



RESEARCH
ARTICLE



OPEN
ACCESS



PEER
REVIEWED

From Compliance to Disclosure: Tracing Cybersecurity and Supply Chain Risk in Dutch Annual Reports

Clara Boggini *Erasmus University Rotterdam*

DOI: <https://doi.org/10.14763/2026.4.2127>

Published: 6 October 2026

Received: 19 April 2025 **Accepted:** 19 May 2026

Funding: This research has been made possible through external funding. Ahold Delhaize N.V. provided the research funding. The author confirms that there is no contractual relationship with Ahold Delhaize N.V.; the author's only contractual relationship is with Erasmus University Rotterdam, which received and managed the funds.

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Licence: This is an open-access article distributed under the terms of the Creative Commons Attribution 3.0 License (Germany) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. <https://creativecommons.org/licenses/by/3.0/de/deed.en>
Copyright remains with the author(s).

Citation: Boggini, C. (2026). From Compliance to Disclosure: Tracing Cybersecurity and Supply Chain Risk in Dutch Annual Reports. *Internet Policy Review*, 15(4).
<https://doi.org/10.14763/2026.4.2127>

Keywords: Cybersecurity, NIS2, DORA, Annual reports, Corporate governance

Abstract: In 2022, the European Union legislator adopted Directive (EU) 2022/2555 (NIS2) and Regulation (EU) 2022/2554 (DORA). Combined, these laws introduced mandatory cybersecurity and supply chain security controls for several in-scope companies. However, their introduction raised the question of whether they improved cybersecurity practices or merely increased formal compliance. This article seeks to answer this question using annual reports. Annual reports are publicly available documents through which a company explains to its stakeholders the risks it faces and how it manages them. If, over time, a company changes its internal policies and practices for a given risk, subsequent annual reports will reflect these changes in the way that risk is disclosed. As cyber and supply chain risks are included in annual reports, changes in cybersecurity disclosure can signal shifts in how the company perceives and manages these risks. This article uses the annual reports of 67 Dutch companies listed on the AEX, AMX, and AscX to investigate whether observable changes in cybersecurity disclosure occurred before and after the introduction of NIS2 and DORA. A change in cybersecurity disclosure might be a signal that the new cybersecurity legislation has possibly contributed to ensure a shift in internal practices, going beyond mere compliance.

Introduction

Annual reports provide stakeholders with any existing or prospective financial and non-financial risks that could influence the performance of a company (Yuthas et al., 2002; Stanton & Stanton, 2002, p. 478; Linsley & Shrives, 2006, p. 387). Among the mentioned risks, annual reports also include cyber risks. Cyber incidents can have a significant impact on a company, both financially and non-financially. In the aftermath of a cyber incident, a company can suffer from loss of business, reputational damage, patching costs, and potential legal liability (Campbell et al., 2003, pp. 432–433; Kosseff, 2016, p. 404; Agrafiotis et al., 2018; Romanosky, 2016). These effects can impact the revenues or finances of a company, affecting in the end its overall performance in the market and its long-term continuity (Bhakhri et al., 2024; Wolff, 2022). Stakeholders can use the information on the types of controls adopted or the standard under which the company is certified to assess the company's cyber health. This information, hereafter defined as cybersecurity information, provides stakeholders with an understanding of the resilience of the company against cyber incidents and its ability to avoid losses (Arena et al., 2022, pp. 41–42; Boggini, 2024, p. 2).

To prevent cyber incidents and their potential long-term effects, companies must implement various cybersecurity controls and risk frameworks (Edwards & Weaver, 2024). The adoption of cybersecurity controls and risk management frameworks comes not only as a practical necessity but also as a compliance issue (Bygrave, 2025; Fuster & Jasmontaite, 2020; Kasper, 2020; Porcedda, 2018; Rupp, 2024). In 2022, the European Union (EU) legislator adopted Directive 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) and Regulation 2022/2554 on digital operational resilience for the financial sector (DORA). While having two different scopes and aims, these laws established for the first time cybersecurity obligations for several in-scope companies. Before 2022, only a limited number of EU companies were required under Directive 2016/1148 (NIS) to adopt cybersecurity controls. The majority of EU companies were required to adopt cybersecurity controls only to the extent necessary to ensure the security of personal data processing under Article 32 of Regulation (EU) 2016/679 (GDPR). However, only from 2022 cybersecurity has become a compliance concern for several EU companies (Schmitz-Berndt, 2021, p. 580; Schip, 2024, p. 12; Vandezande, 2024, p. 5). The obligations of NIS2 and DORA require the in-scope companies to establish cybersecurity controls or improve their already existing cyber risk management frameworks. Article 21 NIS 2 requires entities within its scope to implement technical, operational, and organisational measures to manage cyber risks

and prevent or minimise the impact of potential cyber-attacks. Article 5 DORA requires financial entities in the scope to implement an internal governance and control framework that ensures an effective and prudent management of Information and Communication Technologies (ICT) risks. While Article 21 NIS2 dictates a minimum list of measures,¹DORA provides a detailed description of the content of the ICT risk management framework (Articles 6-14).

Additionally, DORA and NIS2 introduced obligations regarding supply chain cybersecurity. Supply chain cyber risk has drastically increased over the past few years (Colicchia et al., 2019; Davis, 2015; Ghadge et al., 2019; Lee, 2021; Melnyk et al., 2022). Cyber threat actors shifted their attention to suppliers and the vulnerabilities in their systems. Suppliers are considered the weakest link of the broader network and information system of a company (Böhme & Moore, 2016, p. 82; Ghadge et al., 2019, p. 25; Khan & Estay, 2015, p. 6; Urciuoli et al., 2013, p. 51; Varian, 2004). EU documents and academic literature have noted that suppliers are more likely to have less rigorous risk management procedures, limited resources dedicated to cybersecurity investments, and fewer legal obligations, therefore representing ideal targets for threat actors (Urciuoli et al., 2013, p. 51; Creazza et al., 2022, p. 19; Melnyk et al., 2022, pp. 173–174; Schip, 2024, p. 9; Recital 56 NIS2; European Union Agency for CyberSecurity, 2025). In the digital supply chain, the network and information system of the company and those of the suppliers often are interconnected, facilitating cascading effects in case of cyber incidents (Colicchia et al., 2019; Davis, 2015; Ghadge et al., 2019; Lee, 2021; Melnyk et al., 2022). Therefore, by targeting the network and information system of a supplier, threat actors can easily gain access to the network and information system of another company. Thus, relying solely on a company's risk management framework is insufficient, as poor cybersecurity practices of suppliers can also be the root cause of cyber incidents (European Union Agency for CyberSecurity, 2025). For these reasons, NIS2 and DORA introduced additional obligations for companies to manage their supply chain cybersecurity risk. Article 21(2)(d) NIS2 requires in-scope companies to have a supply chain security policy to secure their direct suppliers, while

1. Based on article 21, the measures to be adopted should at least include: “(a) policies on risk analysis and information system security; (b) incident handling; (c) business continuity, such as backup management and disaster recovery, and crisis management; (d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers; (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure; (f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures; (g) basic cyber hygiene practices and cybersecurity training; (h) policies and procedures regarding the use of cryptography and, where appropriate, encryption; (i) human resources security, access control policies and asset management; (j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate”.

Articles 28-30 of DORA establish a third-party ICT risk management framework. These articles are playing a crucial role in enhancing the security of digital supply chains.

Building on this scenario, this article examines the patterns in cybersecurity risk disclosure in annual reports before and after the 2022 regulatory changes. When a company includes a risk in its annual report, different teams and bodies will review and discuss the risk management policies for that risk (Lombardi et al., 2021, p. 1441). Most importantly, drafting and approving an annual report require the involvement of the management and supervisory bodies. These bodies are best positioned to initiate and require modifications and improvements to internal policies (Galle & Vletter-van Dort, 2025; Kiesow Cortez & Dekker, 2022, pp. 451–153). Therefore, in light of the involvement of various company bodies, the discussion linked to annual reports can lead to revisions and improvements in company policies (Athanasakou & Boshanna, 2025, p. 5;; Kamiya et al., 2021). These changes would then be reflected in the annual reports of the following years, where the risk management practices related to these changed policies will be discussed differently.

This article applies this reasoning to cybersecurity and supply chain security risks, as well as to the regulatory timeline. If a company changes its approach and perception of cyber risk, the annual reports of the subsequent years will reflect these changes. An increased level of cybersecurity disclosure would signal that the cybersecurity legislation did not push companies to mere compliance, but rather to more active revision and improvement of cybersecurity risk management practices. Due to the role that annual reports have and due to the changes in the EU cybersecurity legislation, this study aims to answer the following research question: *“To what extent is there an observable change in how Dutch listed companies disclose cyber risk and supply chain cyber risk in their annual reports before and after the introduction of NIS2 and DORA in 2022?”*. Understanding whether and to what extent these changes have occurred enables me to assess the effectiveness of the regulatory changes introduced in 2022 in altering companies' cybersecurity risk management approaches. This research will focus exclusively on listed companies due to the more harmonised legislation on annual reporting and cybersecurity (Boggini, 2024).

However, before starting with the data collection and analysis, this article makes a preliminary consideration. This study limits itself at organising and describing quantitative data and will not conduct any analysis to establish causal inference. Establishing causal inference would allow me to determine whether the introduc-

tion of DORA and NIS2 directly caused a change in the data (Lawless et al., 2016). Therefore, if changes in the data are observed during the data analysis, these changes might also have been caused by other factors such as a rise in cyberattacks or changes in reporting standards/frameworks. Nonetheless, this study is the first to investigate how cybersecurity disclosure in annual reports has evolved over time. As annual reports provide an overview of the risks and risk management practices of companies, this study offers the literature and policymakers relevant information on the evolution of cyber risk perception in companies, comparing these changes with the regulatory time frame.

To answer the research question, this article employs a keyword research methodology. A similar methodology has already been used to study cybersecurity disclosure in annual reports in Eijkelenboom and Nieuwesteeg (2021). The authors used keywords to identify the cybersecurity content of an annual report, and this article further develops their approach by covering additional cybersecurity-related keywords and controls keywords. By doing so, this study gains a deeper understanding of the actual content and nature of the disclosed information. Furthermore, this study adopts a longitudinal approach, focusing on the annual reports of Dutch listed companies published in 2020, 2022, and 2024. This time frame was chosen as it allows for a before-and-after comparison. Taking 2020, the year of the adoption of NIS2 and DORA, as a point of reference, this research goes two years backwards and two years forward. In 2020 the majority of the companies in this study were not subject to any cybersecurity obligations, while in 2024 DORA and NIS2 were about to be enforced.

The remainder of this article proceeds as follows. First, Section 2 addresses the relationship between legislation and compliance, discussing the various ways in which compliance efforts can impact companies. Then, Section 3 provides an overview of the risks and benefits of including cybersecurity information in annual reports. Lastly, Section 4 introduces the empirical research and its results. Section 5 discusses the results and presents its limitations. Section 6 offers a conclusion.

Legislation and compliance

Legislation often struggles to keep pace with technological advancements, with repercussions for the compliance efforts of companies. As technology develops faster than corresponding regulation, the legislator has to choose between legislating without sufficient knowledge or doing nothing in the face of emerging risks (Butenko & Larouche, 2015, p. 66; Marchant, 2011, p. 19; Fenwick et al., 2017, p. 561). As being unresponsive is not an option, the legislator often opts to regulate

new technologies, often in spite of insufficient knowledge and uncertainties, following the principle of risk-based regulation (Berg, 2026, pp. 12–13; Black & Baldwin, 2010, pp. 7–8). However, as discussed in the academic literature, the legislative output appears, at times, suboptimal, creating burdens or redundancies for the entities within its scope.

These burdens or redundancies increase the compliance costs of companies. For instance, the changes in cybersecurity incident response introduced by GDPR and NIS, while building on existing practices, added an additional layer of complexity to companies' practices. Companies had to introduce new mechanisms and bodies, or to modify perfectly working practices, just to ensure compliance (Hurel & Weissinger, 2021, p. 11). Similarly, existing compliance requirements under GDPR and Regulation (EU) 2024/1689 (AI Act) require companies to conduct separate but overlapping assessments, without allowing for the reuse of the same assessment twice for the two different laws (Rintamäki et al., 2026, p. 13). This means that companies risk doubling the compliance costs by duplicating procedures just to avoid legal sanctions. Lastly, the complexity of certain laws has transformed compliance into a commodity over the years. For instance, regarding GDPR, companies are willing to pay third parties to purchase automated assessment, dashboards, or templates to ensure compliance with privacy obligations (de Olazábal, 2026, p. 3). However, this creates a system in which compliance is merely performative rather than a substantive effort to protect rights (van Zeeland, 2024). Compliance with legislation thus appears as a burden that companies are required to bear, rather than a conscious assumption of responsibilities.

This theme has become more relevant since the Draghi report in 2024. The Draghi Report frames legislation on technology, including cybersecurity laws, as a factor that could potentially hinder companies' ability to innovate. Since EU companies must comply with multiple tech laws, much of their resources are spent on regulatory compliance rather than in research and development (R&D) initiatives. In turn, the lack of R&D investments prevents EU companies from growing in the global tech market and positioning themselves as leaders in fields such as artificial intelligence, cloud computing, and quantum computing (Draghi, 2024, pp. 77–81).

However, this paper adopts a different view of legislation. While not denying the intrinsic problems of compliance, this paper aims to look at legislation from another angle. The obligations introduced by the legislation, even when unclear or redundant, represent an input to initiate change. While this input can also lead to modifications of perfectly working practices or redundancies, compliance with legislation requires a mandatory review of internal policies, possibly bringing to light

shortcomings and limitations in existing practices.

The importance of cybersecurity in annual reports

Previous literature has addressed the extent to which EU reporting legislation requires companies to include cybersecurity content in the annual report (Arena et al., 2022; Boggini, 2024; Eijkelenboom & Nieuwesteeg, 2021; Nieuwesteeg et al., 2022). However, the literature has only briefly discussed the practical benefits of including cybersecurity in an annual report. The literature highlights three main benefits for the stakeholders of a company. Firstly, disclosing cybersecurity information signals the ability of the company to resist cyber-attacks (Eijkelenboom & Nieuwesteeg, 2021, p. 4). The ability to be resilient to cyber-attacks ensures business continuity, prevents financial losses, and protects the rights of consumers and end users. Secondly, the inclusion of cybersecurity information in the report signals compliance with cybersecurity legislation (Eijkelenboom & Nieuwesteeg, 2021, p. 4). Nonetheless, aside from these benefits for stakeholders, including this topic in an annual report can also improve how risk is managed internally.

The process of preparing the annual report incentivises internal collaboration among teams, management, and supervisory board (Athanasakou & Boshanna, 2025, p. 5; Galle & Vletter-van Dort, 2025). The reporting process incentivises internal data collection, helping the company assess the effectiveness of its risk management policies. The data gathered can be presented to the different involved teams and offer an opportunity for organisational learning (Athanasakou & Boshanna, 2025, p. 5). Through organisational learning, companies can review their policies and practices, adjust their risk appetite for a specific risk, and enhance their internal risk management framework. Including the topic of cybersecurity comprehensively and understandably in an annual report implies that this information gathering – and also organisational learning – is performed regarding cybersecurity practices and policies. Consequently, these policies are subject to review and subsequent improvements.

Another positive aspect of including cybersecurity in the annual report concerns the responsibilities of the management bodies in cybersecurity under DORA and NIS2 (Boggini 2024, pp. 7–8). Under Article 20 NIS2, the management bodies of the in-scope entities must approve and oversee the implementation of the cybersecurity risk-management measures adopted under Article 21 NIS2. These same bodies can also be held liable for noncompliance with Article 21. Similarly, Article 5(2) DORA requires the management bodies of financial in-scope entities to define, approve, oversee, and take overall responsibility for implementing the ICT risk

management framework. The management bodies should be responsible for managing the financial entity's ICT risk profile and setting its risk appetite, and for ensuring clear and appropriate risk governance. As explained in Section 1, the drafting of annual reports requires the involvement of the management and supervisory bodies. The inclusion of cybersecurity information in the annual report contributes to reinforcing their understanding and ownership over the cybersecurity practices of the company (Boggini 2024, pp. 7-8). In turn, this can help ensure better compliance with the corporate governance dimension of cybersecurity introduced by Article 20 NIS2 and Article 5 DORA.

Academic literature has also theorised a fourth and last benefit associated with the inclusion of cybersecurity information in a company's annual report. Besides the internal effect, including supply chain information in an annual report can also have a positive external effect. According to Eijkelenboom & Nieuwesteeg (2021), including cybersecurity in the annual report can stimulate discussion at the supplier level. The authors believe that suppliers and other affiliated entities might follow the example set by the disclosing company and implement the same cybersecurity measures. In other words, companies along the value chain can read the annual reports and initiate the same organisational learning. While a study analysing how suppliers can use this information is still missing, the literature does not exclude that disclosure of certain information can influence decision-making and risk assessments of stakeholders as suppliers (Amani et al., 2025, pp. 658–659).

However, cybersecurity disclosure should be balanced with security. Excessive details could expose the company to cyber risks. Cyber threat actors could gather details on the security policies or the cyber risk management framework of a company and launch an attack. Still, companies are legally required to report on how they manage financial and non-financial risks – including cyber risks (Boggini, 2024). As reliance on ICTs increases, not including cybersecurity in the annual report would lead to noncompliance with the financial and non-financial reporting obligations and missed opportunity for internal organisational learning.

Ultimately, companies should disclose cybersecurity information in a balanced way. The disclosure should provide a general overview of the cybersecurity risk management framework, including, for instance, references to key cyber controls or relevant international standards. However, the disclosure should avoid detailed descriptions of the operationalisation of these controls or where they apply in the network and information system. An approach such as this would ensure transparency for stakeholder, while maintaining security and prompting organisational learning.

Extent of disclosure²

Time frame and sample composition

To determine whether there is an observable change in how companies disclose cyber risk and supply chain risk, this study will investigate the 2020, 2022 and 2024 annual reports. This research focuses on the 2020, 2022, and 2024 annual reports, as this time frame allows for a before-and-after comparison. 2022 marks the year when NIS2 and DORA were adopted, and this study considers it the starting point of the research. To obtain the before-and-after comparison, this study investigates the annual reports of two years forward and two years backwards from 2022.

In 2020, companies were reasonably aware of the impending adoption of cybersecurity legislation, although they were not aware of its specific content. For NIS2, discussions about updating the EU digital strategy began in 2019. Only in December 2020, the EU published a proposal for NIS2. Similarly, for DORA, starting in 2019, the Commission launched a public consultation to determine whether new cybersecurity regulations for the financial sector were necessary (*European Commission – Financial Services – Improving Resilience against Cyberattacks (New Rules)*, n.d.). It was not until September 2020 that the Commission proposed introducing DORA. Therefore, 2020 was a year when companies were still unaware of the content of future legislation, nor whether the proposal would be adopted. It should be noted that before 2020, another cybersecurity law applied in the EU, namely NIS. NIS was the first EU-wide legislation on cybersecurity, introducing mandatory cybersecurity measures for the in-scope entities (Chiara, 2022, p. 269; Vandezande, 2024, p. 2; Schmitz-Berndt, 2021, p. 580). Compared with NIS2, the scope of NIS was limited, covering only operators of essential services from specific sectors – defined in Annex II NIS – and identified as such by the Member States (MS) under Article 5 NIS. Building on NIS, NIS2 has expanded the scope of its predecessor to include new sectors and replace the discretionary identification with a size cap rule (Schip, 2024, p. 12; Vandezande, 2024, p. 5). Furthermore, along with NIS, GDPR also had – and still has – a cybersecurity dimension, requiring compliance efforts even before 2020. While primarily a privacy law, GDPR requires all companies that process or collect personal data of EU citizens to implement cybersecurity controls to reduce the risk of unauthorised access and breaches of confidentiality (Hoofnagle et al., 2019, p. 87; Kosseff, 2016, p. 405; Tikkinen-Piri et al., 2018, p.

2. For the full data set, please refer to Boggini, C. (2026). *Cybersecurity Disclosure in Dutch Annual Reports [Dataset]*. DataverseNL. <https://doi.org/10.34894/T9HSVE>.

148; Voigt & von dem Bussche, 2017, pp. 3–7). Therefore, for the purpose of this research, it is important to note that some companies in the sample may have already reflected compliance efforts linked to NIS or GDPR in their 2020 annual reports.

On the other side of the timeline for this study, there is 2024, a year when cybersecurity legislation was already adopted. However, it is necessary to state that in 2024, the legislation had not applied to companies yet. For instance, DORA began applying to companies starting from January 2025. NIS2, on the contrary, was supposed to apply starting from October 2024, but delays across MS make its applicability to entities operating in the EU still pending. Notwithstanding, it is reasonable to assume that companies had already started updating their cybersecurity strategies or information security frameworks to comply with the upcoming legislation.

The sample composition for the empirical research comprises the companies listed on the AEX, AMX, and AscX Indices of the Euronext Amsterdam in March 2024. The AEX is the main index, including the 25 largest and most traded companies. The AMX is the mid-cap index, comprising the next 25 largest companies not included in the AEX. The AscX is the small-cap index, consisting of the next 25 largest companies not included in the AMX. Overall, the indices contain 75 public companies.³ Table 1 lists the companies that were part of these three indices in March 2024.

TABLE 1: List of companies part of the AEX, AMX, AscX index in March 2024

COMPANY'S NAME	INDEX	COMPANY'S NAME	INDEX	COMPANY'S NAME	INDEX
ABN AMRO	AEX	AALBERTS	AMX	A COMO	ASCX
ADYEN	AEX	AIR FRANCE – KLM	AMX	ACCSYS	ASCX
AEGON	AEX	ALFEN	AMX	AVANTIUM	ASCX
AHOLD	AEX	ALLFUNDS GROUP	AMX	AZERION	ASCX
AKZO NOBEL	AEX	AMG	AMX	B&S GROUP	ASCX
ARCELORMITTAL	AEX	APERAM	AMX	BAM GROUP KON	ASCX
ASM INT	AEX	ARCADIS	AMX	BRUNEL	ASCX

3. The composition of the indices is derived from Euronext Amsterdam - AEX | Live in March 2024

COMPANY'S NAME	INDEX	COMPANY'S NAME	INDEX	COMPANY'S NAME	INDEX
ASML	AEX	BASIC-FIT	AMX	CM.COM	ASCX
ASR	AEX	CORBION	AMX	EBUSCO HOLDING	ASCX
BE SEMICONDUCTOR	AEX	CTP	AMX	FASTNED (FAST)	ASCX
DSM	AEX	EUROCOMMERCIAL	AMX	FORFARMERS	ASCX
EXOR NV	AEX	FAGRON	AMX	HEIJMANS	ASCX
HEINEKEN	AEX	FLOW TRADERS	AMX	KENDRION	ASCX
IMCD	AEX	FUGRO	AMX	NEDAP	ASCX
ING GROEP	AEX	GALAPAGOS	AMX	NSI	ASCX
KPN	AEX	INPOST	AMX	NX FILTRATION	ASCX
NN GROUP	AEX	JDE PEET'S	AMX	PHARMING GROUP	ASCX
PHILIPS	AEX	JUST EAT TAKEAWAY	AMX	PostNL	ASCX
Prosus	AEX	OCI	AMX	RENEWI	ASCX
RANDSTAD	AEX	SBM OFFSHORE	AMX	SIF	ASCX
RELX	AEX	SIGNIFY	AMX	SLIGRO	ASCX
SHELL	AEX	TKH GROUP	AMX	THEON INTERNAT	ASCX
UMG	AEX	V LANSCHOT KEMPEN (VLK)	AMX	Tomtom	ASCX
UNILEVER	AEX	VOPAK	AMX	Vastned	ASCX
WoltersKluwer	AEX	WDP	AMX	WERELDHAVE	ASCX

I reviewed the sample to ensure that all 75 companies were listed on Euronext Amsterdam in 2020, 2022, and 2024. Companies not listed during these years would not have been subjected to the same financial reporting obligations, and, therefore, this could bias the sample. Thus, the final sample includes only the companies that remained continuously listed on the Amsterdam Euronext throughout the selected period. As a result, I excluded eight companies, leaving a final sample of 67 companies: 23 from the AEX, 23 from the AMX, and 21 from the As-cX. The selected 67 companies operate across different sectors and Table 2 shows their distribution by sector. Almost one-fourth of the sample operated in the man-

ufacturing and industry, followed by companies in the chemical and food production sector, and those in the digital infrastructure sector (Figure 1).

TABLE 2: Sectoral distribution of the 67 sample companies

SECTOR	NR COMPANIES
Chemical & Food Production	13
Digital & ICT Infrastructure	8
Energy	4
Financial Entities	7
Health & Pharmaceuticals	5
Manufacturing & Industry	16
Other	9
Postal & Logistics	2
Research	1
Transport	1
Waste	1
Total	67

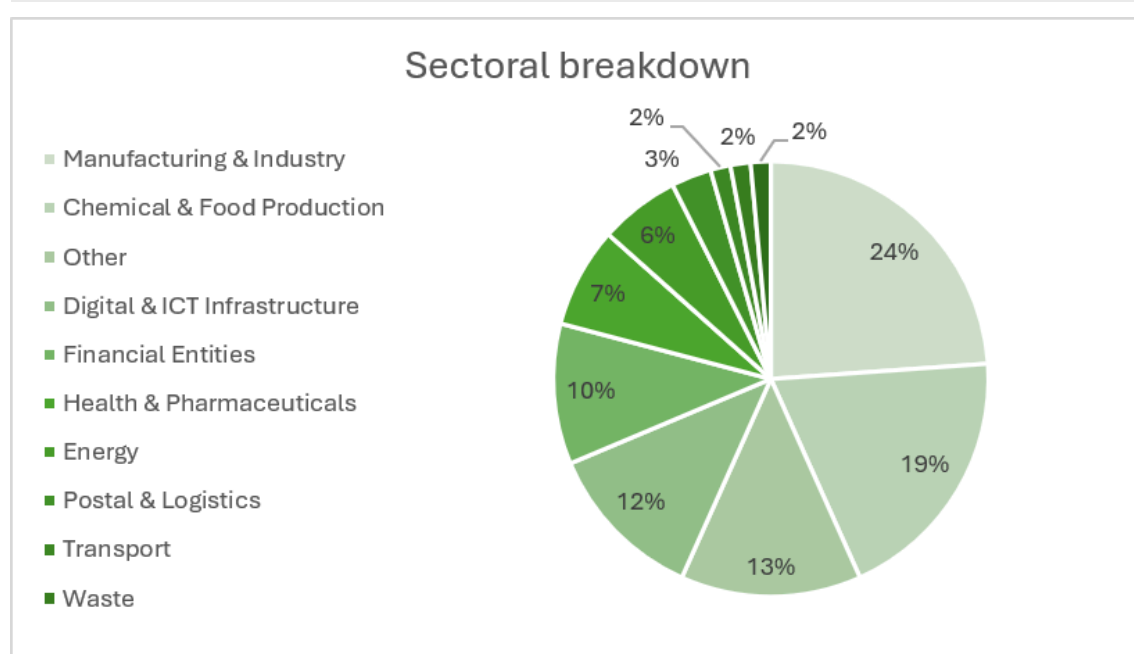


FIGURE 1: Sector breakdown of the 67 sampled companies.

Data Collection and methodology

This study used a keywords methodology. The keywords methodology, also defined as text mining or word frequency analysis, has several variants and is used to analyse the content of large volumes of textual data (Witten, 2004, p. 314; Sebastiani, 2002). In its most traditional approach, the keywords methodology entails first selecting documents from which the most frequent words are extracted. This document and the frequency of its words are later compared with a second document with the respective word frequency analysis (Archer, 2016, p. 2). Through this methodology, a researcher can identify with relative ease and in a systematic fashion patterns and variances in the documents, thus making inferences or qualitative evaluations (Archer, 2016, p. 2; Witten, 2004, p. 314, Weber, 1990, p. 10; Stemler, 2001, p. 1; Sebastiani, 2002). This methodology has been applied to a variety of research fields and documents, including legal and policy ones to identify patterns for policy or legal prediction (Laver et al., 2003; Archer, 2022, p. 87; Hietala, 2014). Most importantly, the keywords methodology represents a user-friendly and time-effective method for analysing large data sets, while maintaining methodological transparency and guaranteeing verifiable output (Stemler, 2001, p. 1; Archer, 2022, p. 87).

The study at hand has adopted the keywords methodology with a variation. As this study focuses solely on cybersecurity, I selected a set of keywords at the outset of the data collection to limit the analysis of the word frequency. In this way, I was able to quickly isolate the content in the annual reports related to cybersecurity and focus the analysis only on these words. I compared the word frequencies of each annual report with the word frequencies of the annual reports of the following selected years. This process allowed me to highlight patterns in cybersecurity disclosures and compare them with the legislative timeline. By doing so, I could answer the research question underpinning this article while ensuring methodological transparency and verifiable results. Furthermore, I replicated the methodology used in a study investigating cybersecurity disclosure in 2018 Dutch annual reports (Eijkelenboom & Nieuwesteeg, 2021).

For each company in the sample, I downloaded the annual reports for 2020, 2022, and 2024 directly from their official websites. After downloading the annual reports, I conducted an initial round of keyword research. In this first phase, I searched for the following keywords or words containing the following stem:

- Cyber(-)
- Information Security
- Information Technology

- Information Technology security
- IT security
- Data security

I selected these words because they are all related to cybersecurity. Firstly, I recorded the frequency of each keyword, then extracted the paragraphs from the reports that mentioned them. When keywords were found in a table, I retrieved the full row in which each keyword appeared, to preserve the surrounding context and associated data. If a keyword appeared in a graph, I extracted the keyword along with both the horizontal and vertical axis labels to understand what the graph was measuring and how the keyword related to it. Furthermore, I also recorded the page number and the section of the annual report where the keyword appeared. Each search hit was verified by hand, meaning the information surrounding the keyword was read and interpreted to ensure it concerned cybersecurity.

After identifying the sections where companies disclosed cybersecurity information, I carried out a second round of keyword research. This second round of keywords search was conducted on the extracted paragraphs or texts obtained in the previous phase of the research. In this phase, I focused on a different set of keywords to analyse the nature of the cybersecurity measures and supply chain security information disclosed by the companies. Table 3 lists all the selected keywords and the associated cybersecurity and supply chain security controls.

TABLE 3: Key words selected to represent supply chain security information or controls information

CYBERSECURITY CONTROL	KEYWORDS
Supply chain security practices	"third party", "third parties", "third party service provider", "third party service providers", "third party vendors", "vendors", "vendor", "third party vendor", "third party risks", "third party risk", "third-party", "third-parties", "third-party service provider", "third-party service providers", "third-party vendors", "third-party vendor", "third-party risks", "third-party risk", "service provider", "service providers", "supplier", "suppliers", "partner", "partners", "supply chain", "supply chain security"
Incident management	"incident handling", "vulnerability handling", "vulnerability management", "incident management", "incident reporting"
Business continuity	"business continuity", "business continuity plan"
Testing	"testing", "penetration test", "test", "tests", "tested"
Access management	"access control", "access management", "control management", "access controls"

CYBERSECURITY CONTROL	KEYWORDS
Data management	"data management", "asset management"
Secure communication	"multifactor authentication", "multi-factor authentication", "two-factor authentication", "two factor authentication"
Monitoring	"monitoring", "monitor", "monitors", "monitored"
Training	"training", "awareness", "training awareness", "trainings", "awareness training", "awareness trainings"
Security policy	"framework", "policy", "policies", "frameworks"

The selected keywords were deliberately broad, making them suitable for use in annual reports. Given the need to balance disclosure with security, these terms enable companies to provide relevant cybersecurity information without disclosing sensitive or detailed data.

I recorded the frequency of each keyword in this second group, verifying by hand that the information presented around the search hit related to cybersecurity. During this phase, while verifying by hand the information, I recorded noteworthy examples of cybersecurity disclosure. I chose these examples based on the completeness of the information provided and the extent to which stakeholders could use this information to determine the cybersecurity posture of a company.

At the start of the research, I conducted a pilot study with these words. I randomly selected five annual reports and manually verified that the search terms covered all the cybersecurity and supply chain cybersecurity information in those annual reports. After the pilot, for each company, I analysed the 2020 annual report by first locating the cybersecurity related keywords and then analysing the extracted text to determine the presence of cybersecurity controls keywords and supply chain security keywords. I then repeated the same process for the 2022 and 2024 annual report.

Results

Data analysis: cybersecurity keywords

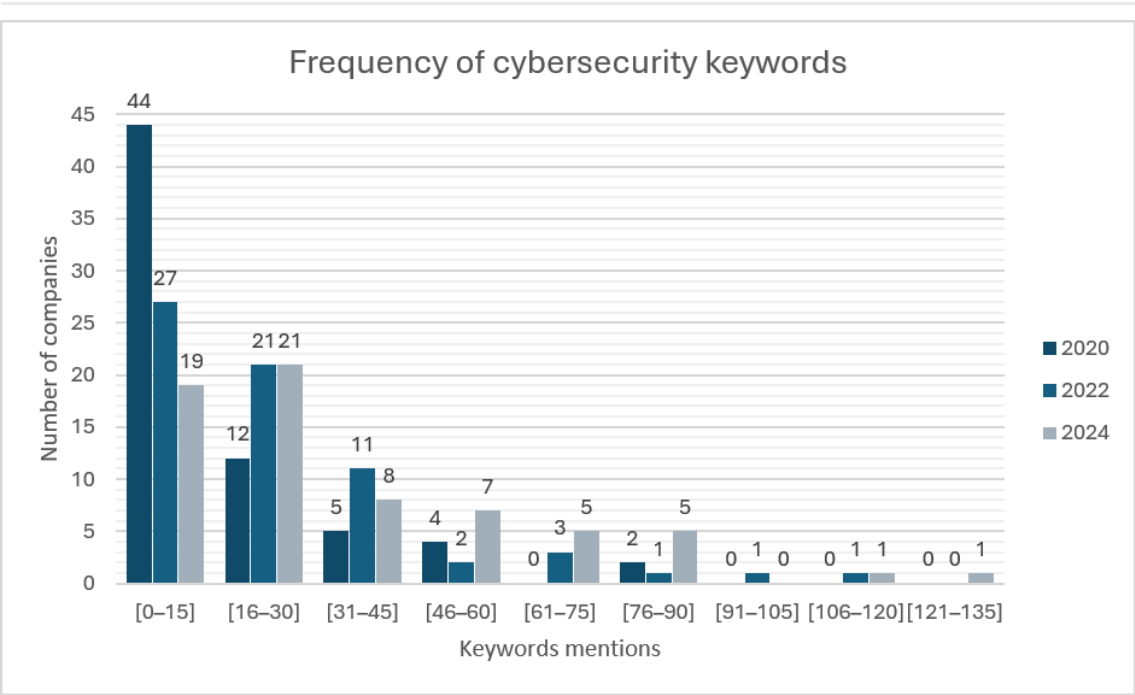


FIGURE 2: Frequency distribution of cybersecurity keyword mentions in annual reports (2020–2024). The figure shows an increase in the number of companies including cybersecurity-related keywords.

TABLE 4: Maximum and minimum value registered in cybersecurity keywords mentioned each year across sample

	2020	2022	2024
MAX	86	108	132
MIN	0	1	0

The analysis of the data revealed a substantial increase in the frequency of cybersecurity keywords mentioned in company reports over the years. I categorised the data into nine brackets, each representing 15 mentions, and I assigned each company to the bracket corresponding to its number of mentions. This analysis highlights a growing focus on cybersecurity in annual reporting. As shown in Figure 2, in 2020, a majority of companies (66%) made limited reference to cybersecurity, mentioning the selected keywords fewer than 15 times. However, a noteworthy 9% of the annual reports mentioned the cybersecurity keywords more than 45 times, with one company reaching the maximum recorded value of 86 mentions.

By 2022, I observed a substantial shift in the frequency distribution of cybersecuri-

ty keyword mentions. The number of companies in the 0-15 bracket dropped from 44 to 27, indicating a general increase in the other frequency brackets. While the largest share of companies (40%) still fell into the lowest reporting bracket, there was a noticeable increase in the other brackets. Companies mentioning cybersecurity keywords between 16 and 45 times nearly doubled – from 25% in 2020 to 48% in 2022. This shift in distribution confirms the increasing importance of cybersecurity in corporate discussions.

In 2024, the trend of increased cybersecurity keyword mentions continued, further underlining the importance of cybersecurity in the corporate world. The 16-30 keywords bracket was the most populated (31% of the sample), while the proportion of companies with the lowest disclosure (0 -15 mentions) further declined to 28% of the sample. Furthermore, the mid-range buckets (above 46 and below 91 mentions) substantially increased, rising from only 9% of the sample in 2022 to 25% in 2024. The highest brackets (from 91 mentions) remained unchanged, with only two companies in both 2022 and 2024. However, the highest recorded value increased from 108 to 132, signalling a further right shift in the histogram even within the high-range bracket.

There is a noticeable upward trend in the inclusion of cybersecurity keywords in the annual reports of Dutch companies. This trend was further contextualised by disaggregating and reaggregating the data based on the AEX, AMX, and AscX indices. This approach allows me to identify potential differences in how companies of varying sizes and capital structures disclose cybersecurity information. I then calculated the mean of the recorded values per index. The mean, calculated through the mathematical mean, provides an overview of the average recorded frequency in the index.

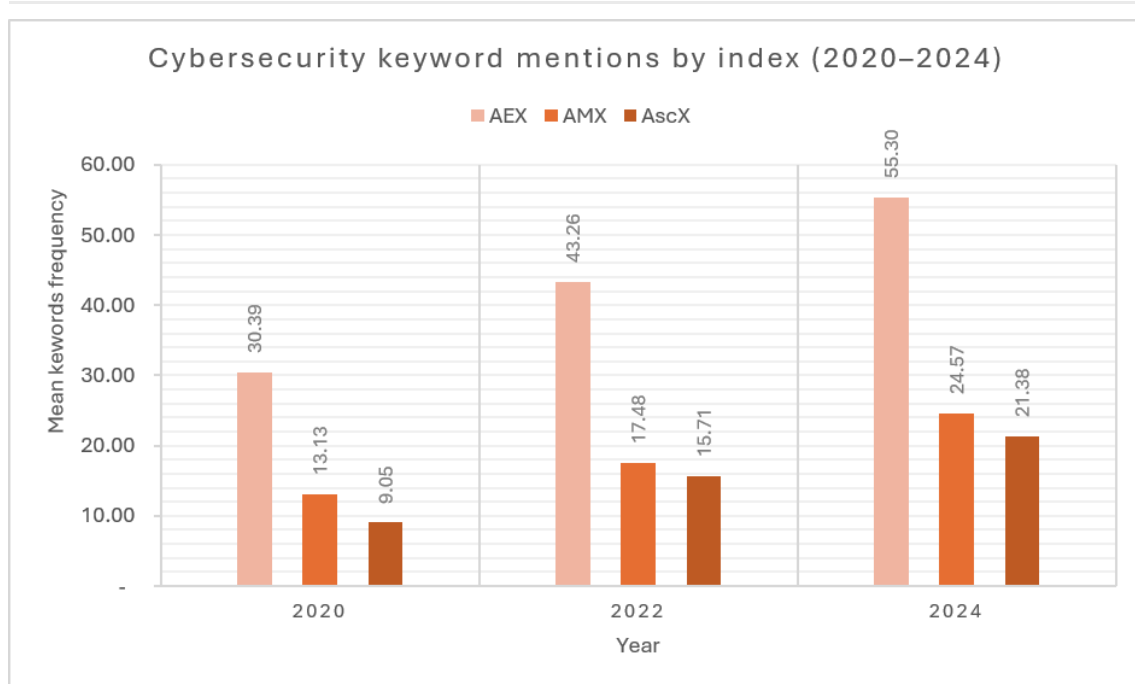


FIGURE 3: Cybersecurity keyword frequency mean by index (AEX, AMX, and AscX). The figure compares the mathematical mean of cybersecurity keyword mentions across companies listed on the AEX, AMX, and AscX indices in 2020

Figure 3 shows that AEX index companies consistently lead in cybersecurity keyword mentions compared to AMX and AscX index companies. Over the observed period, the upper and mid frequency brackets were predominantly occupied by AEX companies, indicating their strong focus on cybersecurity. Large-cap companies, in general, included more cybersecurity information in their annual reports than mid-cap and small-cap companies. Cybersecurity has undoubtedly gained relevance in the annual reports of Dutch companies, with AEX companies leading the trend in including more cybersecurity information.

Lastly, to better contextualise the growth in mentions of cybersecurity keywords, I compared the frequency of cybersecurity keywords across three time intervals: 2020-2022, 2022-2024, and 2020-2024. This comparative analysis allows me to identify both increases and decreases in the frequency of cybersecurity keywords disclosed by each company at the beginning and at the end of the interest interval. More precisely, the comparative analysis allows me to contextualise the extent of growth in cybersecurity mentions in comparison with the adoption of cybersecurity legislation. By comparing the 2020-2022 with the 2022-2024 time interval, this study can determine whether the observed growth in mentions for each company occurred before or after the adoption of NIS2 and DORA. The overarching time interval (2020-2024) offers me insights into the overall growth trend.

To do so, I calculated the mathematical difference between the value recorded at the beginning of the interval and at the end of the interval. Additionally, I recorded the maximum and minimum changes registered. Furthermore, I calculated the sample mathematical mean and the sample standard deviation for each interval. The mean allows me to determine the overall trend of increases or decreases in cybersecurity keywords during the given interval. The standard deviation of the sample offers insights into how widespread the data is compared to the mean, i.e., whether the companies increased or decreased the number of cybersecurity keywords uniformly, or if the change happened only within limited companies.

TABLE 5: Changes in cybersecurity keyword mentions between 2020, 2022, and 2024. The table summarises the mean, maximum, minimum, and standard deviation of changes in the number of cybersecurity keyword mentions between reporting years

	DIFFERENCE 2020-2022	DIFFERENCE 2022-2024	DIFFERENCE 2020-2024
MEAN	7.99	8.36	16.34
MAX	43	80	85
MIN	-19	-24	-20
STDDEV	10.93	19.30	19.39

The comparative analysis shows an upward trend in cybersecurity disclosure, along with consistent variability across the sample. In the 2020-2022 interval, as shown in the stacked bar of Figure 4, 76% of the sample increased the number of cybersecurity keywords, while only 18% decreased. In the 2022-2024 time interval, while 61% of the sample increased the number of cybersecurity keywords, the number of companies decreasing the cybersecurity keywords almost doubled from 12 to 23 companies. This data shows that, while the frequency of cybersecurity keywords increased across the three years, the most substantial increase occurred mainly in the first time interval, i.e., 2020-2022. Nonetheless, across the entire 2020-2024 time period, the growth was consistent. The right-skewed stacked bar in Figure 4 shows that 82% of companies increased the number of cybersecurity keywords, while only 15% decreased it over the entire period. Overall, while undeniable growth was visible in the overarching 2020-2024 period, the increase in the 2020-2022 interval did not reflect the same symmetric increase in the 2022-2024 period. The spike in attention to cybersecurity occurred over the 2020-2022 interval, followed by a decrease in interest among some companies.

The recorded standard deviation confirms this (Table 5). In the 2022-2024 interval (Figure 4), some companies substantially increased their mentions of cybersecurity

keywords, reaching up to 80 more mentions, while others reduced their mentions by as much as 24. The relatively high standard deviation of 19.30 highly reflects the presence of both positive and negative outliers within the time interval. Even though the standard deviation remained around 19.30 over the overarching period, the 2020-2024 graph is more right-skewed, suggesting the presence of more positive outliers rather than negative ones.

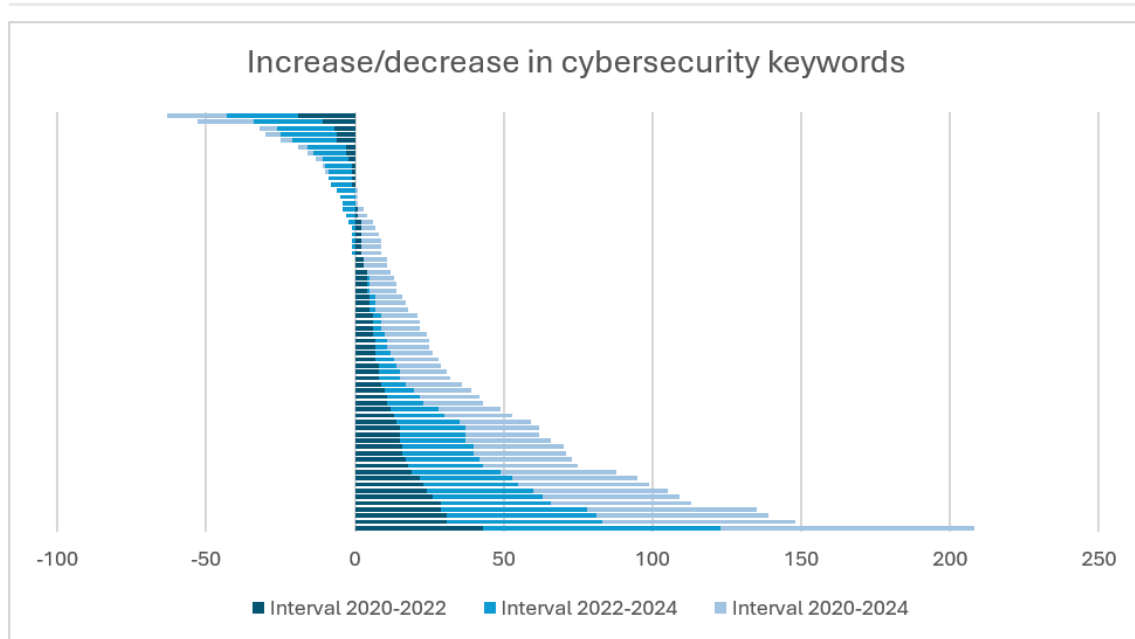


FIGURE 4: Change in cybersecurity keyword mentions between 2020 and 2024. The figure illustrates the variation in the number of cybersecurity keyword mentions per company in the three selected intervals: 2020-2022, 2022-2024, and 2020-2024

Data analysis: Supply chain keywords and controls keywords

Having established that attention to cybersecurity has increased over the years, this paper proceeds to analyse the content disclosed regarding cybersecurity using data on the frequency of supply chain and controls keywords.

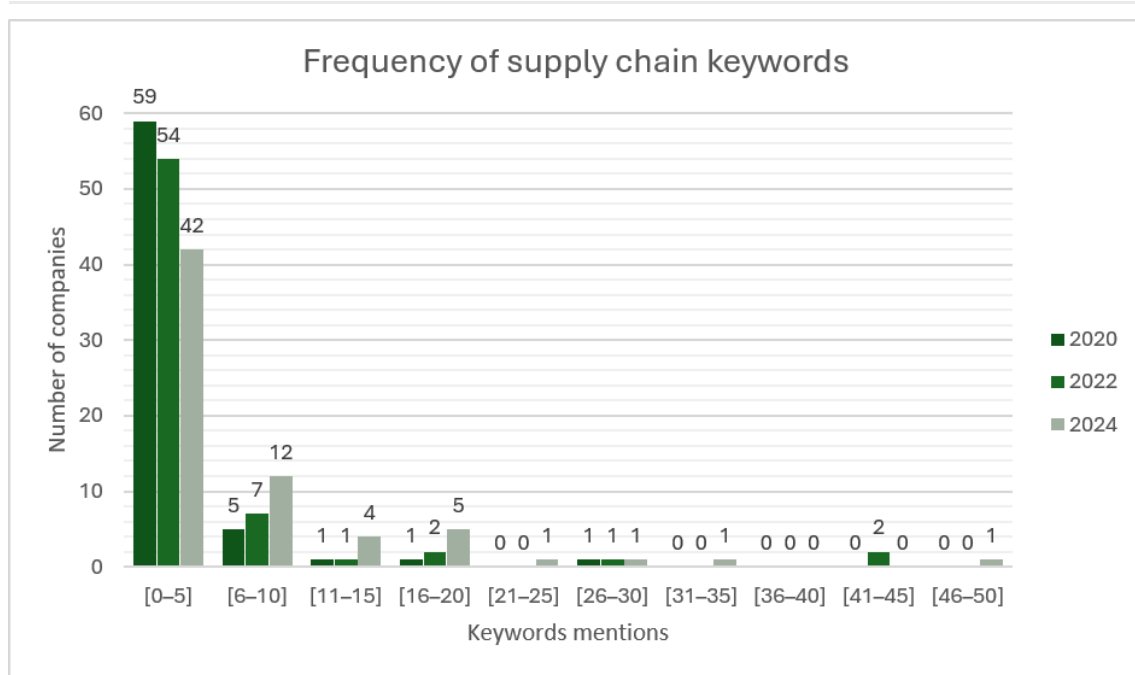


FIGURE 5: Frequency distribution of supply chain keyword mentions in annual reports (2020–2024). The figure shows an increase in the number of companies including supply chain-related keywords.

What immediately emerges is that, over the years, the mentions of supply chain keywords remained almost entirely in the first four frequency brackets (Figure 5). In 2020, 88% of the sample fell within the 0-5 bracket, a figure that decreased to 81% in 2022. However, the number of companies with zero mentions decreased by almost one-third, from 34 in 2020 to 24 in 2022, representing a substantial improvement. This data suggests a modest increase in the inclusion of supply chain security information in annual reports. By 2024, the lowest-frequency bracket included only 63% of the companies; nevertheless, it was the majority of the sample. The 6-10 bracket saw a gradual increase, rising from five in 2020 to 12 in 2024. This slow and limited increase trend is further confirmed by the fact that, in 2024, 13 companies disclosed more than 11 keywords, a substantial increase from 2020, when only three companies did so.

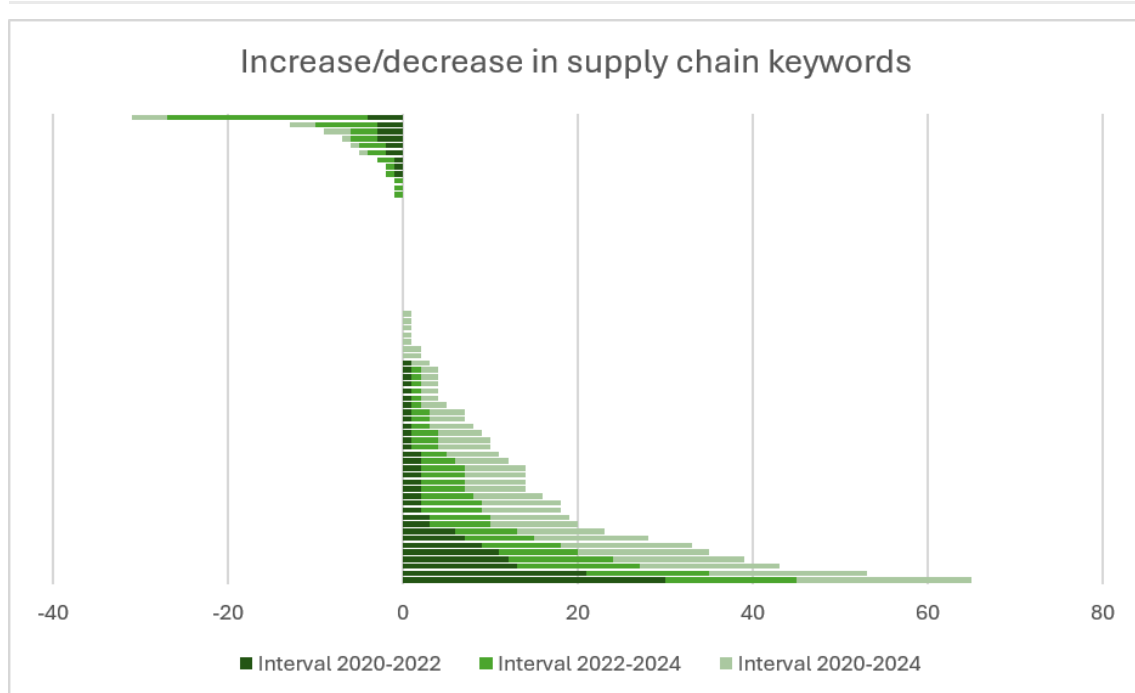


FIGURE 6: Change in supply chain keyword mentions between 2020 and 2024. The figure illustrates the variation in the number of supply chain keyword mentions per company in the three selected intervals: 2020-2022, 2022-2024, and 2020-2024

TABLE 6: Changes in supply chain keyword mentions between 2020, 2022, and 2024. The table summarises the mean, maximum, minimum, and standard deviation of changes in the number of supply chain keyword mentions between reporting years

	DIFFERENCE 2020-2022	DIFFERENCE 2022-2024	DIFFERENCE 2020-2024
MEAN	1.89	1.82	3.70
MAX	30	15	20
MIN	-4	-23	-4
STDDEV	5.26	5.27	5.39

When comparing the time intervals, the registered changes remain relatively low across the three analysed intervals. In both the first and second time intervals, each company, on average, added two more words and nearly four words in the overarching 2020-2024 time interval (Table 6). However, as highlighted by the relatively moderate-high standard deviation (which remained around five mentions), the distribution of this increase was not uniform across the sample. While the topic gained prominence in the annual reports, its distribution remained quite spread and uneven within the sample. Nonetheless, the overall time interval from 2020 to 2024 confirms that growth occurred, although in some cases it was minimal (Fig-

ure 6). More than half of the sample (58%) increased the keywords supply chain mentions, 33% remained unchanged, and only 9% of the companies decreased the number of mentions.

Overall, supply chain security issues still play a marginal role in annual reports. Nevertheless, the security of the supply chain is only one aspect of cybersecurity, and this data should be analysed in the broader context of cybersecurity in annual reports. As cybersecurity information has become more prevalent, mentions of supply chain security have increased (albeit modestly), confirming the relevance of cyber supply chain issues in corporate discussions.

As previously done for the supply chain words and for cybersecurity, I grouped the data on the frequency of control keywords to assess the extent to which reporting has changed over time.

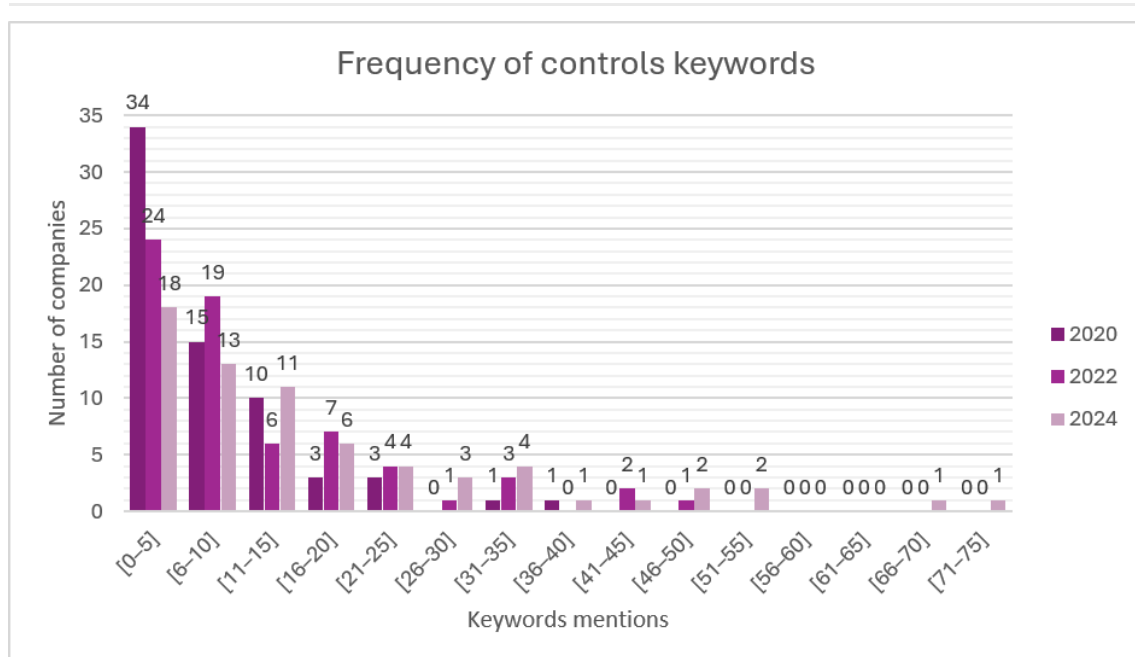


FIGURE 7: Frequency distribution of controls keyword mentions in annual reports (2020–2024). The figure shows an increase in the number of companies including controls related keywords.

Data on control keywords behaved similarly to data on supply chain keywords. Over the three years, the vast majority of the sample was concentrated in the first five brackets, i.e., with 0-25 control keywords in their annual report (Figure 7). Nonetheless, the histogram shows an evident and progressive leftward shift. In 2020, the inclusion of control keywords was quite limited. Over half of the companies (51%) mentioned only 0-5 controls keywords. By 2022, the number of companies in the lowest bracket had dropped to just 24, while more than half of the

sample (54%) fell into the next four frequency brackets (6-25). By 2024, these four brackets accounted for 51% of the sample, signalling a decrease in the first five brackets in favour of mid- and high-range brackets. The number of companies in these medium and high-range brackets rose substantially from two in 2020 to seven in 2022, and then to 14 in 2024, indicating a growing trend towards higher controls keyword disclosure.

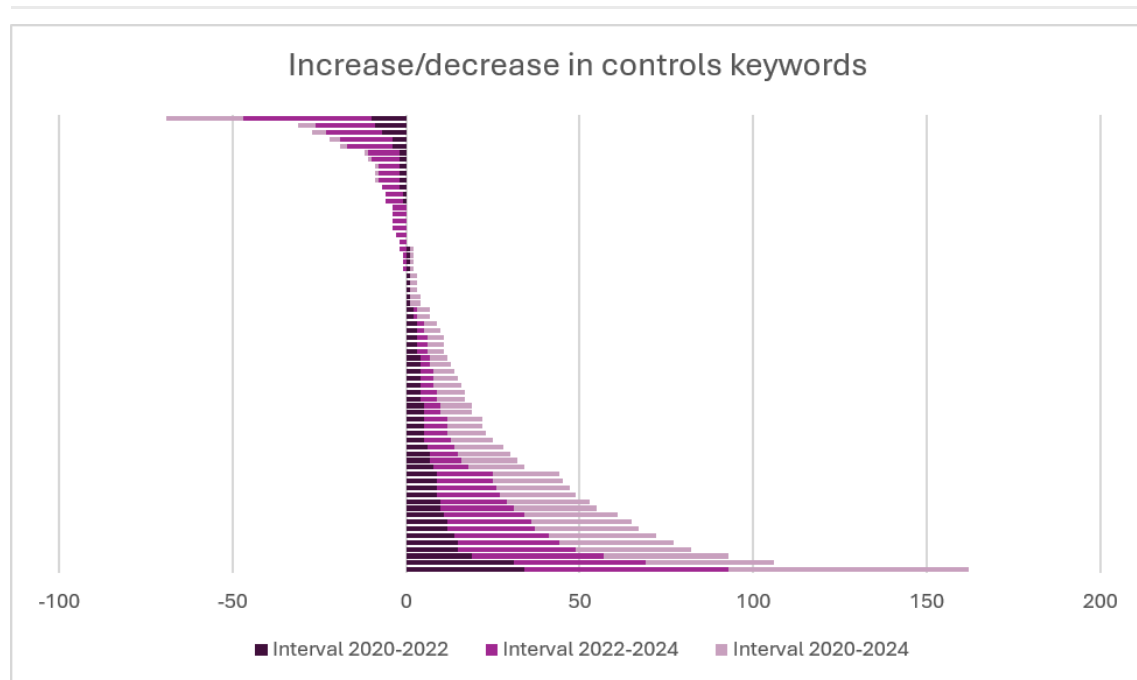


FIGURE 8: Change in controls keyword mentions between 2020 and 2024. The figure illustrates the variation in the number of controls keyword mentions per company in the three selected intervals: 2020-2022, 2022-2024, and 2020-2024

TABLE 7: Changes in supply chain keyword mentions between 2020, 2022, and 2024. The table summarises the mean, maximum, minimum, and standard deviation of changes in the number of controls keyword mentions between reporting years

	DIFFERENCE 2020-2022	DIFFERENCE 2022-2024	DIFFERENCE 2020-2024
MEAN	4.25	5.18	9.43
MAX	34	59	69
MIN	-10	-37	-22
STDDEV	7.44	14.77	13.78

Lastly, the comparative analysis gives insights into how the growth happened. The mean of the registered changes in the three intervals confirms the growing trend (Table 7). In the first time interval (2020-202), each company, on average, added

four additional control keywords to its annual reports. By the second time interval (2022-2024), the number of words further increased by five words, resulting in a total mean growth of nine words in the overall time period (2020-2024). However, as indicated by the high standard deviation and Figure 8, the growth was uneven. While the majority of companies (72%) increased the mentions of controls in the first interval, in the second interval the growth slowed. Between 2022 and 2024, 58% of the sample continued to include more control keywords in their annual reports, while 34% reduced them. The higher mean in the second interval is explained by the overall increase in the frequency of mentions registered throughout the sample (Figure 8). Nonetheless, despite this decrease in the second interval, the overall period shows a substantial surge in the number of mentions. Figure 8 shows a right-skewed distribution, indicating that most companies (48 out of 67) increased the number of mentions during the 2020-2024 period. Despite the uneven growth, the overall trend is one of progress, with the annual reports providing more details and insights into cybersecurity risk management.

Data analysis: Comparison by legislation

Overall, the data confirms observable growth in the 2020-2024 period regarding the inclusion of cybersecurity information in annual reports. At the beginning of the study, for each company, I identified the sectors in which the company operated. Determining the sector helps understand the applicability of cybersecurity legislation. For the final part of this study, I conducted an additional analysis by aggregating the data according to the scope of NIS2 and DORA. This analysis allows for determining whether observable changes were recorded based on the applicability of cybersecurity legislation.

As explained earlier, some of the companies in this study were already within the scope of NIS. I also sought to identify the companies that may have reflected NIS compliance efforts in 2020 by referring to the previous study on cybersecurity disclosure in 2018 Dutch annual reports (Eijkelenboom & Nieuwesteeg, 2021). While the identification as an essential services operator was fully at the discretion of the single MS (Vandezande, 2024, p. 6), Eijkelenboom & Nieuwesteeg assumed the identification as essential operator of a few companies part of the 2018 AEX, AMX, and AscX indices. However, when comparing the composition of the 2018 indices with that of 2024, only four companies out of 67 were within the scope of NIS (Eijkelenboom & Nieuwesteeg, 2021, p. 11). The limited number of companies and the fact that identification was at the discretion of MS prevented me from definitively isolating the companies within the scope of NIS and making further evaluations.

Therefore, after identifying the sector in which each company operates, I conducted an assessment to determine which companies were within the scope of the NIS2 and which were within the scope of NIS2-DORA.⁴ I made the assessment based on information available on the companies' official website and in accordance with the requirements set out in Article 2 NIS2 and Article 2 DORA. Over half of the companies were within the NIS2 scope, while only 16% were within the DORA-NIS2 scopes. Either legislation did not cover the remaining 21%. Overall, more than three-quarters of the sample are required by either DORA or NIS2 to adopt cybersecurity controls or a cybersecurity risk framework.

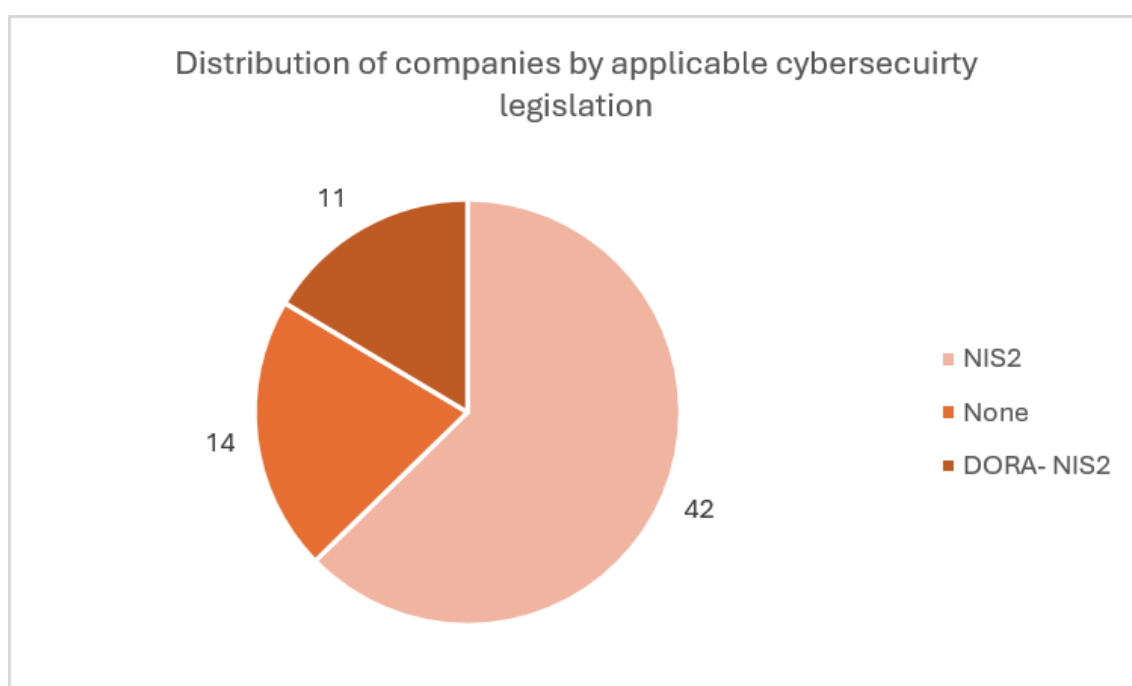


FIGURE 9: *Distribution of companies by applicability of cybersecurity legislation (NIS2 and DORA)*

I disaggregated and reaggregated the collected data based on the scope of DORA-NIS2, NIS2, or no legislation. For each group, I calculated the sample mathematical mean and standard deviation from the frequency of keywords in 2020, 2022, and 2024. Additionally, for each year, I recorded the highest and lowest registered values. Furthermore, for each group and keyword set, I conducted a comparison over a two-year time interval. For each time interval (2020-2022, 2022-2024, 2020-2024), I calculated the sample mathematical mean, standard deviation, and maximum and minimum registered values. Tables 8, 9, and 10 below show the

4. NIS2 scope overlaps with DORA scope. DORA is *lex specialis* when compared to NIS2 (Article 3 DORA). As stated in recital 16 DORA, DORA introduces more stringent risk management and reporting requirements in NIS2. For this reason DORA can be deemed *lex specialis* and NIS2 shall not apply (Article 4 NIS2).

findings.

TABLE 8: Descriptive statistics of cybersecurity keyword mentions by legislative scope (2020–2024). The table summarises the mean, maximum, minimum, and standard deviation of cybersecurity keyword mentions for companies subject to DORA–NIS2, NIS2 only, and no cybersecurity legislation.

CYBERSECURITY KEY WORDS						
DORA-NIS2	Total 2020	Total 2022	Total 2024	Difference 2020-2022	Difference 2022-2024	Difference 2020-2024
MEAN	36.64	48.45	63.91	11.82	15.45	27.27
MAX	86.00	108.00	132.00	31.00	49.00	65.00
MIN	6.00	2.00	25.00	-19	-15	-20
STDDEV	29.80	31.52	32.79	17.47	20.44	22.99

NIS2	TOTAL 2020	TOTAL 2022	TOTAL 2024	DIFFERENCE 2020-2022	DIFFERENCE 2022-2024	DIFFERENCE 2020-2024
MEAN	14.60	22.31	30.64	7.71	8.33	16.05
MAX	48.00	91.00	110.00	43.00	80.00	85.00
MIN	0	2.00	1.00	-6	-24	-4
STDDEV	11.23	16.54	23.39	10.11	19.56	17.77

NONE	TOTAL 2020	TOTAL 2022	TOTAL 2024	DIFFERENCE 2020-2022	DIFFERENCE 2022-2024	DIFFERENCE 2020-2024
MEAN	12.50	18.36	21.14	5.86	2.79	8.64
MAX	40.00	51.00	68.00	19.00	50.00	58.00
MIN	0	1.00	0	-3	-23	-19
STDDEV	11.98	13.55	19.39	5.50	16.98	18.49

TABLE 9: Descriptive statistics of supply chain keyword mentions by legislative scope (2020–2024). The table summarises the mean, maximum, minimum, and standard deviation of supply chain keyword mentions for companies subject to DORA–NIS2, NIS2 only, and no cybersecurity legislation

SUPPLY CHAIN KEYWORDS						
DORA-NIS2	Total 2020	Total 2022	Total 2024	Difference 2020-2022	Difference 2022-2024	Difference 2020-2024

SUPPLY CHAIN KEYWORDS						
MEAN	6.27	8.27	11.91	2.00	3.64	5.64
MAX	30.00	41.00	48.00	11.00	14.00	18.00
MIN	0	0	0	-2	-3	-3
STDDEV	9.22	11.88	15.08	3.58	5.48	7.15

NIS2	TOTAL 2020	TOTAL 2022	TOTAL 2024	DIFFERENCE 2020-2022	DIFFERENCE 2022-2024	DIFFERENCE 2020-2024
MEAN	1.83	3.93	5.86	2.10	1.93	4.02
MAX	13.00	43.00	29.00	30.00	15.00	20.00
MIN	0	0	0	-3	-23	-3
STDDEV	2.93	8.35	7.13	6.06	5.76	5.34

NONE	TOTAL 2020	TOTAL 2022	TOTAL 2024	DIFFERENCE 2020-2022	DIFFERENCE 2022-2024	DIFFERENCE 2020-2024
MEAN	0.79	1.93	2.00	1.14	0.07	1.21
MAX	5.00	13.00	9.00	13.00	5.00	7.00
MIN	0	0	0	-4	-7	-4
STDDEV	1.63	3.52	3.14	3.72	2.67	2.86

TABLE 10: Descriptive statistics of controls keyword mentions by legislative scope (2020–2024). The table summarises the mean, maximum, minimum, and standard deviation of controls keyword mentions for companies subject to DORA–NIS2, NIS2 only, and no cybersecurity legislation.

CONTROLS KEYWORDS						
DORA-NIS2	Total 2020	Total 2022	Total 2024	Difference 2020-2022	Difference 2022-2024	Difference 2020-2024
MEAN	13.64	19.45	34.09	5.82	14.64	20.45
MAX	38.00	42.00	75.00	19.00	59.00	69.00

CONTROLS KEYWORDS						
MIN	0	1.00	3.00	-4	-16	-4
STDDEV	11.79	13.89	25.07	7.10	21.31	21.85

NIS2	TOTAL 2020	TOTAL 2022	TOTAL 2024	DIFFERENCE 2020-2022	DIFFERENCE 2022-2024	DIFFERENCE 2020-2024
MEAN	6.33	10.14	14.71	3.81	4.57	8.38
MAX	32.00	47.00	48.00	34.00	38.00	37.00
MIN	0	0	0	-10	-37	-5
STDDEV	6.16	9.02	12.73	6.95	13.41	10.59

NONE	TOTAL 2020	TOTAL 2022	TOTAL 2024	DIFFERENCE 2020-2022	DIFFERENCE 2022-2024	DIFFERENCE 2020-2024
MEAN	6.50	10.86	10.43	4.36	-0.43	3.93
MAX	23.00	41.00	34.00	31.00	16.00	20.00
MIN	0	0	0	-9	-17	-22
STDDEV	6.98	11.55	10.08	9.34	8.94	10.23

On average, companies subject to both DORA and NIS2 outperformed those subject to either only NIS2 or no legislation (Tables 8, 9, 10). DORA-NIS2 companies performed better not only in the single-year comparison but also in the interval comparison. The total yearly data on cybersecurity keywords, supply chain security, and control keywords indicate that DORA-NIS2 companies have included more keywords each year, signalling a more open and detailed discussion of cybersecurity issues than the other companies in the sample. Furthermore, in the three-year interval comparison, DORA-NIS2 companies systematically included, on average, more cybersecurity, supply chain, and control keywords than NIS2 and no-legislation companies. This data confirms that, compared with other companies, DORA-NIS2 companies increased the most in the disclosure of cybersecurity information. Consequently, this signals that, on average, companies in the financial sector were providing increasingly detailed information to stakeholders about their cybersecu-

rity practices. Nonetheless, as indicated by the high standard deviation, growth was not uniform across the three groups, even in the DORA-NIS2 group. In each group, some companies were more inclined than others to disclose cybersecurity information, making it impossible to determine regular patterns in growth.

Examples of disclosure

During data collection, I recorded noteworthy examples of cybersecurity disclosure. The tension between disclosure and security often surfaced. In some instances, companies often did not disclose sufficient information to stakeholders to allow them to understand how cyber risk was addressed. This was especially evident in companies with few mentions of cybersecurity controls. However, many other companies demonstrated that cybersecurity disclosure can be easily carried out by balancing disclosure with security. I chose these examples because they present information in a sufficiently clear fashion while maintaining a sufficient level of generality.⁵

An example in this regard is to list numerous types of controls in place to protect the network and information system from cyber threats:

“To protect our data and systems, [X] [...] implement[s] in-depth defense and a zero-trust environment, using [...] detection mechanisms, anti-malware, anti-phishing protection, and identity threat-prevention solutions/controls. In addition, we have [...] monitoring mechanisms to detect [...] potential vulnerability or weakness [...]. We [...] educate our employees and enhance our cybersecurity training programs [...]. We [...] continue to review and improve our incident response [...] and conduct[...] cyber drills to make sure [X] is equipped to handle any [...] incidents.”

“[X] regularly perform[s] internal control testing of IT general controls including identity & access management, change management and incident management and we have [...] processes in place to mitigate cyber security threats such as single sign on and multi-factor authentication, patch management, firewall management and back-up and recovery management.”

“Organisational measures include[s] an ongoing training programme, awareness

5. These examples are presented in an anonymised format, so as to maintain the anonymised format of this empirical research.

campaigns, phishing tests, identity access management and more [...] to prevent cybersecurity risk [...]. In addition, multiple layers of technical safeguards and measures have been established that [...] protect against cyberattacks and ensure business continuity; these include measures such as network segmentation, multi-factor authentication and backups. Amongst others, penetration tests are performed on a regular basis [...]. The Internal Audit department is also involved to monitor progress [...]"

"[...] The Company believes [...] [the] preventative measures in place adequately mitigate the risk of a significant [...] IT incident. Such measures include: • Diversity and physical separation of systems across our businesses[...] • Complete asset management of IT and IT network inventory. [...] • Proactive patching processes [...] • Separation of business IT networks, operational technology, and production networks • Segregation of IT networks in different risk segments • [...] monitoring activities on the networks and/or endpoints • Disaster recovery planning including dry runs and tabletop exercises • Information security training and compliance programs • [...] next generation firewalls, encryption, physical access controls, endpoint detection and response software for virus and malware detection and remote-controlled countermeasures, multi-factor authentication [...], staff and privileged accounts, on-site and off-site offline backup schemes • Regular testing of backup [...] • Websites [...] hosted and maintained by an external partner and [...] not connected to the company's computer network [...]."

These examples show how the companies provided stakeholders with a sufficiently detailed explanation of how they addressed cybersecurity risk. Furthermore, all the examples mentioned above show that the companies at hand included several controls, often exceeding the keywords used in this research. Nonetheless, this kind of information does not provide details on how these actual controls work or which segment of the network or information system they are applied to. This prevents potential threat actors from gaining useful knowledge to mount an attack.

Alternatively to listing controls, to demonstrate to stakeholders how the company secures its network and information system, a company can refer to the technical standards that underpin the company's information system framework:

"[X]'s information security policy is based on [...] standards, like ISO 2700x, COBIT 2019, NIST Cybersecurity framework, SOC2 principles, PCI DSS, COSO, [...], ITIL. [...]"

“[X] developed our information security framework by applying the ISO 27001 [...] across its 14 domains and by driving security maturity – from policy setting, asset management and access control to incident management and more. For each of these domains, [X] have tailored controls in place, [...] assessed routinely [...] to ensure compliance and effectiveness. In addition, [...] incident-reporting tool[s] [...] make sure that all IT and information security issues can be reported, correlated and investigated”

“[...], [X] [...] has introduced the Cybersecurity [...] Framework, which aligns with industry best practices such as ISO 27001 and NIST. This framework provides a [...] foundation for our cybersecurity initiatives and ensures [...] assurance and maturity in our cybersecurity posture”

By referencing the standards, a company can effectively and briefly show its approach to cyber risk. For a stakeholder, knowing that a company complies with a given standard provides a certain level of reassurance. On the contrary, for a threat actor seeking to exploit information published in the annual report, knowing that the company has obtained a given certification or complies with a given standard does not automatically clarify where the network and information system's vulnerabilities lie. Therefore, without explaining how and to what extent these frameworks are implemented in practice, a company can easily allow the stakeholders to understand how cyber risk is managed and solve the transparency vs security dichotomy.

While conducting the research, I also found noteworthy disclosure practices regarding supply chain risk. For stakeholders to be able to use this information, the annual report should cover topics such as how a company assesses its suppliers, how the company monitors the suppliers' compliance with contractual obligations, how the company's internal policies account for the risk of supply chain cyber disruptions, or how they coordinate cybersecurity practices with suppliers. For instance:

“As the dependence of our safety relies on the [...] protection of our vendors and partners we keep investing in a better control of these risks. [...] we updated our procurement procedures by adding requirements for both IT and OT, setup risk profiles for [...] vendors and partners. We also assessed our [...] IT vendors on NIS-2 compliance and have put a monitoring tool in place to track [...] their [...]

cybersecurity health.”

“Business Continuity Planning (BCP) and IT security are [...] areas of focus to make sure suppliers and sub-tier suppliers have clear contingency plans to continue to supply [...] in the event of external events, [...]. Having robust IT plans in case of cyberattacks and other threats are [...] growing in priority. We are working with suppliers to validate that [...] IP is protected, and is able to continue to operate should an attack take place.”

“Cybersecurity remains a major source of concern for our suppliers, and [X] has [...] experienced supply shortages and delivery risks due to suppliers [...] cybersecurity issues. We [...] added cybersecurity to our supplier audits and supplier scorecards. From this, we [...] identified gaps in suppliers’ cyber environments, and driven them to correct these or risk losing [X]’s business. [...] we expect continued advancements from malicious actors, and we will drive our suppliers to keep up with the latest protocols and protections, [...] ensuring that [...] continuity plans are in place in the event of an incident”

“[...] [X] started the [...] Circles of Trust initiative [...]. The ‘circle of trust’ is a network of peers and suppliers who [...] embrace the same information security standards and raise their performance against these standards. The network also drives the exchange of knowledge and best practices between [X], suppliers and ecosystem partners. We share best practices to help our [...] partners develop and reinforce security maturity. [...] Annually we hold master classes with our [...] key suppliers and [...] our neighbour companies to increase information security awareness and knowledge [...], and to share practical tips, tricks and strategies, for example about [...] ransomware.[...]”

“[...] [X] [...] conducted an IT Risk Survey which received responses from [...] suppliers. The purpose of this survey was to assess the risk profile of our [...] suppliers with a focus on [...] governance of issues such as data protection, regulatory compliance and data breach risk management. The survey responses were analyzed [...] which led to the categorization of suppliers into different risk levels. Following the survey, two IT security sessions were organized to ensure that [...] suppliers remained at manageable risk levels. [...]”

A last topic that emerged from the annual report is the link between legislation and compliance efforts. Several companies signalled to stakeholders how legislation was used to revise or improve their internal policies to align them with regulatory requirements. These paragraphs confirm the role that legislation can play in forcing companies to rethink their practices. For instance:

“[...] In 2024, the Supervisory Board identified areas where further education was required, particularly in emerging technologies developments [...]. For instance, the Audit & Risk Committee received an in-depth briefing on the implications of the NIS2 [...], enhancing the Supervisory Board’s understanding of its impact on cybersecurity and compliance. [...]. These educational activities align with the best practice provisions from the corporate governance code.”

“[...]To protect our information technology (IT) infrastructure, we conduct ongoing assessments with a particular focus on cybersecurity. Our IT team is partway through implementing an IT security and governance framework [...]. As part of this process, we are developing a complete set of updated and modernized IT policies, aligned with industry standards and the NIS2 directive”

“NIS2, which aims to enhance the cybersecurity of critical infrastructure and digital service providers in the EU, must be implemented into national law by October 2024. [...]. In recent years [X] invested heavily in cybersecurity across the organization and has taken extensive measures, both on technical and governance perspective, intensified reporting protocols and has a detailed security roadmap, to comply with the NIS2 directive prior to the conversion into Dutch and Belgian law.”

“In the upcoming year, the NIS2 directive will be implemented. [...] [G]roundwork for this initiative was already laid in past years. We have set up an incident response procedure and held cyber crisis exercises on how to respond in case of an incident. Furthermore, [X]’s IT unit has been expanded, as have the roles related to security. [X] becomes more dependent on (information security in) supply chains, such as [...] partners and various third party [...] software tools and services. This requires careful supply chain management to ensure both security and compliance with applicable regulations [...].”

All the above paragraphs are tailored to the types of initiatives in place in the reporting companies. Stakeholders could use such information to assess companies’

risk management approaches to cyber and supply chain risks. The reader should consider this collection of paragraphs as examples representative of how companies can explain their internal cybersecurity policies and compliance efforts. This study abstains from making any qualitative evaluation of these paragraphs.

Discussion and limitations

The analysis shows an increase in the frequency of keywords in the annual reports of Dutch-listed companies. From 2020 to 2024, the amount of cybersecurity content in annual reports has increased. Companies not only increased cybersecurity controls but also improved their quality. The annual reports have started to provide more detailed content, including examples of the types of controls in place to prevent cyber threats. Nonetheless, although cybersecurity issues have gained greater importance in Dutch companies' annual reports, the presence of supply chain issues remains limited. While the growth has been relatively limited in terms of numbers, the overall data show a gradual increase in the mention of supply chain cybersecurity issues over the years. While in 2020 the number of companies in the sample with zero mentions was 34, in 2024 it decreased to 22, meaning that almost two-thirds of the companies included at least a reference to supply chain security issues in their annual reports.

As the analysis shows, growth has occurred mainly during the 2020-2022 period rather than during the 2022-2024 period. The companies increased their cybersecurity content more before the entry into force of NIS2 and DORA than in the subsequent time interval. While growth continued during the 2022-2024 period, not all the companies in the sample proportionately increased their cybersecurity content during this second interval. The pressure created by the implementation of NIS2 and DORA may have brought greater attention to cybersecurity. Annual reports provide stakeholders with information on any existing or prospective events that can impact the company. Compliance efforts are an example of such events. Therefore, compliance with NIS2 and DORA may justify the larger increase in the first time interval than in the second.

Nonetheless, over the three years, companies did not grow evenly, with some growing more than others. Based on the data, companies in the AEX and those subject to DORA-NIS2 had the highest recorded values and led growth in cybersecurity content. AEX companies are the largest companies in the Euronext Amsterdam index. Therefore, these companies have greater exposure to risks than the other companies. Their annual reports cover a wider range of financial and non-financial risks. As cybersecurity risks have emerged, these companies might have

felt the need to discuss cybersecurity more. This explains why these companies might also include more cybersecurity information, always staying ahead of the curve. As per the DORA-NIS2 companies, i.e. financial companies, they are also often exposed to more risks than other companies. Furthermore, the additional legal pressure from DORA might have pushed these companies to discuss cybersecurity internally and thus include it in their annual reports.

Overall, the data collected confirm a clear shift in how companies disclose cybersecurity and supply chain security in their annual reports. Cybersecurity information has become more prevalent and more detailed, as well as supply chain security information. If in 2020 cybersecurity covered only a limited part of annual reports, by 2024 cybersecurity issues were undeniably more widely discussed. This provides a positive answer to the research question posed at the beginning of this article.

The changes in the annual report reflect growing attention to cybersecurity in the corporate domain. This growing presence means more discussion at the management and board levels about cybersecurity, leading to greater organisational learning and better cyber risk management practices. Overall, this increased attention contributes to improving the security of the EU network and information systems, thereby achieving the goals of NIS2 and DORA. Based on the evidence in this paper, the compliance efforts for DORA and NIS2 seem not to have translated into on-paper compliance but have actually permeated the corporate structure and fostered more discussion regarding cybersecurity. To continue this trend, it would be fundamental that the EU bodies continue to further legislate on cybersecurity, so as not to lose the momentum gained with DORA and NIS2.

While the data show that 2022 was a turning point in cybersecurity disclosure practices, this study has a few limitations. The study does not establish causality, and, based on the collected data, it is therefore impossible to prove that legislation was the sole driver of this increase in cybersecurity information. Other factors, such as recent cyberattacks, changes in reporting standards/frameworks, and geopolitical tensions, could also have affected the amount of cyber information included in a company's annual report. An annual report might highlight events such as cyber-attacks or geopolitical crises as events that impacted the company financially or non-financially during the year. Therefore, a more extensive discussion of cybersecurity might have occurred, affecting the data collection for this study. Similarly, changes in reporting standards can affect how companies discuss a specific risk, such as cyber risk, to varying degrees. Lastly, this research is based on keyword research. Information on cybersecurity, controls, or supply chain issues might

not have been captured if discussed under other keywords not considered by this study. A further study using a qualitative approach may confirm the results of this research.

Conclusion

This article examined whether observable changes occurred in how companies disclose cyber risks and supply chain risk in their annual reports after 2022. The 2022 regulatory changes introduced more cybersecurity and supply chain security obligations. These obligations required companies to review or modify their cybersecurity and supply chain security policies. As an annual report reflects how a company perceives and acts on a specific risk, the 2022 regulatory changes might have changed how companies perceive and address cyber risk and supply chain risk. To understand this, I investigated the 2020, 2022, and 2024 annual reports of 67 Dutch-listed companies. For each annual report, I searched and recorded specific keywords related to cybersecurity, controls, and supply chain. The data showed an observable change not only in the amount of information disclosed but also in its quality. Given the role of annual reports in reflecting changes in corporate policies, the changes registered in cybersecurity disclosure signal a shift in cybersecurity corporate governance practices.

References

- Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, 4(1), tyy006. <https://doi.org/10.1093/cybsec/tyy006>
- Amani, F., Magnan, M., & Moldovan, R. (2025). Cybersecurity risks and incidents disclosure: A literature review. *Accounting Perspectives*, 24(3), 605–667. <https://doi.org/10.1111/1911-3838.12411>
- Archer, D. (Ed.). (2016). *What's in a word-list? Investigating word frequency and keyword extraction*. Routledge, Taylor & Francis Group.
- Archer, D. (2022). 5. Data mining and word frequency analysis. In *Research Methods for Reading Digital Data in the Digital Humanities* (pp. 72–92). Edinburgh University Press. <https://www.degruyterbrill.com/document/doi/10.1515/9781474409629-006/html?lang=en>
- Arena, C., Catuogno, S., Lamboglia, R., Silvestri, A., & Veltri, S. (2022). The disclosure of non-financial risk. The emerging of cyber-risk. In L. Cinquini & F. De Luca (Eds), *Non-financial Disclosure and Integrated Reporting: Theoretical Framework and Empirical Evidence* (pp. 29–60). Springer International Publishing. https://doi.org/10.1007/978-3-030-90355-8_2
- Athanasakou, V., & Boshanna, A. (2025). Linkage between strategy and financial performance disclosure in annual reports: A new reporting path for organizational learning. *The British*

Accounting Review, 101643. <https://doi.org/10.1016/j.bar.2025.101643>

Berg, B. van den. (2026). Risk and uncertainty in the digital ecosystem. *Technology and Regulation*, 2026, 10–27. <https://doi.org/10.71265/veh8cc91>

Bhakhri, K., Sethi, M., Sharma, I., & Kaushik, K. (2024). Examining the consequences of cyberattacks on businesses and organizations. In A. Bhattacharya, S. Dutta, P. Dutta, & D. Samanta (Eds), *Innovations in Data Analytics* (pp. 227–239). Springer Nature. https://doi.org/10.1007/978-981-97-3466-5_17

Black, J., & Baldwin, R. (2010). Really responsive risk-based regulation. *Law & Policy*, 32(2), 181–213. <https://doi.org/10.1111/j.1467-9930.2010.00318.x>

Boggini, C. (2024). Reporting cybersecurity to stakeholders: A review of CSRD and the EU cyber legal framework. *Computer Law & Security Review*, 53, 105987. <https://doi.org/10.1016/j.clsr.2024.105987>

Böhme, R., & Moore, T. (2016). The “iterated weakest link” model of adaptive security investment. *Journal of Information Security*, 07(02), 81–102. <https://doi.org/10.4236/jis.2016.72006>

Butenko, A., & Larouche, P. (2015). Regulation for innovativeness or regulation of innovation? *Law, Innovation and Technology*, 7(1), 52–82. <https://doi.org/10.1080/17579961.2015.1052643>

Bygrave, L. A. (2025). The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes. *Computer Law & Security Review*, 56, 106071. <https://doi.org/10.1016/j.clsr.2024.106071>

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, 11(3), 431–448. <https://doi.org/10.3233/JCS-2003-11308>

Chiara, P. G. (2022). The Cyber Resilience Act: The EU Commission’s proposal for a horizontal regulation on cybersecurity for products with digital elements. *International Cybersecurity Law Review*, 3(2), 255–272. <https://doi.org/10.1365/s43439-022-00067-6>

Colicchia, C., Creazza, A., & Menachof, D. A. (2019). Managing cyber and information risks in supply chains: Insights from an exploratory analysis. *Supply Chain Management: An International Journal*, 24(2), 215–240. <https://doi.org/10.1108/SCM-09-2017-0289>

Creazza, A., Colicchia, C., Spiezia, S., & Dallari, F. (2022). Who cares? Supply chain managers’ perceptions regarding cyber supply chain risk management in the digital transformation era. *Supply Chain Management: An International Journal*, 27(1), 30–53. <https://doi.org/10.1108/SCM-02-2020-0073>

Davis, A. (2015). Building cyber-resilience into supply chains. *Technology Innovation Management Review*, 5(4), 19–27. <https://doi.org/10.22215/TIMREVIEW/887>

de Olazábal, I. D. (2026). False choices: Competitiveness, deregulation, and the erosion of GDPR’s regulatory integrity. *Computer Law & Security Review*, 60, 106237. <https://doi.org/10.1016/j.clsr.2025.106237>

Draghi, M. (2024). *The future of European competitiveness Part B | In-depth analysis and recommendations*.

Edwards, J., & Weaver, G. (2024). *The cybersecurity guide to governance, risk, and compliance* (1st edn). Wiley. <https://doi.org/10.1002/9781394250226>

Eijkelenboom, E. V. A., & Nieuwesteeg, B. F. H. (2021). An analysis of cybersecurity in Dutch annual reports of listed companies. *Computer Law & Security Review*, 40, 105513. <https://doi.org/10.1016/j.clsr.2020.105513>

European Commission—Financial services – improving resilience against cyberattacks (new rules). (2025, July 10). [Text]. European Commission - Financial Services – Improving Resilience against Cyberattacks (New Rules). https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation_en

European Union Agency For Cybersecurity. (2024). *2024 Report on the state of the cybersecurity in the Union*. <https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union>

Fenwick, M., Kaal, W. A., & Vermeulen, E. P. M. (2017). Regulation tomorrow: What happens when technology is faster than the law? *American University Business Law Review*, 6(3), 561–594.

Fuster, G. G., & Jasmontaite, L. (2020). Cybersecurity regulation in the European Union: The digital, the critical and fundamental rights. In M. Christen, B. Gordijn, & M. Loi (Eds), *The Ethics of Cybersecurity* (pp. 97–115). Springer International Publishing. https://doi.org/10.1007/978-3-030-29053-5_5

Galle, A., & Vletter-van Dort, H. (2025). From cybersecurity to cyber resilience in the board room: Key steps for supervisory board members and non-executives. *International Cybersecurity Law Review*. <https://doi.org/10.1365/s43439-025-00151-7>

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2019). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*, 25(2), 223–240. <https://doi.org/10.1108/SCM-10-2018-0357>

Hietala, J. (2014). *Linguistic key words in ediscovery* (SSRN Scholarly Paper No. 2394254). Social Science Research Network. <https://doi.org/10.2139/ssrn.2394254>

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. *Information & Communications Technology Law*, 28(1), 65–98. <https://doi.org/10.1080/13600834.2019.1573501>

Hurel, L. M., & Weissinger, L. (2021). *The networked politics of cybersecurity: Co-production and tensions around incident response*. (SSRN Scholarly Paper No. 3898137). Social Science Research Network. <https://doi.org/10.2139/ssrn.3898137>

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, 139(3), 719–749. <https://doi.org/10.1016/j.jfineco.2019.05.019>

Kasper, A., & Vernygora, V. (2021). The EU's cybersecurity: A strategic narrative of a cyber power or a confusing policy for a local common market? *Cuadernos Europeos de Deusto*, (65), 29–71. <https://doi.org/10.18543/ced-65-2021pp29-71>

Khan, O., & Estay, D. A. S. (2015). Supply chain cyber-resilience: Creating an agenda for future research. *Technology Innovation Management Review*, 5, 6–12.

Kiesow Cortez, E., & Dekker, M. (2022). A corporate governance approach to cybersecurity risk disclosure. *European Journal of Risk Regulation*, 13(3), 443–463. <https://doi.org/10.1017/err.2022.10>

Kosseff, J. (2016). Positive cybersecurity law: Creating consistent and incentive-based system. *Chapman Law Review*, 19(2), 401–420.

Laver, M., Benoit, K., & Garry, J. (2003). Extracting policy positions from political texts using words as data. *American Political Science Review*, 97(2), 311–331. <https://doi.org/10.1017/S0003055403000698>

Lawless, R. M., Robbennolt, J. K., & Ulen, T. S. (2016). *Empirical methods in law* (Second edition). Wolters Kluwer.

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, 64(5), 659–671. <https://doi.org/10.1016/j.bushor.2021.02.022>

Linsley, P. M., & Shrives, P. J. (2006). Risk reporting: A study of risk disclosures in the annual reports of UK companies. *The British Accounting Review*, 38(4), 387–404. <https://doi.org/10.1016/j.bar.2006.05.002>

Lombardi, R., Cosentino, A., Sura, A., & Galeotti, M. (2021). The impact of the EU Directive on non-financial information: Novel features of the Italian case. *Meditari Accountancy Research*, 30(6), 1419–1448. <https://doi.org/10.1108/MEDAR-06-2019-0507>

Marchant, G. E. (2011). The growing gap between emerging technologies and the law. In G. E. Marchant, B. R. Allenby, & J. R. Herkert (Eds), *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem* (pp. 19–33). Springer Netherlands. https://doi.org/10.1007/978-94-007-1356-7_2

Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., & Friday, D. (2022). New challenges in supply chain management: Cybersecurity across the supply chain. *International Journal of Production Research*, 60(1), 162–183. <https://doi.org/10.1080/00207543.2021.1984606>

Nieuwesteeg, B., Eijkelenboom, E., & Hoogerwaard, R. (2022). An analysis of changing transparency regarding cybersecurity in annual reports. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4268272>

Porcedda, M. G. (2018). Patching the patchwork: Appraising the EU regulatory framework on cyber security breaches. *Computer Law & Security Review*, 34(5), 1077–1098. <https://doi.org/10.1016/j.clsr.2018.04.009>

Rintamäki, T., Golpayegani, D., Lewis, D., Celeste, E., & Pandit, H. J. (2026). Impact assessment requirements in the GDPR vs the AI Act: Overlaps, divergence, and implications. *Computer Law & Security Review*, 61, 106317. <https://doi.org/10.1016/j.clsr.2026.106317>

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2), 121–135. <https://doi.org/10.1093/cybsec/tyw001>

Rupp, C. (2024). *Navigating the EU cybersecurity policy ecosystem*. Interface.

Schip, M. van 't. (2024). The regulation of supply chain cybersecurity in the NIS2 directive in the context of the internet of things. *European Journal of Law and Technology*, 15(1).

Schmitz-Berndt, S. (2021). European Union • Cybersecurity is gaining momentum – NIS 2.0 is on its way. *European Data Protection Law Review*, 7(4), 580–585. <https://doi.org/10.21552/edpl/2021/4/14>

Sebastiani, F. (2002). Machine learning in automated text categorization. *ACM Computing Surveys (CSUR)*, 34(1), 1–47. <https://doi.org/10.1145/505282.505283>

Stanton, P., & Stanton, J. (2002). Corporate annual reports: Research perspectives used. *Accounting, Auditing & Accountability Journal*, 15(4), 478–500. <https://doi.org/10.1108/09513570210440568>

Stemler, S. (2001). An overview of content analysis. *Practical Assessment, Research & Evaluation*, 7(11).

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1), 134–153. <https://doi.org/10.1016/j.clsr.2017.05.015>

Urcioli, L., Männistö, T., Hintsa, J., & Khan, T. (2013). Supply chain cyber security – Potential threats. *Information & Security: An International Journal*, 29, 51–68. <https://doi.org/10.11610/isij.2904>

van Zeeland, I. (2024). *We value your privacy: The organisational protection of personal data*.

Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review*, 52, 105890. <https://doi.org/10.1016/j.clsr.2023.105890>

Varian, H. (2004). System reliability and free riding. *Economics of Information Security*, 1–15. https://doi.org/10.1007/1-4020-8090-5_1

Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR)*. Springer International Publishing. <https://doi.org/10.1007/978-3-319-57959-7>

Weber, R. (1990). *Basic content analysis*. SAGE Publications, Inc. <https://doi.org/10.4135/9781412983488>

Witten, I. H. (2004). Text mining. In M. P. Singh (Ed.), *The Practical Handbook of Internet Computing* (pp. 314–341). Chapman and Hall/CRC. <https://doi.org/10.1201/9780203507223>

Wolff, J. (2022). *Cyberinsurance policy: Rethinking risk in an age of ransomware, computer fraud, data breaches, and cyberattacks*. The MIT Press. <https://doi.org/10.7551/mitpress/13665.001.0001>

Yuthas, K., Rogers, R., & Dillard, J. F. (2002). Communicative action and corporate annual reports. *Journal of Business Ethics*, 41(1), 141–157. <https://doi.org/10.1023/A:1021314626311>

Published by



ALEXANDER VON HUMBOLDT
INSTITUTE FOR INTERNET
AND SOCIETY



RESEARCH
FOR THE
DIGITAL AGE

in cooperation with



CREATE



centre
— internet
et — societe



R&I IN3
Internet
interdisciplinary
Institute
Universitat Oberta de Catalunya



UNIVERSITY OF TARTU
Johan Skytte Institute of
Political Studies