…] What are we managing? Compliance, security or risks?" (16-26),
"[…] Compliance is what we like best in the Netherlands while risk management is what we should want. […] But we live in a compliance country which then often becomes a goal in itself" (05-08),
and
"[…] The risk of interpretating NIS2 in this manner is that it becomes a bureaucracy which drives organizations towards compliance management instead of security or risk management" (07-12).

Organizations must balance the often resource-intensive process of maintaining compliance with the need for a proactive security strategy that addresses emerging cyber threats[38]:

"[…] The same amount of people will have to carry the additional burden of (NIS2) audits on top of their existing audits" (04-05)", and
"[…] It will mean more work, but I think they underestimate how much work goes into checking logs" (09-14).

4.1.2. Incongruent View Between Compliance and Digital Security Risk Management

Synergy was found in research by Marotta & Madnick who point out that if an organization has achieved compliance, it might neglect important aspects of security that have not been addressed thus putting itself at risk [33]. Participating CNI organizations in the study that were already subject to the NIS1 (Energy, Transportation) consider themselves high-risk environments that require high reliability and security on all types of risks including digital. Their informants take a different starting point for managing digital security risks:

"[…] My first priority as a CISO is: make sure nobody gets killed" (10-17), and
"[…] If you look at our risk strategies, you'll find cyber and digital safety on number 1 and 2" (13-22).

Theories on cyber norms point out that creating and maintaining cyber norms as the basis for a security risk framework comes takes time [40]. Informants confirm the existence of a "pacing problem" identified by Boeken where technologyevolves faster than law leaving a gap where there is a lack of legislation and enforcement for new technologies which strengthen security blind-spots created by a strong focus on compliance [41].

"[…] It remains dynamic and for me that is still an important and difficult topic. Just try to keep a framework up-to-date after an incident like Log4J, […] it'll be five years later"" (15-25),
"[…] The NIS2 is only successful if it's dynamic by nature" (08-11),
"[…] Rapid changes in technology can mean that you are never completely in sync in terms of authority and measures" (05-07), and
'[…] OT, IoT? […]that's four steps back in maturity" (13-23).

The consequence of accepting this dynamic nature of digital security risks is the existence of residual risks and to admit one cannot eliminate all cybersecurity risks to achieve 100% security [42]. This thinking is contrary to managing the risk of (non)compliance where the outcome is black-and-white: to be compliant or not.

"[…] The more measures you'll take, the more resilient you become but you'll never make it to 100%" (12-21), and
[…] If you do the math, […] you'll have to accept that there is a residual risk" (16-26).

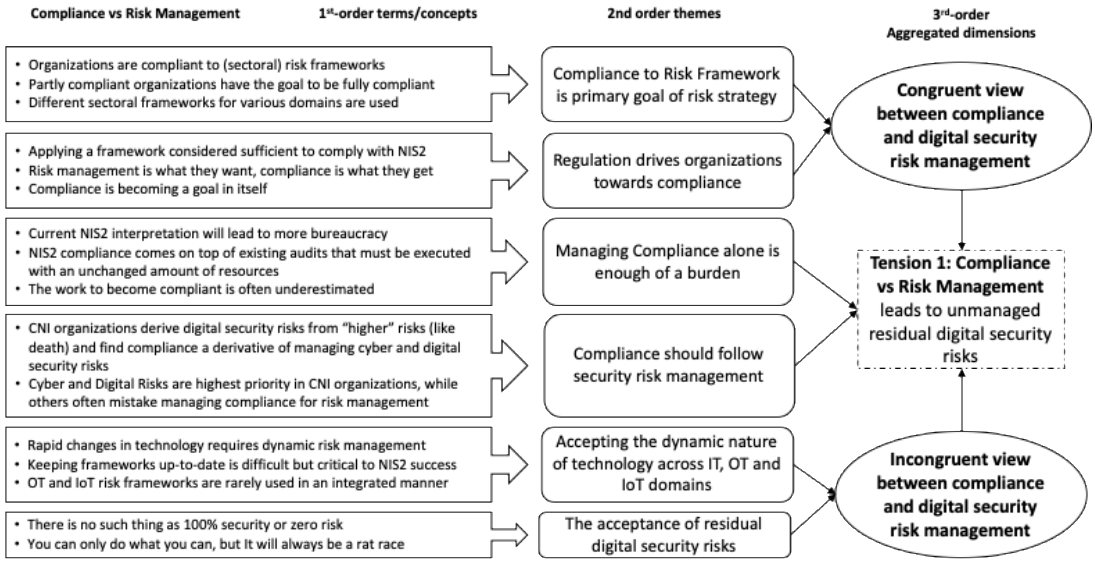

Figure1. Data structure presenting the Compliance Management vs Risk Management Tension

Marotta & Madnick found that organizations with lower levels of (cyber)maturity may view compliance as a motivating factor[33]which corresponds with the observations in this study amongst the organizations(often CNI) that hold the incongruent view, while organizations that are new under the NIS2 Directive hold the congruent view. Our study confirms that large groups of organizations may seek to manage compliance as described by Folorunso, while neglecting inevitable residual risks as found by CNI organizations who take security risk management as a starting point, instead of compliance management.

4.2. Tension 2: Single vs Shared Risk Ownership

The second tension identified in this paper shines light on the tension between the responsibilities that NIS2 puts on an organization and the reality of that organization becoming increasingly dependent on third and fourth parties for its continuity. In framing this tension, we draw upon an ongoing debate in literature on the ownership of security risks. One view in literature takes, like the NIS2, a legal approach by attributing security risks failures to an organization or its decision makers through accountability or liability. However, another view in literature finds that global sourcing, supply chain ownership, different legal jurisdictions and the extensive use of third parties require a holistic approach [43]and risks should be collectively owned by the ecosystem since single attribution is no longer feasible. The authors call this the collaborative perspective since parties manage the risks collectively.

4.2.1. Attribution Perspective on Single Versus Shared Risk Ownership

To ensure that organizations take care of their duties, governmental authorities use two familiar instruments for influencing risk management behaviour: accountability and liability. The GDPR provides yearly examples where organizations were held liable and had to pay the penalty such as Accor SA, Meta on Instagram and WhatsApp in 2022 [44]. Cyber incidents at Equifax, Target and Capia are examples where CEO's were held accountable and lost their jobs. Research shows several benefits of using accountability and liability as drivers to influence the risk propensity of decision makers. Already in 1992, Wagner identified a need to establish organizational accountability for risk assessment and safety measures and to define this as a major management task [45]. Sheedy & Canestrari-Soh provide evidence that, consistent with theory and previous experimental research, enhanced accountability stimulates more proactive and diligent risk management behaviour [46].The CISO's amongst the informants confirm this with many using it towards the decision-makers to put security risk management (higher) on the agenda:

"[…] Soon you will be held personally liable for gross negligence" (04-06),
"[…] Soon you will be held liable and accountable" (12-20),
"[…] He knows it's no longer a question if he's held accountable, but when" (17-29), and
"[…] You always need to remind Directors that they are, and always will be, accountable" (01-01)

The CISO informants did not differentiate between accountability and liability in their messaging, in spite of the NIS2 explicitly adding personal liabilities to "ensure that a natural person has the authority to take decisions on its behalf or the authority to exercise control of it has the power to ensure its compliance with this Directive"[16].The value of introducing personal liability is a more cacophonous endeavour since this becomes a litigation matter. When deciding director negligence cases, jurors assess whether directors acted in good faith and had a reasonable basis for determining that their actions (or inactions) were sufficient to satisfy the best interest of the company [47]. Directors are also more likely to be held liable when their organization previously experienced a cyberattack [48]. If the board makes an informed decision in this regard, it should satisfy its fiduciary obligations with respect to the duty of care to the company [49] as shown in the derivative action against the board of Wyndham Worldwide Corporation[50]. The directors amongst the informants share the scepticism in literature on the effectiveness of personal liabilities:

"[…] Liable, accountable, responsible […] I have to see it first" (12-20),
"[…] Personal liability doesn't affect my risk management behaviour. It's just politics" (16-26),
"[…] The reflex is: I'm insured, onto the next item on the agenda" (10-17), and
"[…] Make sure you have a good insurance policy or lawyer, and then go back to work" (05-07)

Third parties' role in performing business activities for organizations is becoming more significant. When a Third-Party provider is the victim of an (cyber)attack or an incident, this can impact the digital resilience of the organization [51]. The NIS2 acknowledges the dependency of firms on third parties [52] by mandating supply chain security, "including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers" in article 21 section 2[16].A way of managing third-party risks is by formulating contractual agreements [53] that take into account several types of risks: operational, legal, regulatory, cybersecurity, compliance, reputational, strategic and financial [54].Many CISO informants express their concern about third party risk management within their organization:

"[…] We have general conditions in our procurement and tendering processes, but security hasn't been fully embedded yet" (12-20),
"[…] There is much to improve in tendering processes and supplier contracts" (13-22), and

"[…] The supply chain, which needs to be across all processes and outwards facing, is a neglected child" (07-12).

4.2.2. Collaborative Perspective on Single Versus Shared Risk Ownership

Interestingly, many of the informants referred to the 2022 Log4Shell (a.k.a. Log4J) incident, confirming a study by Wu that prior research into digital security risk management rarely considers the impact of risk interdependency on security decisions [55]:

"[…] If there is another Log4J, we will have a challenge again" (04-06),
'[…] If Log4J comes along, we drop everything and report immediately" (16-26),
"[…] Software Bill-of-Materials is a topic of conversation for us" (14-23), and
[…] We found one of our suppliers being incapable of patching in-spite-of their remote access" (02-02).

Log4J, in which an open-source software library used by many software products turned out to contain a dangerous vulnerability, shows it gets more complicated when taking into account the whole chain, including fourth and fifth parties within the supply chain [56]. Through the Log4J example, CISO informants indicate that supply chain risk management needs to include Fourth-Party Risks [57] and move beyond its current technical focus [58]. However, many organizations don't have adequate visibility on their third parties, and even less so concerning their third parties' third parties and beyond, so-called Nth parties [59]. Several informants express their hopethat the NIS2 will prioritize Nth-Party security risk management:

"[…] In supplier management, we need to have better conversations and express our mutual expectations" (11-18),
"[…] Visibility of your supply chain is necessary and a challenge" (04-05),
"[…] I hope the NIS2 will create the opportunity to get our suppliers to take cybersecurity more seriously and (provide) us (with) the possibility to test them" (01-01), and
"[…] The biggest incidents are now often in the supply chain. Understanding that problem and getting it on the agenda gets an extra boost by the NIS2" (15-25)

Another challenge that organizations face with regard to third-party risk management is an increasingly fragmented chain of service providers [56].Digital dependencies have extended the boundaries of traditional organisations [9], systems have transitioned from the organisational level to the inter-organisational level [60] and digital security risk governance are no longer restricted to a single organisation [61] as some of our informants confirm:

"[…] I'm convinced: the supply chain doesn't exist. It has become a complex and intertwined ecosystem […] And a system risk can only be controlled by the whole system, and never by one party alone" (16-27), and
"[…] I view cyber as everything that is both information and digital which we have to deal with (07-12).

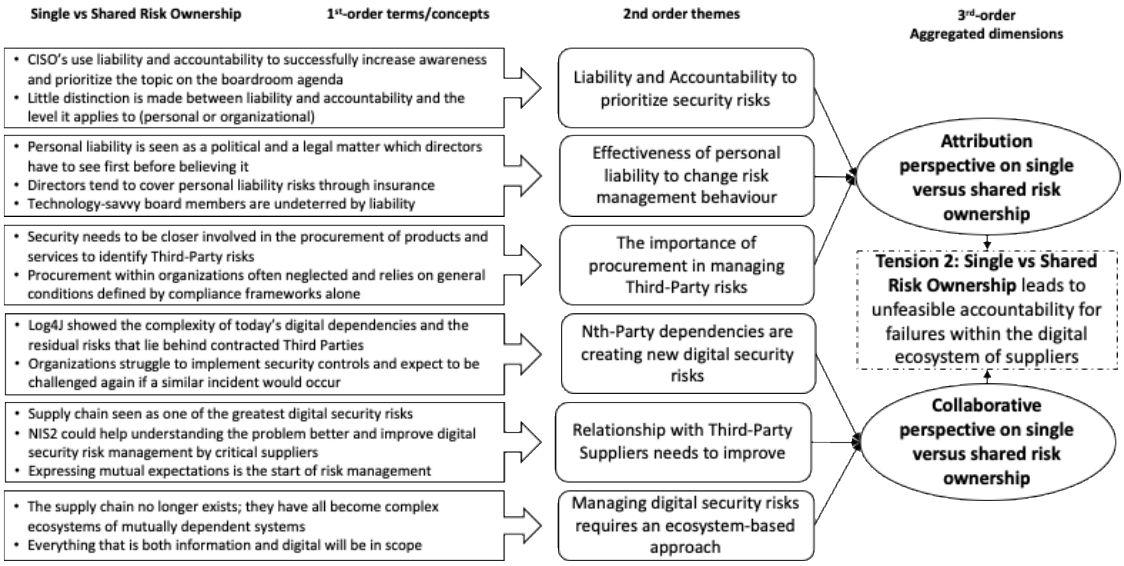

Figure 2. Data structure presenting the Single versus Shared Risk Ownership Tension

4.3. Tension 3: National versus Global Perspective

The third and final tension outlined in this paper reveals a tension between the national responsibilities for the implementation of the NIS2 and the global scale at which digital security risks occur. Articles 4 and 288 of the Treaty on the Functioning of the European Union place national security responsibilities on each member state[26], as shown with the NIS2 Directive having to be adopted to each national legal structure. This leads to incoherent strategies across member states, leaving gaps for adversaries to exploit [62]. Social contract theory provides a lens to understand these incoherences and gaps better.

Cyberspace challenges the traditional understanding of rights and responsibilities[63], forcing all parties to change their social contract accordingly [64]. Accordingly, the Internet Security Alliance developed the social cyber contract[65, 66] that forms the basis of Bierens & van den Berg's two interrelated "social cyber contracts" [23]: a direct social contract between governments and citizens by constitutional principles [67]and an indirect social contract where the interplay between government, corporations and citizens sustains the direct contract[68]. These two types of social cyber contract form the basis for the perspectives describing this tension.

4.3.1. Imperfect Market Forces on Managing Digital Risks within the Indirect Social Contract

When risk may affect any part of society, government is expected to respond which implies a need for governance and accountability. Under social contract theory, governments are obligated to protect citizens' safety and uphold collective security. Several of the informants share Gardenier's view that the continuity of their organizations for modern society has made them essential[1]:

"[…]If this fails, society immediately has a problem" (15-25), and
"[…] We have a duty to society, and we must be accountable to our citizens and to the government" (11-18),

Little research exists on the willingness to pay for security risk management, let alone, pay for security beyond compliance. Several directors amongst the informants feel they're taking a commercial risk by implementing more security measures than required by compliance or compared to their competitors since the additional costs may increase the price of their products and services. The willingness-to-pay amongst consumers for a more resilient CNI found by Lambert[69], was not recognized by our informants in their commercial discussions with the government in a customer capacity, who feel driven by limited budgets in-stead:

"[…] I am also bound by the budgets that I have to stick to" (17-29),
"[…] what matters to our information security, is our total budget" (15-25),
"[…] Everybody needs to think about budget cuts" (15-25),
"[…] Obtaining a concession is done through a tendering procedure. […] We invest substantially more in digitalization and security. Our risk is to be punished, because we are then more expensive because the rest is lagging. […] with a bit of bad luck, you are found to be too expensive. (10-16)",
*"[…] Our entire finances must be approved by the Ministry […] And I can tell you that the financial position of […] has been a topic of discussion for years" (15-25),*and
"[…] You are allowed to make a little profit in a concession, which means that you must also determine your risk profile yourself." (12-20)

4.3.2. Government is Critical to Maintaining the Direct Social Contract by Managing Digital Risks

The role of government in making the NIS2 implementation a success is acknowledged by our informants but there is little mentioning on their role towards the willingness to pay for additional security, let alone, pay for additional security beyond compliance. However, the "check-the-box" mentality described by Folorunso for regulatory compliance is recognized by our informants:

"[…] The success of the NIS2 depends onhow the supervisory authority from government will execute it's role" (04-06),

"[…] Government should say: this is the standard. And then to everyone: you shall…" (13-22),

"[…] If something goes wrong, we'll get stricter regulation which triggers the checkbox-ticking reflex, as we're also seeing with the NIS. […] It's a bit like the director on the Titanic telling its orchestra: "You're playing very well" (16-26), and
"[…] Government's interest is not in continuity, in people, in processes. That is only in the political accountability. I call that the cover-your-ass methodology" (04-06).

Van den Berg identifies two huge challenges for governments: the governance of national and international IT & OT infrastructures, and securing cyber activities and processes in all cyber subdomains [70]. Many informants acknowledge the challenges of national and international governance limitations but also express their concern about the lack of knowledge:

"[…] The government is still lagging behind in some areas" (07-12),

"[…] You need to accept that there is a residual risk. Supervisory authorities are having trouble dealing with that" (16-26),
"[…] The supervisory authority, as enforcer of the NIS, must also grow its maturity" (04-06),
"[…] Two years ago, […] I decided to have an investigation done into the administrative powers surrounding digital disruptions and whether Thorbecke, with his thinking from the 19th century, is still leading. The answer turned out to be 'yes'" (05-07), and

"[…] We have so many supervisors, you sometimes laugh your head off and don't think that they will talk together, because then they will have to decide among themselves who is the most important and that is not going to happen" (16-26).

4.3.3. Competing Social Cyber Contracts Between National and Data Sovereignties

Public risk governance is complicated by the multiplicity of different stakeholders and the network of interactions [4]. With democracies like the U.S. and Europe already diverging on topics like privacy [71], a comparative analysis between democracies like U.S. and EU to China as an autocracy by Ekmekçi found that cybersecurity has evolved into a strategic tool in global competition, with cyberattacks being used for coercion and disruption, while the rise of cyber espionage has heightened the stakes in digital diplomacy [72] in which the interplay with corporations outside a country or region plays a critical role. One of our informants outlined how he dealt with these conflicting sovereignties:

"[…] You think you can keep the US government out of your organization? You just have to accept it […] Just worry about keeping the Russians and the Chinese out, or those from Iran, because the Americans are our friends, on paper at least" (06-09)

Unsurprisingly, cloud migration was often mentioned by our informants, which corresponds with the definition in the NIS2 of electronic communications networks. In today's world, Big Tech has evolved into the new data sovereigns that governments must accept in the data era [73]. However, the informants broadened the definition of Big Tech by adding several other global technology providers such as ABB and Siemens to Big Tech since their interactions with them show similar lock-in effects as they experienced with cloud providers.

Many informants held the opinion that working with Big Tech requires the acceptance of a vendor lock-in confirming Van Den Berg[70]who states that the dependence and power of the big IT companies should be kept within acceptable limits by intensifying the efforts in international forums:
"[..] There are only 4 or 5 major suppliers in the world, to enter those power blocs and say: we are jointly responsible, how are we going to solve this together?" (10-17), and

"[…] A GE or a Siemens, or […] Microsoft […] what influence do I have? It can be said so nicely: "You have to have a grip on your suppliers and demand this and that..." But compared to those big players, we are crumbs to them." (16-27).

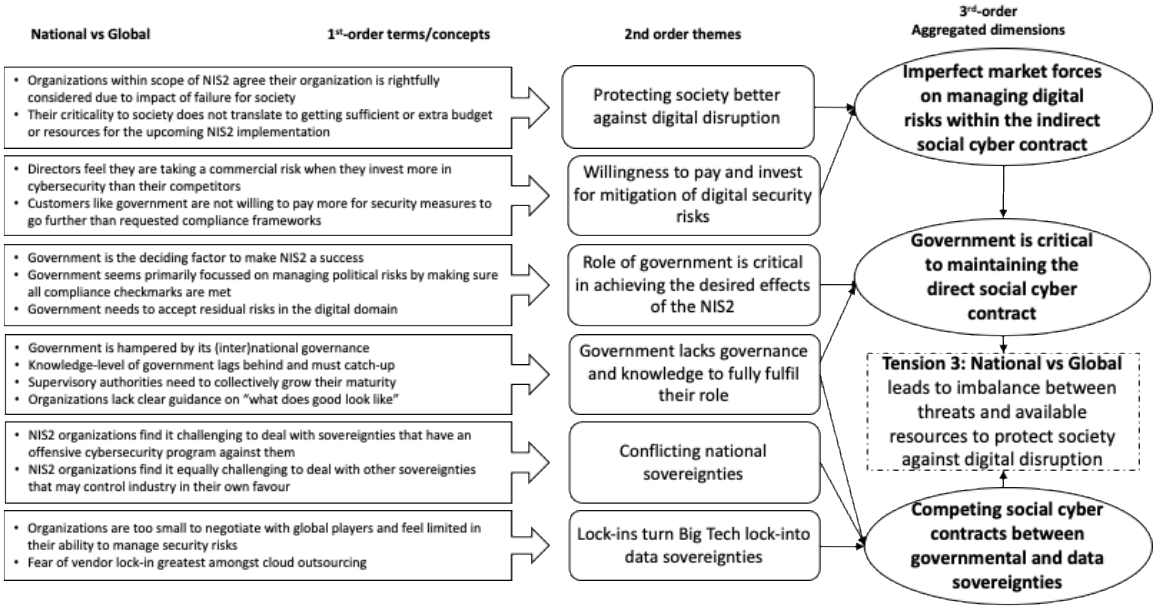

Figure3. Data structure presenting the National versus Global Perspective Tension

5. QUALITATIVE RESEARCH IN SUPPORT OF THE TENSIONS FOUND

Two separate surveys in 2024 by SANS Institute [74] and the European Cyber Security Organization [75] confirmed the identified tensions in this study for the whole of Europe. For example, the 155 respondents from 23 European countries that participated in the ECSO research identified lack of clarity from government (26%), supply chain security concerns (16%), framework alignment (12%), resource constraint (12%), management buy-in (8%) as their main challenges in the NIS2 implementation which are all covered by the tensions in this research. Regarding tension 1, 92% of the ESCO respondents requested more standardized guidelines to facilitate compliance with NIS2, while only 10% emphasized the importance of risk management, assessment, or prioritization based on risk. Regarding tension 2, 66% reported of the ECSO respondents successfully involved management, while 60% of the SANS respondents held a positive attitude towards the NIS2. SANS also reported 35% of the organizations started the NIS2 implementation while 50% was planning to start. Regarding tension 3, 60% of ECSO respondents have had some form of contact with national supervisory authorities but rated their collaboration a modest 6.59 out of 10 which means the quality and effectiveness of these interactions may not be meeting all their needs confirming tension 3 in this study. Lack of constraints were reported by SANS on resources (45%), budget (37%) and ECSO reporting that 73% is allocating up to 10% of their current cybersecurity budget for the NIS2 implementation.

6. INTERRELATEDNESS IDENTIFIED BETWEEN THE TENSIONS

While the various perspectives provide of the identified tension, interrelatedness between the various tensions was also observed during the interviews. Figure 4 structures all 2nd order themes by their mentioning in the same interviews with fixed connectors showing relations within a single tension, while dotted connectors show interrelatedness between two different tensions.

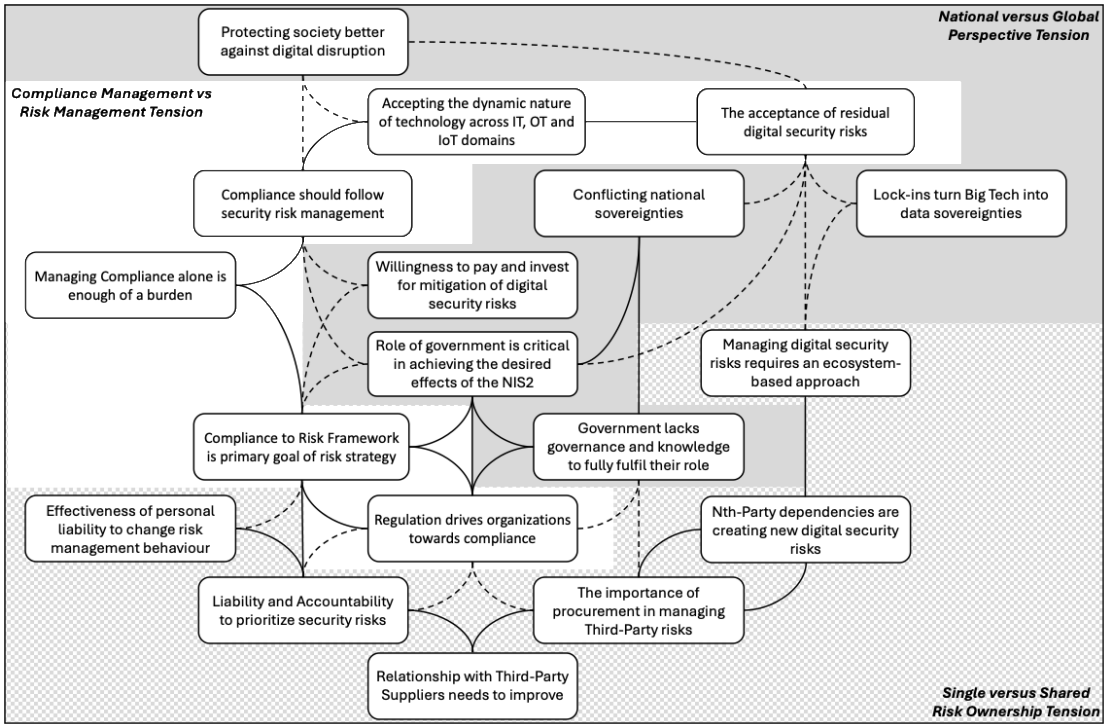

Figure 4. Observed interrelations between 2nd order themes across all tensions

Figure 4 shows that protecting society better against digital disruption requires accepting the dynamic nature of technology across global IT, OT and IoT domains, but will always result in some residual risks. However, figure 4 also suggest that managing digital security risks by compliance alone that is reinforced by personal liabilities, in-stead of starting with a digital-by-design perspective due a lack of knowledge withgovernments and affected organizations, may result in an increase of the residual risks.

Describing the interrelatedness of the 2nd order themes between the tensions was not the main purpose of the study. Figure 4 therefore does imply a positive or negative reinforcement between the (inter)related 2nd order themes. However, it does provide an understanding of the various factors that could impact the residual digital security risks for society as shown when Figure 4 is read counterclockwise. For example, the effectiveness of compliance to reduce residual security risk is determined by government as a policymaker, but governments are limited to their national sovereignty powers and the legal limitations in managing Nth-party risks.

7. CONTRIBUTIONS AND RESEARCH IMPLICATIONS

Our work responds to reoccurring calls for more research that supports the holistic management of all technological risks and the many dynamic external dependencies that each of these technologies create [29, 61]. We offer the following contributions. First, we built a theory of the digital security risk managment phenomenon, in particular, on “implementation”. Discussing the tensions from a theoretical view helps research indicate, label and further understand what hinders organizations when implementing digital security risk managment. Second, our work is relevant for practitioners as was demonstrated in the final validation workshop with government. The findings described in this paper help to become aware of possible tensions in today’s security risk management designs. The paper also provides a deeper understanding of how and why the implementation of the NIS2 is affected by the tensions and hinder reaching a high common level

of cybersecurity. Managing the tensions can lead to more effective and established digital security risk management approaches. Third, we provide a novel view by using social contract theory to study the global challenges of digital security risk management. By doing so, we contribute to a question of how governments can turn their role as regulator and supervisor into a positive driver for change.

This study has limitations since it strongly focused on identifying and explaining why tensions are present. This study did not examine underling relations or barriers. Also, our paper provides little insight into how this knowledge can be made operational. Further research can examine the underlying relations between the presented tensions as outlined in Figure 4. For example, it is valuable to understand how regulatory compliance can become more dynamic to become congruent to digital security risk management, which residual risks are deemed acceptable for society, what changes are needed to move from Third-Party Risk Management to an ecosystem approach in managing risk and how to deal with national and international barriers preventing the working of the social contract to create a more cyber resilient society.

8. CONCLUSION

Our study found that most informants agree that their organizations are rightfully within scope of NIS because of the importance of their continuity to society and the growing threat of digital security risks. The organizational accountability that comes with it seems to be effective in making NIS2 a boardroom topic. The threat of personable liability often being used by CISO's, but without any noticeable change in risk management behavior at the decision-making level. Except for current CNI organizations, the overall effect of the NIS2 is that compliance is becoming the dominant goal for organizations. Informants agree that, as part of their social contract responsibility, government should therefore determine the appropriate, preferably sector-specific, policies for compliance to allow policymaking and supervision to be effective while incorporating the dynamic nature of digital security risks.

However, many informants find the current level of knowledge and governance structure of government inconsistent with what's required to guide them on the management of digital security risks. This goes beyond managing compliance as our study finds but is confronted by a general unwillingness to pay more for additional security measures.The ongoing digital transformation is also shifting risks outside of the organization, which is incongruent with the accountability,let alone liability, as defined by NIS2. This shift also requires the CISO function to become closer involved with their internal procurement processes. Informants acknowledge that managing Nth-Party risks is a major concern in which they hope the NIS2 will back their efforts to address them, while the balance of power is quickly shifting due to conflicting sovereignties and the emergence of data sovereignties from Big Tech corporations and various other forms of lock-ins.

Overall, the study finds that the implementation of the NIS2 primarily drives compliance management with cyber resilience being determined by the quality of the compliance frameworks and the government that (co)creates them. However, the dynamic nature of digital risk will inevitably require more measures to be taken while residual risks will remain for those that only manage compliance, especially when risks are moving beyond the organizational capability-to-control. The authors call this residual risk the digital deficit of the NIS2.

ACKNOWLEDGMENTS

The authors would like to thank all the informants and participants in the various validation workshops for their time and their valuable contributions to this study.

REFERENCES

[1] A. Gardenier, "Strengthening the Role of Citizens in Governing Disruptive Technologies: The Case of Dutch Volunteer Hackers," 2024, pp. 399-409.

[2] K. Prislan, A. Mihelic, and I. Bernik, "A real-world information security performance assessment using a multidimensional socio-technical approach," (in English), *PLoS One*, Article vol. 15, no. 9, p. 28, Sep 2020, Art no. QL, doi: 10.1371/journal.pone.0238739.

[3] M. van Haastrecht, B. Y. Ozkan, M. Brinkhuis, and M. Spruit, "Respite for SMEs: A Systematic Review of Socio-Technical Cybersecurity Metrics," (in English), *Appl. Sci.-Basel*, Review vol. 11, no. 15, p. 28, Aug 2021, Art no. QL, doi: 10.3390/app11156909.

[4] G. Andreeva, J. Ansell, and T. Harrison, "Governance and Accountability of Public Risk," (in English), *Financ. Account. Manag.*, Article vol. 30, no. 3, pp. 342-361, Aug 2014, doi: 10.1111/faam.12036.

[5] K. A. Barton, G. Tejay, M. Lane, and S. Terrell, "Information system security commitment: A study of external influences on senior management," (in English), *Comput. Secur.*, Article vol. 59, pp. 9-25, Jun 2016, Art no. QL.

[6] B. Heath, "Before the Breach: The Role of Cyber Insurance in Incentivizing Data Security," (in English), *George Wash. Law Rev.*, Article vol. 86, no. 4, pp. 1115-1151, Jul 2018, Art no. QL.

[7] M. Vitunskaite, Y. He, T. Brandstetter, and H. Janicke, "Smart cities and cyber security: Are we there yet?A comparative study on the role of standards, third party risk management and security ownership," (in English), *Comput. Secur.*, Article vol. 83, pp. 313-331, Jun 2019, Art no. QL.

[8] K. Quigley, C. Burns, and K. Stallard, "'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection," *Gov. Inf. Q.*, vol. 32, no. 2, pp. 108-117, Apr 2015, Art no. QL.

[9] B. von Solms, "Information security - The Fourth Wave," *Comput. Secur.*, vol. 25, no. 3, pp. 165-168, May 2006, Art no. QL.

[10] M. Niemimaa, "Information systems continuity process: Conceptual foundations for the study of the "social"," (in English), *Comput. Secur.*, Article vol. 65, pp. 1-13, Mar 2016, Art no. QL.

[11] W. J. Caelli, "Trusted ... or ... trustworthy: the search for a new paradigm for computer and network security," *Comput. Secur.*, vol. 21, no. 5, pp. 413-420, 2002, Art no. QL.

[12] Y. D. Luo, "A general framework of digitization risks in international business," (in English), *J. Int. Bus. Stud.*, Article; Early Access p. 18, 2021, doi: 10.1057/s41267-021-00448-9.

[13] *Measures for a high common level of security of network and information systems across the Union*, O. J. o. t. E. Union, 2016.

[14] D. Markopoulou, V. Papakonstantinou, and P. Hert, "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation," *Comput. Law Secur. Rev.*, vol. 35, 11/01 2019, doi: 10.1016/j.clsr.2019.06.007.

[15] B. P. Adami M., Barbizan T., Billois G., Bonanni F., Cole M., Dinand P., Endrodi G., Herrera F., Juskesvicius R., Maridis G., Massacci F., Milio S., Polito C., Pupillo L., Richardson M., Schmitz M., Talpo S., Thirriot A., Zamboni A., "Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) - No. 2020-665," Directorate-General for Communications Networks, Content and Technology, 2021.

[16] *Measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148*, O. J. o. t. E. Union, 2022.

[17] A.-V. Dragomir, "What's New In The NIS2 Directive Proposal Compared To The Old NIS Directive," *Practical Application of Science*, no. 27, pp. 155-162, 2021. [Online]. Available: https://ideas.repec.org/a/cmj/seapas/y2021i26p155-162.html.

[18] T. Sievers, "Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations," *International Cybersecurity Law Review,* vol. 2, 12/01 2021, doi: 10.1365/s43439-021-00033-8.

[19] D. Ferguson, "The outcome efficacy of the entity risk management requirements of the NIS 2 Directive," *International Cybersecurity Law Review,* vol. 4, pp. 1-16, 08/17 2023, doi: 10.1365/s43439-023-00097-8.

[20] V. Lucini, "THE EVER-INCREASING CYBERSECURITY COMPLIANCE IN EUROPE: THE NIS 2 AND WHAT ALL BUSINESSES IN THE EU SHOULD BE AWARE OF," *Russian Law Journal,* vol. 11, 04/07 2023, doi: 10.52783/rlj.v11i6s.911.

[21] NCTV, "CSIRT-STELSEL - Een beleidskader voor het herinrichten van het stelsel met een nationale en sectorale CSIRT's in Nederland," Ministerie van Justitie en Veiligheid, The Hague, 2023.

[22] J. D. Michels and I. Walden, "Beyond "Complacency and Panic": Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?," (in English), *Eur. Law Rev.*, Article vol. 45, no. 1, pp. 25-47, Feb 2020, Art no. QL. [Online]. Available: <Go to ISI>://WOS:000514110800003.

[23] R. H. Bierens, van den Berg, J., Klievink, B., , "A Social Cyber Contract Theory Model for Understanding National Cyber Strategies," (in English), *Lecture Notes in Computer Science*, vol. 10428, no. Proceedings of International Conference on ElectronicGovernment 2017, pp. 166-176, 2017, doi: doi.org/10.1007/978-3-319-64677-0_14.

[24] A. Tsohou, M. Karyda, and S. Kokolakis, "Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs," *Comput. Secur.*, vol. 52, pp. 128-141, Jul 2015, Art no. QL. [Online]. Available: <Go to ISI>://WOS:000382271400008.

[25] E. McFadzean, J. N. Ezingeard, and D. Birchall, "Perception of risk and the strategic impact of existing IT on information security strategy at board level," *Online Information Review,* vol. 31, no. 5, pp. 622-660, 2007, Art no. QL. [Online]. Available: <Go to ISI>://WOS:000250991700005.

[26] *Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union,* O. J. o. t. E. Union, 2012.

[27] D. A. Gioia, K. G. Corley, and A. L. Hamilton, "Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology," (in English), *Organ. Res. Methods,* Article vol. 16, no. 1, pp. 15-31, Jan 2013, doi: 10.1177/1094428112452151.

[28] M. Eling, "Cyber risk research in business and actuarial science," (in English), *Eur. Actuar. J.*, Article vol. 10, no. 2, pp. 303-333, Dec 2020, Art no. QL, doi: 10.1007/s13385-020-00250-1.

[29] R. H. Bierens, Shahim, A., "Are we ready to manage digital risks today and tomorrow?," *Journal of Information Systems Security,* vol. 18, 2, p. 41, 2023.

[30] H. Zhang, K. Chari, and M. Agrawal, "Decision support for the optimal allocation of security controls," (in English), *Decis. Support Syst.*, Article vol. 115, pp. 92-104, Nov 2018, Art no. QN.

[31] OECD, "Digital Security Risk Management for Economic and Social Prosperity," OECD, Paris, 2015.

[32] M. Brunner, C. Sillaber, L. Demetz, M. Manhart, and R. Breu, "Towards data-driven decision support for organizational IT security audits," (in English), *IT-Inf. Technol.*, Article vol. 60, no. 4, pp. 207-217, Aug 2018, Art no. QN. [Online]. Available: <Go to ISI>://WOS:000440077100004.

[33] A. Marotta and S. Madnick, "Perspectives on the relationship between compliance and cybersecurity," vol. 16, pp. 151-177, 01/01 2020.

[34] C. Sillaber, A. Mussmann, and R. Breu, "Experience: Data and Information Quality Challenges in Governance, Risk, and Compliance Management," (in English), *ACM J. Data Inf. Qual.*, Article vol. 11, no. 2, p. 14, May 2019, Art no. QL. [Online]. Available: <Go to ISI>://WOS:000468045500002.

[35] F. O. Sveen, J. M. Torres, and J. M. Sarriegi, "Blind information security strategy," *Int. J. Crit. Infrastruct. Prot.*, vol. 2, no. 3, pp. 95-109, Oct 2009, Art no. QL. [Online]. Available: <Go to ISI>://WOS:000208416100005.

[36] C. C. Lo and W. J. Chen, "A hybrid information security risk assessment procedure considering interdependences between controls," *Expert Systems with Applications,* vol. 39, no. 1, pp. 247-257, Jan 2012, Art no. QL. [Online]. Available: <Go to ISI>://WOS:000296214900029.

[37] M. T. Siponen, "An analysis of the traditional IS security approaches: implications for research and practice," *Eur. J. Inform. Syst.*, vol. 14, no. 3, pp. 303-315, Sep 2005, Art no. QL. [Online]. Available: <Go to ISI>://WOS:000231872800009.

[38] A. Folorunso, I. Wada, B. Samuel, and V. Mohammed, "Security compliance and its implication for cybersecurity," *World Journal of Advanced Research and Reviews*, vol. 24, pp. 2105-2121, 10/21 2024, doi: 10.30574/wjarr.2024.24.1.3170.

[39] L. Magnusson, F. Dalipi, and P. Elm, "Cybersecurity Compliance in the Public Sector: Are the Best Security Practices Properly Addressed?," 2023, pp. 219-226.

[40] B. Madnick, K. Huang, and S. Madnick, "The evolution of global cybersecurity norms in the digital age: A longitudinal study of the cybersecurity norm development process," *Information Security Journal: A Global Perspective*, pp. 1-22, 2023, doi: 10.1080/19393555.2023.2201482.

[41] J. Boeken, "From compliance to security, responsibility beyond law," (in English), *Comput. Law Secur. Rev.*, Article vol. 52, p. 5, Apr 2024, Art no. 105926, doi: 10.1016/j.clsr.2023.105926.

[42] L. D. Bodin, L. A. Gordon, M. P. Loeb, and A. Wang, "Cybersecurity insurance and risk-sharing," (in English), *J. Account. Public Policy*, Article vol. 37, no. 6, pp. 527-544, Nov-Dec 2018, Art no. QL. [Online]. Available: <Go to ISI>://WOS:000454970800003.

[43] H. Boyes, "Cybersecurity and Cyber-Resilient Supply Chains," *Technol. Innov. Manag. Rev.*, pp. 28-34, Apr 2015, Art no. QL.

[44] (2023). *Annual Report 2022 - Streamlining Enforcement Through Corporation*.

[45] I. Wagner, "VULNERABILITY OF COMPUTER-SYSTEMS - ESTABLISHING ORGANIZATIONAL ACCOUNTABILITY," (in English), *Ifip Transactions a-Computer Science and Technology*, Article vol. 13, pp. 433-439, 1992. [Online]. Available: <Go to ISI>://WOS:A1992LD44400064.

[46] E. Sheedy and D. S. B. Canestrari-Soh, "Does executive accountability enhance risk management and risk culture?," (in English), *Accounting and Finance*, Article vol. 63, no. 4, pp. 4093-4124, Dec 2023, doi: 10.1111/acfi.13087.

[47] T. Brown, T. Majors, and M. Peecher, "The Influence of Evaluator Expertise, a Judgment Rule, and Critical Audit Matters on Assessments of Auditor Legal Liability," *SSRN Electronic Journal*, 01/01 2014, doi: 10.2139/ssrn.2483221.

[48] M. L. Frank, J. H. Grenier, and J. S. Pyzoha, "Board liability for cyberattacks: The effects of a prior attack and implementing the AICPA's cybersecurity framework," (in English), *J. Account. Public Policy*, Article vol. 40, no. 5, p. 16, Sep-Oct 2021, Art no. 106860, doi: 10.1016/j.jaccpubpol.2021.106860.

[49] J. M. Westerlind. (2016) The Board's Cybersecurity Responsibility. *ForeFront*.

[50] H. Yegelwel, "CYBERSECURITY OVERSIGHT: A CAUTIONARY TALE FOR DIRECTORS," *Journal of Technology Law & Policy*, no. vol. 20, no. 2, pp. 229-264, 2015.

[51] M. Leo, "Operational Resilience Disclosures by Banks: Analysis of Annual Reports," (in English), *Risks*, Article vol. 8, no. 4, p. 15, Dec 2020, Art no. 128, doi: 10.3390/risks8040128.

[52] Y. B. Chang, V. Gurbaxani, and K. Ravindran, "INFORMATION TECHNOLOGY OUTSOURCING: ASSET TRANSFER AND THE ROLE OF CONTRACT," (in English), *Mis Q.*, Article vol. 41, no. 3, pp. 959-+, Sep 2017. [Online]. Available: <Go to ISI>://WOS:000407896800013.

[53] R. Khalef, I. H. El-adaway, R. Assaad, and N. Kieta, "Contract Risk Management: A Comparative Study o Risk Allocation in Exculpatory Clauses and Their Legal Treatment," (in English), *J. Leg. Aff. Dispute Resolution Eng. Constr.*, Article vol. 13, no. 1, p. 19, Feb 2021, Art no. 04520036, doi: 10.1061/(asce)la.1943-4170.0000430.

[54] M. H. Uddin, M. H. Ali, and M. K. Hassan, "Cybersecurity hazards and financial system vulnerability: a synthesis of literature," (in English), *Risk Manag.*, Article vol. 22, no. 4, pp. 239-309, Dec 2020, doi: 10.1057/s41283-020-00063-2.

[55] Y. Wu, L. P. Wang, D. Cheng, and T. Dai, "Information security decisions of firms considering security risk interdependency," (in English), *Expert Systems with Applications*, Article vol. 178, p. 15, Sep 2021, Art no. QN, doi: 10.1016/j.eswa.2021.114990.

[56] M. Pournader, A. Kach, and S. Talluri, "A Review of the Existing and Emerging Topics in the Supply Chain Risk Management Literature," *Decis. Sci.*, vol. 51, no. 4, pp. 867-919, 2020, doi: https://doi.org/10.1111/deci.12470.

[57] G. Stewart, "Fourth parties: Concentration risk and its mitigation," *Journal of Supply Chain Management, Logistics and Procurement*, vol. 6, no. 3, pp. 213-231, 2024.

[58] A. Creazza, C. Colicchia, S. Spiezia, and F. Dallari, "Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era," (in English), *Supply Chain Manag.*, Article; Early Access p. 24, 2021, Art no. QN, doi: 10.1108/scm-02-2020-0073.

[59] J. Jaeger. (2018) Reducing third-party risks with eyes wide open: Recent analyses show that many companies don't have adequate visibility into their third parties, and even less so their third parties' third parties and beyond (so-called Nth parties). *Compliance Week*. 7.

[60] F. Fang, M. Parameswaran, X. Zhao, and A. B. Whinston, "An economic mechanism to manage operational security risks for inter-organizational information systems," *Inf. Syst. Front.*, vol. 16, no. 3, pp. 399-416, Jul 2012, Art no. QN. [Online]. Available: <Go to ISI>://WOS:000338280900006.

[61] S. Schinagl and A. Shahim, "What do we know about information security governance? "From the basement to the boardroom": towards digital security governance," (in English), *Inf. Comput. Secur.*, Review; Early Access p. 32, 2019, Art no. QL.

[62] J. Ruohonen, *The Incoherency Risk in the EU's New Cyber Security Policies*. 2024.

[63] A. Liaropoulos, "A Social Contract for Cyberspace, Journal of Information Warfare, 19, 2 (2020)," vol. 29, pp. 1-11, 06/25 2020.

[64] J. H. Kaufman, S. Edlund, D. A. Ford, and C. Powers, "The social contract core," in *Proceedings of the 11th international conference on World Wide Web*, 2002, pp. 210-220.

[65] I. S. Alliance. *The Cyber Security Social Contract*. (2008). Washington: Internet Security Alliance.

[66] I. S. Alliance. *Social Contract 2.0: A 21st Century Program for Effective Cyber Security*. (2009). Washington: Internet Security Alliance.

[67] L. Henkin, "The United States Constitution as Social Compact," *Proceedings of the American Philosophical Society*, vol. 131, no. 3, pp. 261-269, 1987. [Online]. Available: http://www.jstor.org.vu-nl.idm.oclc.org/stable/987021.

[68] C. Inglis and H. Krejsa, "The cyber social contract," *Foreign Affairs. February*, vol. 21, p. 2022, 2022.

[69] D. M. Lambert *et al.*, "Consumer willingness-to-pay for a resilient electrical grid," *Energy Economics*, vol. 131, p. 107345, 2024.

[70] J. van den Berg, "Present-Day Cybersecurity: Actual Challenges and Solution Directions," IntechOpen, 2024.

[71] J. Reidenberg, "Resolving Conflicting International Data Privacy Rules in Cyberspace," *Stanford Law Review*, vol. 52, 05/01 2000, doi: 10.2307/1229516.

[72] E. Ekmekçi, "Cybersecurity and the Future of International Relations," *Next Generation Journal for The Young Researchers*, vol. 8, p. 57, 10/25 2024, doi: 10.62802/85tt3452.

[73] H. Gu, "Data, Big Tech, and the New Concept of Sovereignty," *Journal of Chinese Political Science*, 05/03 2023, doi: 10.1007/s11366-023-09855-1.

[74] D. Pearson, "NIS2 Directive Readiness: Compliance, Challenges, and Recommendations," 2024.

[75] S. Čutura, "NIS2 Implementation: Challenges and Priorities," European Cyber Security Organisation, 2024.