An Analysis of Changing Transparency regarding Cybersecurity in Annual Reports

B.F.H. Nieuwesteeg
E.V.A. Eijkelenboom

Abstract

This paper studies the annual reports of 75 listed firms in the Netherlands in relation to the disclosure of cybersecurity information from a financial law and economics perspective in four consecutive financial years (2018-2021). Also, we study legislative developments (especially in the US) regarding cybersecurity disclosure requirements. Furthermore, we discuss the social and private costs and benefits of cybersecurity transparency. We draft hypotheses regarding the actual disclosure of cybersecurity information and propose a research design of an empirical study covering four financial years. The results of our study show that over time disclosing information regarding cybersecurity increases. However, the information value of the disclosures could improve since companies still disclose mostly technical measures that are hard to compare. In order for these efforts to have a social benefits, harmonization efforts need to be made.

KEYWORDS: cybersecurity, transparency, financial law, annual report, information sharing, security regulation.

Table of Contents

1 Introduction[1]

Scholars and academics argue that cybersecurity either is or should be 'a board-level topic'[2]. But, to what extent can shareholders and stakeholders judge whether the board indeed implemented a reasonable cybersecurity strategy and took appropriate measures? The annual report is a well-established method to transfer information from the board to shareholders and stakeholders, for example to improve a constructive dialogue[3] or protect their interests.[4] In our previous contribution on this topic, we performed an exploring empirical analysis of the disclosure of cybersecurity information through the annual reports of listed companies in the Netherlands in 2018.[5] In the meantime, a lot has changed on this topic which we believe justifies a new article on the matter.

---

[1] The authors would like to thank Rens Hoogerwaard and Willem Kuijken for their very valuable research assistance.

[2] Deloitte, 'Cyber security: The Changing Role of the Board and the Audit Committee', (Deloitte 2016) <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-cyber-security-noexp.pdf> Accessed 11 July 2022; E Schneider and others, 'Cyber in the Boardroom. Helping Boards Meet Their Responsibilities Regarding Cyber Security' (2016) 3 Compact <https://www.compact.nl/articles/cyber-in-the-boardroom> accessed 11 July 2022; Jake Olcott, '4 Cybersecurity Factors Every Board Member Must Consider for 2019 Planning' (*Bitsight*, 5 October 2018) <https://www.bitsight.com/blog/4-cybersecurity-factors-board-members-2019-planning> accessed: 11 July 2022; Elif K Cortez and Martijn Dekker, 'A Corporate Governance Approach to Cybersecurity Risk Disclosure' [2022] European Journal of Risk Regulation (forthcoming) < https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/corporate-governance-approach-to-cybersecurity-risk-disclosure/2383DCE62F081000044D5B2CBE9BC125> accessed 11 July 2022; HJ Pace and Lawrence J Trautman, 'Mission Critical: Caremark, Blue Bell, and Director Responsibility for Cybersecurity Governance' [2022] Wisconsin Law Review (forthcoming) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3938128> accessed 11 July 2022; Freddy Dezeure, George Webster and Lokke Moerel, 'Reporting Cyber Risk to Boards' (*freddydezeure*, 14 March 2022) <https://www.freddydezeure.eu/23-reporting-cyber-risk-to-boards-board-edition> accessed 28 October 2022.

[3] Parliament & Council, 'Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive 2013/34/EU, Directive 2004/109/EC, Directive 2006/43/EC and Regulation (EU) No 537/2014, as regards corporate sustainability reporting (CSRD)' COD (2021) 0104, Preambule 2a. . The CSRD is not yet published in the Official Journal, the agreement between Council and European Parliament can be downloaded here: https://www.consilium.europa.eu/media/57644/st10835-xx22.pdf

[4] Preambule 3, DIRECTIVE 2013/34/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EE, *OJ,* L 182 19.

[5] Eva VA Eijkelenboom and Bernold FH Nieuwesteeg, 'An Analysis of Cybersecurity in Dutch Annual Reports of Listed Companies' (2021) 40 Computer Law & Security Review <https://www.sciencedirect.com/science/article/abs/pii/S0267364920301187> accessed on 11 July 2022.

Therefore, we extended our empirical analysis which lead to an increased availability of empirical data. Our dataset covers annual reports of companies listed in Dutch indices (hereafter Dutch annual reports) of the years 2018, 2019, 2020 and 2021. Moreover, in 2020 and 2021, we identified every individual specific cybersecurity measure mentioned in the annual report. Also, we categorised how often such a specific measure occurred among the reports in that particular year.

Furthermore, there have been legislative proposals (especially in the US) regarding cybersecurity disclosure requirements that justify an update of the legislative framework. Also, some additional arguments emerged in the discussion regarding the social and private costs and benefits of cybersecurity transparency.

The combination of these developments resulted in this research in which we build upon our earlier study and analyse and discuss new empirical data regarding cybersecurity disclosures in the annual report. This allows for an analysis of the policy options that are efficient in inducing transparency through reporting, also in relation to the public discussion regarding a (compulsory) IT/cybersecurity audit.[6]

We use the data to discuss whether the current requirements regarding disclosing cybersecurity information in annual reports are sufficient or whether new legislation is needed. Similar to our previous article, we study the data of cybersecurity information from a financial law and economics perspective. Hence, in Section 2 we first provide an update of the requirements in financial law to disclose cybersecurity information in annual reports. Hereafter, in Section 3, we discuss additional insights to the incentives for the board of disclosing cybersecurity related information from an economic perspective and its effects on stakeholders and shareholders. We use the combination of the financial law and economics perspective to propose a research design, to draft hypotheses and to show results regarding the disclosure of cybersecurity information in Section 4. In Section 5, we discuss our findings. Section 6 presents the conclusion.

[6] Stijn van Gils and Jan F van Wijnen, 'Nieuwe IT-check kan Voorwaarde Worden Voor Krediet' *FD* (11 August 2021) <https://fd.nl/futures/1407271/nieuwe-it-check-kan-voorwaarde-worden-voor-krediet-ikg2caAVEQrl> accessed 11 July 2022.

2 Objectives of annual financial reports, requirements regarding disclosing cybersecurity information in annual reports and cybersecurity incident disclosure requirements[7]

This section contains a brief description of the current disclosure requirements regarding cybersecurity information in annual reports for Dutch listed companies. We define annual reports as the combination of the annual financial statements[8] the management report[9] and other information such as the auditor's report[10] which an undertaking is required to publish on a yearly basis. The annual report is an important means of communication and source of information for various stakeholders.[11] Moreover, the information value of the annual report is expected to increase due to the addition of the sustainability report to the annual report resulting in increased attention to the variety of stakeholders and more emphasis on the societal impact of the undertaking.[12] This section starts with a brief overview of reporting requirements for Dutch listed companies focused on cybersecurity. Thereafter, we discuss the mandatory disclosure of cyber incidents.

2.1 Disclosure requirements for annual reports of Dutch listed companies

The annual report of listed companies must be drawn up by the managing directors within four months after the end of the financial year.[13] Under European legislation[14] listed companies must prepare their consolidated financial statements in accordance with the International Financial Reporting Standards endorsed by the EU (EU-

[7] This section builds upon our earlier contribution Eijkelenboom and Nieuwesteeg 2021(n 5).
[8] Article 4 (1) Directive 2013/34/EU. The financial statements consists of a balance sheet, the profit and loss account with notes thereon and, if applicable, the consolidated financial statements.
[9] Art. 19 Directive 2013/34/EU.
[10] See for the auditor's report Article 35 Directive 2013/34/EU and the implementation in the Dutch law in article 2:392 Dutch Civil Code. Another example of required 'other information' is the disclosure of material payments made to governments by large undertakings and public-interest entities which are active in the extractive industry or logging of primary forests Article 41 Directive 2013/34/EU and the implementation in the Dutch law in Article 2:392a Dutch Civil Code.
[11] Preamble (4) Directive 2013/34/EU states that: " Annual reports "pursue various objectives and do not merely provide information for investors in capital markets but also give an account of past transactions and enhance corporate governance".
[12] Preamble 2a – 11 , CSRD compromise.
[13] Legislation applies to listed companies whose securities are admitted to trading on a regulated market as referred to in the Dutch Financial Supervision Act, see Article 2:101/2:210 Dutch Civil Code. Different requirements and terms are applicable for the drawing up of the financial statements of non-listed companies.
[14] Regulation (EC) No 1606/2002 of the European Parliament and of the Council of 19 July 2002 on the application of International Accounting Standards. IFRS are previously known as International Accounting Standards.

IFRS). Additional to the EU-IFRS requirements also national disclosure requirements need to be taken into account. Dutch legislation relating to financial reporting requirements for listed companies is part of the Dutch Civil Code and the Dutch Financial Supervision Act. Notably, in most cases the national disclosure requirements have an European origin therewith contributing to comparability of disclosures by listed companies across EU Memberstates. Currently, disclosure requirements on cybersecurity are absent, both in the European as well in the Dutch legislation relating to annual reporting.

However, major changes in annual reporting are expected in the upcoming years due to the EU Corporate Sustainability Reporting Directive.[15] This EU-directive requires all large undertakings (listed and non-listed), listed SMEs and non EU-undertakings subject to conditions to draft a sustainability report as part of the management report. The sustainability report covers environmental, social and governance (ESG) topics. Double materiality forms the base of sustainability reporting. This objective requires the company not only to report on the impact of the company activities on the environment but also on how various sustainability matters affect the undertaking.[16] Sustainability matters are defined as 'environmental, social and human rights, and governance factors […]'[17] Although, the topic cybersecurity is not part of this definition 'sustainability matters' nor explicitly mentioned in the CSRD, one could argue that sustainability reporting with its broader objective lowers the bar for more comprehensive reporting including mandatory cybersecurity disclosures in the future.

In the United States of America mandatory cybersecurity disclosure requirements is already in development. The Security and Exchange Committee (SEC), the government oversight agency that is responsible for regulating the securities markets and protecting investors proposed, proposed a regulation to enhance comparability and transparency of cybersecurity disclosures by listed companies in March 2022.[18] The proposal includes the provision of information on (i) risk management and strategy, (ii) policy and procedures for risk mitigation (iii) governance and the role and expertise of the board of management and (iv) disclosures on material cybersecurity incidents within four days after the incidents as well as part of the

[15] The CSRD is not yet published in the Official Journal, the agreement between Council and European Parliament can be downloaded here: https://www.consilium.europa.eu/media/57644/st10835-xx22.pdf
[16] Preambule 25 CSRD.
[17] Art. 2b CSRD.
[18] The U.S. Securities and Excha nge Commission, *Proposed Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* (SEC, 2022). The proposal can be found on https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

annual report. US disclosure requirements also affect Dutch listed companies who are also listed in the US stock market.[19]

In addition to the legal requirements, Dutch listed companies[20] are also required to report on compliance with the Dutch Corporate Governance Code (hereafter: the Code) in their annual report in a the corporate governance statement (Dutch Corporate Governance Code, 2016). The corporate governance statement is a formal part of the management report, however listed companies are allowed to (also) publish it separately on their website. In the corporate governance statement the listed company reports on compliance with the Code on a 'comply or explain' base, indicating that only the deviations from the Code are explained. The Code contains principles and best practice provisions that are aimed at defining the responsibilities for, amongst others, risk control. Currently, cybersecurity is (only once) explicitly mentioned in the Code in best practice provision 1.5.1. This provision focuses on the role and responsibilities of the audit committee. As part of monitoring the management board the audit committee is asked to include the application of information and communication technology by the company, including risks relating to cybersecurity.[21] However, the Code is under revision and the new version of the Code is expected at the end of 2022. Although, the consultation version did not show any adjustments of the provisions on cybersecurity several parties emphasized the importance of attention to cybersecurity – or broader IT security – in the Corporate Governance Code.[22]

Furthermore, the Foundation of the Dutch Accounting Standard Board publishes guidelines, the Dutch Accounting Standards. These cover questions arising from practice regarding annual reports. The Guidelines are not considered as legislation but denoted as authoritative statements by the Supreme Court of the Netherlands.[23] The Guidelines of the Dutch Accounting Standard Board have widespread use. The Guidelines 2021/400.1052 provide guidance on disclosure requirements related to risk control which could include cybersecurity risk. However, Guideline 2021/400.1101 guides on the compulsory nature of the disclosure requirements

[19] Several companies in the Dutch indices are dual-listed in the US, examples are Philips N.V. Aegon N.V. and ASML Holding N.V.
[20] More specific, the Dutch Corporate Governance Code applies to " (i) companies whose registered offices are in the Netherlands and whose shares, or depositary receipts for shares, have been admitted to trading on a regulated market or a comparable system; and (ii) all large companies whose registered offices are in the Netherlands (balance sheet value > €500 million) and whose shares, or depositary receipts for shares, have been admitted to trading on a multilateral trading facility or a comparable system (the Dutch Corporate Governance Code, p. 7).
[21] Bpp 1.5.1 Dutch Corporate Governance Code.
[22] For instance observe responses by the Centre for the Law and Economics of CyberSecurity and Norea.
[23] Supreme court of the Netherlands 10-02-2006 (KPN/Sobi), ECLI:NL:HR:2006:AU7473.

applicable to the management report.[24] The disclosure of information is obliged to the extent that important interests do not preclude this. In other words: The company does not have to harm itself with the dissemination of certain information. (Reference made to par 3.2.)

2.2 Cybersecurity incident disclosure requirements

Additional to disclosure requirements regarding information on cybersecurity in annual reports, undertakings subject to conditions are mandated to disclose cybersecurity incidents. These disclosure requirements are part of General Data Protection Regulation (GDPR)[25] and the EU Directive on security of network and information systems (NIS Directive).[26] The GDPR and NIS Directive, introduce a similar notification obligation based on the assumption that security threats can only be eliminated if security risks and data breaches are communicated to public authorities (and consequences can be mitigated by informing the data subject). For our discussion regarding the GDPR, we refer to our previous contribution.[27]

The NIS Directive[28] applies to 'operators of essential services (OES)' such as the energy and utility industry and certain digital service providers (DSPs), being search engines, online market places and cloud computing services.[29] Article 14 (3)

---

[24] See Article 2:391(2) Dutch Civil Code.

[25] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[26] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[27] Eijkelenboom and Nieuwesteeg (n 5).

[28] In the Netherlands, the Directive has been transposed into national regulation by a law called 'Wet beveiliging netwerk- en informatiesystemen', hereafter Wbni. Recital 1 of the NIS Directive provide information regarding the economic rationale of protecting network and information systems and services because they 'play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market.' Recital 2 continues with stating that 'the magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union'.

[29] Recital 7 of the NIS directive states that 'to cover all relevant incidents and risks, this Directive should apply to both operators of essential services and digital service providers.' Article 4(4) states that an 'operator of an essential service means a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2) of the Directive.' Article 5(1) states that 'by 9 November 2018, for each sector and subsector referred to in Annex II, Member States shall identify the operators of essential services with

NIS Directive regulates the security breach notification for operators of essential services. Operators of essential services should, without undue delay, notify incidents having a significant impact on the continuity of the essential services they provide to a competent authority.[30] Article 16 (3) NIS Directive regulates the security breach notification for digital service providers. However, on 22 June 2022, the EU Member States and the European Parliament agreed on revising the EU Network and Information Security Directive, which is referred to as 'NIS2'.[31] The scope of NIS2, will be extended. More sectors will fall under the scope of the NIS2 directive. However, the directive will most probably apply from 2024 onwards, and as such no impact is to be expected on current disclosure of cybersecurity information in financial reports. For a detailed discussion of the original NIS directive and the relation between the NIS directive and the GDPR, we refer to our original contribution.

The importance of disclosing vulnerabilities of ICT products, services and processes to decrease cyber security risks is also emphasized in the EU Cyber Security Act.[32] The Cyber Security Act strengthens the role of the EU Agency for Cyber Security (ENISA) by increasing ENISA's resources and tasks and granting ENISA a permanent mandate. For example, based on article 6 (1b) Cyber Security Act, ENISA shall assist EU Member States with establishing and implementing vulnerability disclosure policies on a voluntary basis. Furthermore, ENISA is assigned a key role in setting up and maintaining the European cybersecurity certification system. Article 54 (1n) Cyber Security Act specifies that disclosure policies should be part of this scheme. And article 55 (1d) Cyber Security Act specifies that manufacturers or providers of certified ICT products, services of processes shall, amongst others, make a reference to online repositories listing publicly disclosed vulnerabilities

---

an establishment on their territory.' Furthermore, a digital service provider performs a digital service, which is of a type listed in Annex III (either an online marketplace, an online search engine or a cloud computing service.). The security requirements and incident notification for digital service providers do not apply to micro- and small enterprises according to Article 16 (11).

[30] Which is an often different authority than the data protection authority of the GDPR. In the Netherlands, this is the National Cyber Security Center and/or the specific supervisory authority for this organisation.

[31] 'Cybermaatregelen in Meer Sectoren Maken Nederland en EU Digitaal Veiliger' (*Government of the Netherlands*, 22 June 2022) <https://www.rijksoverheid.nl/actueel/nieuws/2022/06/22/cybermaatregelen-in-meer-sectoren-maken-nederland-en-eu-digitaal-veiliger> accessed 14 October 2022; Commission, 'Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148' COM (2020) 823.

[32] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), *OJ, L 151, 7.6.2019, p. 15–69.*

related to these ICT products, services or processes and to any relevant cybersecurity advisories publicly available.

The GDPR, NIS1 Directive, NIS2 Directive and the Cyber Security Act do not specifically mandate incorporation of cybersecurity incidents in the annual report

3 What are the costs and benefits of disclosing cybersecurity information in annual reports?

In Eijkelenboom and Nieuwesteeg (2021) we discussed the potential costs and benefits of cybersecurity disclosures and cybersecurity related information diffusion in annual reports.[33] We distinguished 'private' and 'social' costs and benefits. Private costs and benefits are the negative and positive incentives for the board of directors and the supervisory board. These corporate bodies are responsible for whether and if so which cybersecurity information is included in the annual report due to their decision-making and supervisory authority.:. Social benefits and costs are the costs and benefits for society. The society includes actors that directly or indirectly can benefit from or are harmed by the disclosure of cybersecurity information excluding the actors with decision-making authority. We concluded that mentioning cybersecurity has clear benefits and only little cost for the organisation that discloses it in the annual report.

In this section, we highlight additional aspects of the cost benefit analysis that were not mentioned explicitly in Eijkelenboom and Nieuwesteeg (2021) but are relevant to consider when analysing empirical data and drafting policy recommendations. We base our analysis on the development of the public and academic discussion regarding cybersecurity transparency.

3.1 The value chain

Cybersecurity disclosures by the board of directors and the supervisory board (hereafter: the board) in the annual report is beneficial for:

1.) market actors such as potential investors, shareholders, and creditors.
2.) regulatory actors, such as the data protection authority or cybersecurity centres.
3.) the internal organisation of the company.[34]

[33] Eijkelenboom and Nieuwesteeg (n 5).
[34] Ibid.

Furthermore, cybersecurity transparency not only benefits external market actors, but also those actors with whom a company already has a business relation with in the value chain. In the case of business to business companies this would be both customers and suppliers. In the case of business to consumer companies this would be the supply chain.[35]

3.2 Negative externalities of suboptimal cybersecurity

Sharing cybersecurity knowledge can 'stimulate information diffusion'.[36] However, one could argue that indeed there are many risks and best practices that justify knowledge sharing that prevents others from reinventing the wheel. What makes cybersecurity different from other types of information diffusion a company can engage in such as HR best practices to prevent burnouts, agile work best practices or best practices with regards to preventing unacceptable behavior? The answer lies in the observation that suboptimal cybersecurity can have negative spill-over effects on society.[37] Hence, the challenge of reaching optimal cybersecurity exceeds a single company, just like sustainability policy. [38] These external effects make cybersecurity a different type of risk with a systemic character[39] and places it in the same category as sustainability.

3.3 Collective action problem

With regard to voluntary disclosure of cybersecurity information, there could be a collective action problem. Cybersecurity transparency generates the highest social surplus when most organisations reach a certain level of transparency. However, when disclosure is not coordinated, an organisation might refrain from providing the

---

[35] Luca Urciuoli and others, 'Supply Chain Cyber Security – Potential Threats' (2013) 29 Information & Security: An International Journal 51; Spyridon Papastergiou and Nineta Polemi, 'MITIGATE: A Dynamic Supply Chain Cyber Risk Assessment Methodology' in Xin-She Yang Atulya, K Nagar and Amit Joshi (eds), *Smart Trends in Systems, Security and Sustainability* (Proceedings of WS4 2017, Springer 2018) < https://link.springer.com/chapter/10.1007/978-981-10-6916-1_1#chapter-info> accessed 11 July 2022; Andrii Boiko, Vira Shendryk and Olha Boiko, 'Information Systems For Supply Chain Management: Uncertainties, Risks and Cyber Security' (2019) 149 Procedia Computer Science 65.

[36] Eijkelenboom and Nieuwesteeg (n 5).

[37] And conversely: optimal cybersecurity positive spill-over effects.

[38] R Anderson, 'Why Information Security is Hard – an Economic Perspective', in ACSAC (ed), *ACSAC '01: Proceedings of the 17th Annual Computer Security Applications Conference*, IEEE Computer Society 2001; T. Moore, 'Introducing the Economics of Cybersecurity: Principles and Policy Options' in National Research Council (ed), *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy,* The National Academies Press 2010.

[39] Michael Faure and Bernold FH Nieuwesteeg, 'The Law and Economics of Cyber Risk Pooling'(2018) 14 NYU Journal of Law & Business 923.

right information which also refrains others from doing so because they do not want to be the first to be exposed to the private costs (perceived reputation damage and perceived liability risk) associated with transparency. [40]

3.4 Which information should be disclosed to generate the highest social surplus?

Another argument that emerged is that cybersecurity transparency is not a goal in itself, in the sense that the private and social benefits of transparency strongly depend on the type of information that is disclosed. This is the reason for our additional categorisation of the individual measures that are disclosed. In this section, we distinguish cybersecurity information that contributes to the benefits above, information that has little positive effects and information that can have a negative effect.

First, we discuss information that is valuable to disclose. We discuss information regarding 1.) governance, 2.) knowledge sharing and 3.) the magnitude and coverage of cyber-risk:

1.) Information indicating the internal governance of cybersecurity is useful to report for external actors. This includes the internal reporting process. When the annual report provides insights about who is reporting to the board and to whom in the board, investors can judge whether cybersecurity is a board level topic.[41]
2.) External knowledge sharing and leadership. As discussed, suboptimal cybersecurity in the value chain has negative externalities.[42] Hence promoting cybersecurity best practices in the value chain can reduce these negative external effects for the company that is affected by other companies that have suboptimal cybersecurity. This means that companies should be fully aware of their supply chain. Suboptimal cybersecurity levels of actors in the system can quickly affect the continuity of the company itself. Examples of knowledge sharing activities are the way the company share knowledge about cybersecurity in the supply chain.

---

[40] Elinor Ostrom, *The Evolution of Institutions for Collective Action,* (1st edn, Cambridge University Press 1990).
[41] Freddy Dezeure, George Webster and Lokke Moerel, 'Reporting Cyber Risk to Boards' (*freddydezeure*, 14 March 2022) <https://www.freddydezeure.eu/23-reporting-cyber-risk-to-boards-board-edition> accessed 28 October 2022; Bernold Nieuwesteeg and Willem Kuijken, 'Publieke Reactie Herziening Corporate Governance Code' (Erasmus University, 15 April 2022) < https://www.eur.nl/en/media/2022-06-clecs-reactie-corporate-governance-code> accessed 26 November 2009.
[42] Bernold FH Nieuwesteeg, *The Law and Economics of Cyber Security* (1st edn, deLex 2018).

3.) The cyber-risk itself. In essence, an investor that makes an investment decision would like to know the magnitude of cyber-risk and the way in which the risk is covered. In such a way, it can calculate the expected value and maximum downside and can incorporate it in its valuation. This also includes incidents that have and will continue to have a material impact on the financial performance of the company.

Second, isolated technical cybersecurity measures without context arguably have little positive impact. For instance; mentioning 'a solid security IT infrastructure in place which consists of advanced spam and internet filters'.[43] A company can disclose this information, but without further context it is hard for external actors (such as investors, but also suppliers), to judge to what extend the technical measures lead to a reduction of cyber-risk. Also, from an internal perspective the disclosure of some relatively arbitrary technical measures may be a sign that the internal trickle-down effect that aims to stimulate prioritization did not function properly because main and side issues are not separated well.

Last, information that has negative impact on the business would be information that provides details about vulnerabilities in the company that not yet have been fixed. Especially if mere disclosure of this information increases the risk for the company.[44]

4 Research Design, Hypotheses, & Results

4.1 Empirical research design

We discussed in Section 2 that companies are not legally obliged to integrate information on cybersecurity in their annual report. In our empirical research design, we observe whether public companies are transparent regarding cybersecurity in their annual reporting. This study analyses annual reports from the years 2018, 2019, 2020 and 2021.[45] Within these years, we observed 75 annual reports in 2018, 2019 and 2021 and 74 annual reports in 2020 from the Duch AEX, AMX and AScX Indices.[46] The research design was originally drafted in 2019 and has been adapted

[43] Annual report 2021 of Fugro. Another example is provided by the 2021 annual report of United Malt Group that mentions it "deploys many methods to protect its systems, including but not limited to, security infrastructures such as firewalls, virus scanning, data back-up systems (...)".
[44] We also referred to this as the private cost 'providing information to the attacker' in Eijkelenboom and Nieuwesteeg (n 5).
[45] This results of the annual analysis was communicated as the Cyber Security Annual Report (CSAR)-index. This index annually studies how companies that are part of the communicate about cybersecurity in their annual reports.
[46]The composition of the indices subject to the CSAR-studies are derived from https://live.euronext.com/nl/markets/amsterdam in respectively October 2019, November

on a few occasions. Especially the design that was used for the 2020 and 2021 annual reports contains some significant alterations. Therefore this section will have the following structure. We will first briefly repeat the main points from the original research design that was used to study the annual reports of 2018 and that served as the basis for the design of later versions.[47] Secondly, we will address the differences in the design that was used for later versions. In this part we will also describe what years these differences apply to.

4.1.1 Original research design

The research design is divided into four parts. In the first part, we inspected the annual reports for the occurrence of several keywords.[48] Secondly, we investigated information about the awareness of cybersecurity on a managerial level by investigating the existence of persons with a special focus on cybersecurity and the attention on cybersecurity at board level.[49]

The third part focuses on the measures described in the reports. First, we searched the annual reports for the following pre-defined cybersecurity measures.[50] Thereafter, we counted the other internal cybersecurity measures mentioned in the report. Using the same search terms as in the first part, we detailly read the reports' sections containing those words to identify these measures. We did not track which specific measures were counted.

In the last part, we investigated whether the reports contained information on data breaches or other cybersecurity incidents companies fell victim to, or their cybersecurity expenses by using search terms.[51] The search terms in the research design were amongst others determined on the basis of a review of leading

---

2020, May 2021 and April 2022. According to this source, the AScX-Index only contained 24 companies in May 2021. Therefore, only 74 annual reports on 2020 were investigated.

[47] A detailed description can be found in the original Article of Eijkelenboom and Nieuwesteeg (n5).

[48] See Eijkelenboom and Nieuwesteeg (n 5) 7-8. The keywords are Cyber (including the more specific terms cybersecurity and cyber risk), information security and data protection.

[49] More specifically we investigated (i(the existence of a manager or director with a special focus on cybersecurity, (ii) the existence of an officer or other special personal specifically tasked with cyber security (for example; an information security officer) and (iii) whether cybersecurity was discussed during meetings of the board of directors or the supervisory board (one variable)

[50] These measures are: 1.) Two-factor or multi-factor authentication, 2.) Penetration test, 3.) Network monitoring, 4.) Network compartmentalization, 5.) Cyber insurance. For more information on what these measures entail and why specifically these were predefined, we refer to Eijkelenboom and Nieuwesteeg (n 5).

[51] We used the search terms of the first part similarly as for the other cybersecurity measures and added data breach and incident.

organisations in the technical sector and manually tested by creators of the CSAR-index. For more information on this procedure, we refer to the previous article.[52]

4.1.2 Adaptations

The research design in the three consecutive years (2019, 2020, 2021) is largely similar to the original design of 2018. Below, we describe adaptations and additions that have been made.

First, in the last three versions (2019, 2020, 2021) of the CSAR-index we slightly altered the way of measuring variables related to the awareness of cybersecurity on a managerial level. In this respect, we adapted the design to measure whether cyber was a topic during meetings of the board of directors or supervisory board separately (two variables). We made this adaptation because we observed differences in the extent in which cybersecurity was discussed in meetings between these two boards.

Second, from the years 2020 and 2021, we extended the analysis regarding specific cybersecurity measures. From these years on, we not only made a quantitative analysis of the amount of measures per company, but also categorised each specific measure. Also, we studied how many companies mentioned such a specific measure in their annual reports.[53] To account for different terminology capturing the same measures, we have categorized synonyms for each measure. When a measure was either more generally or specifically described than the other measures of the same sort, we designated the exception as a separate measure.[54] Because we now identify every individual cybersecurity measure we dropped the distinction between predefined and other measures we made in the years 2018 and 2019.

4.2 Hypotheses

In this section, we draft hypotheses based on the research design on the development and characteristics of disclosure of cybersecurity information in annual reports.

H_1: We expect that companies increasingly mention cybersecurity in their annual reports since our impression is that optimal cybersecurity has increasingly become an important business asset for companies since our previous analysis (which

[52] Eijkelenboom and Nieuwesteeg (n 5).
[53] Corresponding with the studies conducted to the annual reports of 2020 and 2021.
[54] For example; when a lot of companies describe cybersecurity awareness training (general) as a measure and one company describes phishing awareness as a measure (specific), the latter is adopted as a separate measure. Conversely, when a lot of companies describe several specific IT measures (such as firewalls or penetration tests) and one company generally describes to have an IT control framework, the latter is adopted separate from the specific measures.

analysed the annual reports of the year 2018), for instance because of the ransomware epidemic in recent years.[55]

H_2: We expect that companies disclose various types of specific cybersecurity measures and that measures are distributed widely among companies, since there has been, to the best of our knowledge, no hard law or soft law effort to harmonise disclosures.

4.3 Results

In this section we will present the main results of our study. First, we will present trends over the years 2018, 2019, 2020, 2021. Secondly, we will present the results that were retrieved from the analysis over the annual reports of 2020 and 2021 that identified and categorised specific measures more in depth.

Trends between 2018 and 2021:

Some results indicate an increase in transparency between 2018 and 2021. For example, the percentage of companies adopting some information on cybersecurity consistently increased. In the annual reports of 2018, 87 percent of the annual reports contained some information on cybersecurity. In the annual reports of 2021, this percentage grew to 97. This trend is also reflected in the share of reports mentioning that cybersecurity is discussed in supervisory board meetings and the provided information on cybersecurity incidents. Whereas in the annual reports of 2018 and 2019 respectively only 1 and 4 percent of the companies provided information on cybersecurity incidents, this was 7 and 19 percent in the 2020 and 2021 reports. Regarding the discussion in supervisory board meetings regarding cybersecurity, we witnessed growth from respectively 57 and 58 percent in the annual reports of 2019 and 2020, to 72 percent in 2021. The last consistent growth we found relates to the share of reports mentioning that a board member or officer is specifically tasked with cybersecurity. Whereas only 4 percent of the reports in 2018 contained such a reference, this percentage grew to 24 percent in 2021.

Other results indicate that transparency in the annual reports of 2020 had grown in comparison to those of 2018 and/or 2019, but -slightly- decreased from 2020 to 2021. For example, regarding the board of directors meetings, we witnessed a growth from annual reports in 2019 (64 percent) to those in 2021 as well (91 percent). However, in contrast to the earlier results, this percentage -slightly- dropped in comparison to

[55] Daniel W Woods and Rainer Bohme, 'How Cyber Insurance Shapes Incidents Response: A Mixed Methods Study' (2021) 20 WEIS; Mike Simmonds, 'How Businesses Can Navigate the Growing Tide of Ransomware Attacks' [2017] Computer Fraud & Security 9.

the reports of 2020 (93 percent). Similar trends were observed in the data on cybersecurity measures. Although the total reported measures in the annual reports 2021 (318) more than doubled in comparison to those in the annual reports 2018 (124), they also decreased in comparison to the measures in the 2020 reports (418). This is also visible in the percentage of companies that reported at least one measure. Whereas the 85 percent in the annual reports of 2021 was a growth compared to the 71 and 83 percent in the annual reports of respectively 2018 and 2019, it was a reduction compared to the 87 percent in 2020.

Some results that did not indicate a growth in transparency. In all years, the companies barely released any financial information related to cybersecurity. Whereas in the annual reports in 2018, 2019 and 2020 only one company shared some of this information, this number even reduced to zero in the annual reports of 2021. The results on the trends and developments are summarised in Table 1.

Table 1: Trends & developments

	Year of annual report	2018	2019	2020	2021
Percentage (%) or amount	Some information cyber	87%	88%	95%	97%
	Cybersecurity incidents	1.3%	4%	7%	19%
	Board member specifically tasked with cybersecurity	4%	15%	20%	24%
	Supervisory board meetings	82%*	57%	58%	72%
	Board of directors meetings		64%	93%	91%
	Minimum of one specific cybersecurity measure	71%	83%	89%	85%
	Total number of specific measures	124	252	418	318
	Financial information	1	1	1	0

* Measured as one variable (In supervisory board and/or board of directors) .

Results regarding the extended analysis of specific measures

The updated research design for the years 2020 and 2021 provided several insights related to the form and prevalence of the measures. The total number of 418 measures we counted in the annual reports of 2020 are divided over 169 different measures. For the reports in 2021, the total number of 318 specific measures we counted were divided over 95 different measures. In both years, more than half of the measures were only reported once, while only 4 percent of the measures were reported 10 times or more. The long tail of the distribution seems to be somewhat larger in the annual reports of 2020. Whereas a measure in the 2020 reports was averagely reported 2.5 times, the average reporting frequency for measures in 2021 reports was 3.3 times. The distribution of the measures are shown in Table 2 and 3.

Table 2: Distribution specific measures annual reports 2020

Annual reports 2020					Total amount of different measures	Average frequency per measure
Frequency of the measure	1	2-5	6-9	10+		
Amount measures	110	38	14	7	169	2.5
Percentage	65.1%	22.5%	8.3%	4.1%		

Table 3: Distribution measures annual reports 2021

Annual reports 2021					Total amount of different measures	Average frequency per measure
Frequency of the measure	1	2-5	6-9	10+		
Amount measures	49	26	16	4	95	3.3
Percentage	51.1%	27.7%	17%	4.3%		

The most frequently reported measures in the annual reports of both years were awareness training (2020: 28 [times]; 2021: 31), internal controls or test (2020: 16; 2021: 16) and penetration testing (2020: 15; 2021: 14). The ten most reported measures in both years are presented in Table 4. Lastly, we found that measures related to external knowledge sharing and leadership (following our discussion in in

Section 3) were underrepresented. Only 5 measures mentioned in the annual reports of 2020 and 4 measures in the annual reports of 2021 related to this purpose. These measures for example entailed addressing cybersecurity at suppliers or attending a cyber conference.

Table 4: Ten most reported measures

Rank	Measure (Frequency)	
	Annual reports 2020	Annual reports 2021
1.	Awareness training (28)	Awareness training (31)
2.	Internal controls or tests (16)	Internal controls or tests (16)
3.	Penetration testing (15)	Penetration testing (14)
4.	Back-up and recovery management (13)	Back-up and recovery management (10)
5.	Instalment of a cybersecurity framework (11)	Instalment of a cybersecurity framework (9)
6.	Partnership with other organisations (11)	Incident management (9)
7.	Updating critical applications (10)	Instalment of a cybersecurity program (9)
8.	Multi-factor authentication (8)	General or introductory cybersecurity training (9)
9.	Cyberrisk assessments (8)	Cyberrisk assessments (8)
10.	Identity and access management (8)	Disaster recovery plan (8)

5 Discussion

Our longitudinal analysis of cybersecurity information in annual reports provided new insights in cybersecurity disclosure.

From a financial law and economics perspective, our results show that, on average, the number of specific cybersecurity measures has increased, although 2021 shows a decline. From a cost and benefits point of view, this implicates that these companies, at least to some extent, are increasingly willing to take some of the negative private costs associated with disclosing cybersecurity information. Also in other areas of cybersecurity transparency This leads to our prudent conclusion that the first hypothesis is confirmed.

The second hypothesis is also confirmed. Although there has been an increase in the amount of transparency, companies disclose various types of specific cybersecurity measures and that measures are distributed widely among companies. The reason could be that there is no law or soft law or other coordination efforts to harmonise disclosure.

The social surplus of extended disclosure of cybersecurity information in annual reports depends on the type of information that is disclosed. Currently, various cybersecurity measures are scattered among the reports we analysed. It does not necessarily have to be the case that companies take different measures. They could also have used different terminology and specificity, although we controlled for synonyms in our analysis. But still, the vast majority of the measures is reported in only a single annual report. The question remains what an appropriate policy response should be?

An policy approach could harmonize and prioritize the type of information that ought to be disclosed in order to minimize the amount of noise and maximize social surplus. The policy maker could for instance distinguish internal governance, external knowledge sharing and indications with regards to the height and management of the cyber risk.

It is clear that in the current observed trend, cybersecurity information disclosure will not be harmonized by the industry itself. This led to the SEC proposal which will, when adopted, also impact Dutch companies that are listed in the US and might have a spill-over effect on listed companies outside the US. Furthermore, the emergence of sustainability reporting (CSRD) and increased transparency on a wide range of ESG-topics might lower the bar to (voluntary) report on cybersecurity for example as element of the internal risk- and control systems in the corporate governance of the company. Perhaps the revised version of the Dutch Corporate Governance Code might incorporate best practices on cybersecurity disclosures which could, due to the 'comply or explain' basis, stimulate transparency on cybersecurity. Also, if no efforts with regarding to external transparency are made by industry, other policy options might emerge to increase the diffusion of information regarding cybersecurity, such as the proposal for a compulsory IT/cybersecurity-audit.

6 Conclusion

This paper studied the annual reports of 75 listed firms in the Netherlands in relation to the disclosure of cybersecurity information from a financial law and economics perspective in four consecutive financial years (2018-2021). Also, we studied

legislative developments regarding cybersecurity disclosure requirements. Furthermore, we discussed some additional arguments emerged in the discussion regarding the social and private costs and benefits of cybersecurity transparency. We used financial law and economics perspective to draft hypotheses regarding the disclosure of cybersecurity information. Our two hypotheses were confirmed. The number of specific cybersecurity measures has increased, although 2021 shows a decline. Although there has been an increase in the amount of transparency, companies disclose various types of specific cybersecurity measures and that measures are distributed widely among companies. We come to the conclusion that, if the policy maker aims at maximizing the social benefits of cybersecurity information disclosure, it must perform a harmonization effort.

7 References

Ablon, L. et al. (2016) Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information. doi: 10.7249/rr1187

Anderson, R. (2001) 'Why information security is hard - An economic perspective', *Proceedings - Annual Computer Security Applications Conference, ACSAC*, 2001-Janua, pp. 358–365. doi: 10.1109/ACSAC.2001.991552.

Anderson, R., Böhme, R., Clayton, R., Moore, T. (2008) 'Security Economics and the Internal Market', Available at: https://www.enisa.europa.eu/publications/archive/economics-sec/ (Accessed: 26 February 2020).

Biener, C., Eling, M. and Wirfs, J. H. (2015) 'Insurability of cyber risk: An empirical analysis', *Geneva Papers on Risk and Insurance: Issues and Practice*, 40(1), pp. 131–158. doi: 10.1057/gpp.2014.19.

Bisogni, F., Asghari, H. and van Eeten, M. (2017) 'Delft University of Technology Estimating the size of the iceberg from its tip An investigation into unreported data breach notifications', *Proceedings of 16th Annual Workshop on the Economics of Information Security 2017 Citation*, 54.

Böhme, R. and Schwartz, G. (2010) 'Modeling Cyber-Insurance: Towards A Unifying Framework', (June), pp. 1–36, (Ninth Annual Workshop on the Economics of Information, Boston), https://pdfs.semanticscholar.org/7768/84d844f406fbfd82ad67b85ebaabd2b0e360.pdf accessed on 26 February 2020.

CBS (2019) 'Cybersecuritymonitor 2019', Available at: https://www.cbs.nl/-/media/_pdf/2019/37/cybersecuritymonitor-2019.pdf (Accessed: 26 February 2020, Dutch).

Chang, L.S., Most, K.S. and Brain, C.W. (1983) 'The Utility of annual reports: an international study', *Journal of international Business studies,* spring/summer, p.63-84.

Deloitte (2016) 'Cyber security: The changing role of the Board and the Audit Committee', (June), p. 5. Available at: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-cyber-security-noexp.pdf (Accessed: 20 February 2020).

Dudley, R. (2019) *The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks*, *Pro Publica*. Available at: https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks (Accessed: 20 February 2020).

Eling, M. and Schnell, W. (2016) 'What do we know about cyber risk and cyber risk insurance?', *Journal of Risk Finance*, 17(5), pp. 474–491. doi: 10.1108/JRF-09-2016-0122.

de Fuentes, J. M. *et al.* (2017) 'PRACIS: Privacy-preserving and aggregatable cybersecurity information sharing', *Computers and Security*. Elsevier Ltd, 69, pp. 127–141. doi: 10.1016/j.cose.2016.12.011.

Haller, I. *et al.* (2013) 'Dowser: a guided fuzzer for finding buffer overflow vulnerabilities', ;*login:: the magazine of USENIX & SAGE*, 38(6), pp. 16–19.

Hijink, J.B.S. (2010) 'Publicatieverplichtingen voor beursvennootschappen' (dissertation University of Amsterdam), Wolters Kluwer, 2010, Dutch.

https://www.dnb.nl/en/supervision/public-register).

Dutch Corporate Governance Code (2016) 'Dutch Corporate Governance Code' www.mccg.nl accessed 20 February 2020, Dutch.

Dutch DPA (2019) 'Meldplicht datalekken: facts & figures', https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/meldplicht_datalekken_feiten_en_cijfers_1e_helft_2019.pdf (Accessed: 20 February 2020).

Hussain, D., Ross, P. and Bednar, P. (2018) 'The perception of the benefits and drawbacks of internet usage by the elderly people', *Lecture Notes in Information Systems and Organisation*, 23, pp. 199–212. doi: 10.1007/978-3-319-62051-0_17.

ICO (2019) *Intention to fine British Airways £183.39m under GDPR for data breach | ICO*, *Information Commissioner's Office*. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/ (Accessed: 20 February 2020).

Kesan, J. P. and Majuca, R. P. (2004) 'University of Illinois College of Law The Economic Case for Cyberinsurance' Working paper, University of Illinois, IL.

Lawrence, D. and Robertson, J. (2017) *The Global Hack Could Have Been Much, Much Worse*, *Bloomberg Businessweek*. Available at: https://www.bloomberg.com/news/articles/2017-05-18/the-wannacry-global-hack-could-have-been-much-much-worse (Accessed: 22 January 2020).

Maersk (2017) '2017 Annual Report Maersk', (22756214). Available at: http://investor.maersk.com/static-files/250c3398-7850-4c00-8afe-4dbd874e2a85 (Accessed: 20 February 2020).

Moore, T. (2010) 'The economics of cybersecurity: Principles and policy options', *International Journal of Critical Infrastructure Protection*. Elsevier B.V., 3(3–4), pp. 103–117. doi: 10.1016/j.ijcip.2010.10.002.

Mukhopadhyay, A. *et al.* (2013) 'Cyber-risk decision models: To insure IT or not?', *Decision Support Systems*. Elsevier B.V., 56(1), pp. 11–26. doi: 10.1016/j.dss.2013.04.004.

Mulligan, D.K. (2007) 'Security Breach Notification Laws : Views from Chief Security Officers', *Samuelson Law, Technology & Public Policy Clinic, Univ. of California, Berkeley School of Law*, (December), pp. 1–52. Available at: https://www.law.berkeley.edu/files/cso_study.pdf (Accessed: 20 February 2020).

National Cyber Security Center (2018) 'Richt uw beleid voor Coordinated Vulnerability Disclosure in', https://www.ncsc.nl/aan-de-slag/coordinated-vulnerability-disclosure-beleid (Accessed: 20 February 2020, Dutch).

National Cyber Security Center (2018) 'Cybersecuritybeeld Nederland 2019', https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2019/juni/12/cybersecuritybeeld-nederland-2019/CSBN2019.pdf (Accessed: 20 February 2020, Dutch).

Nieuwesteeg, B. F. H. (2018) 'The Law and Economics of Cyber Security : De rechtseconomie van internetveiligheid'. Available at: https://www.narcis.nl/publication/RecordID/oai:repub.eur.nl:108963.

Nieuwesteeg, B.F.H. and Faure, M. (2018) 'An analysis of the effectiveness of the EU data breach notification obligation', *Computer Law and Security Review*. Elsevier Ltd, 34(6), pp. 1232–1246. doi: 10.1016/j.clsr.2018.05.026.

Olcott, J. (2018) *4 Cybersecurity Factors Every Board Member Must Consider for 2019 Planning*, *BITSIGHT*. Available at: https://www.bitsight.com/blog/4-cybersecurity-factors-board-members-2019-planning (Accessed: 20 February 2020).

Ostrom, E, '*The Evolution of Institutions for Collective Action,* (1st edn, Cambridge University Press 1990).

Pfleeger, C. (2003) 'Data security' in: A. Ralston, E.d Reilly and D. Hemmendinger (eds.), *Encyclopedia of Computer Science,* 4th edn., Wiley.

Shabana, K.M., Buchholtz, A.K. and Caroll, A.B. (2017) 'The Institutionalization of Corporate Social Responsibility Reporting', *Business & Society*, Volume: 56 issue: 8, page(s): 1107-1135 https://doi.org/10.1177/0007650316628177

Schneider, E. *et al.*, (2016), 'Cyber in the Boardroom. Helping Boards Meet Their Responsibilities Regarding Cyber Security' https://www.compact.nl/articles/cyber-in-the-boardroom/ (Accessed: 20 February 2020).

Shackelford, S. J. (2012) 'Should your firm invest in cyber risk insurance?', *Business Horizons*. 'Kelley School of Business, Indiana University', 55(4), pp. 349–356. doi: 10.1016/j.bushor.2012.02.004.

Sedee, M. (2017) Cyberaanvalblog https://www.nrc.nl/nieuws/2017/06/27/volg-hier-de-ontwikkelingen-rond-de-wereldwijde-randsomware-aanval-a1564740 (Accessed: 22 January 2020, Dutch).

Verschuren E. (2017) 'Wereldwijde aanval met ransomware treft ook deel Rotterdamse haven en TNT' https://www.nrc.nl/nieuws/2017/06/27/aanval-met-ransomware-op-containerbedrijf-haven-rotterdam-a1564693 (Accessed: 22 January 2020, Dutch).

8 Appendix

2018 ANNUAL REPORTS

AALBERTS
ABN AMRO
ADYEN
AEGON
AHOLD DELHAIZE
AKZO NOBEL
ARCELORMITTAL SA
ASML HOLDING
ASR
ROYAL DSM
GALAPAGOS
HEINEKEN
IMCD
ING GROUP
JUST EAT TAKEAWAY
KPN
NN GROUP
RANDSTAD
RELX
ROYAL PHILIPS
SHELL
UNIBAIL-RODAMCO-WESTFIELD
UNILEVER
VOPAK
WOLTERSKLUWER
AIRFRANCE-KLM
ALTICE EUROPE
AMG
APERAM
ARCADIS
ASM INTERNATIONAL
BASIC-FIT
BE SEMICONDUCTOR
BOSKALIS WESTMINSTER
CORBION
EUROCOMMERCIAL
FAGRON
FLOW TRADERS

FUGRO
GRANDVISION
INTERTRUST
OCI
POSTNL
ROYAL BAM GROUP
SBM OFFSHORE
SIGNIFY
TKH GROUP
TOMTOM
WDP
WERELDHAVE
ACCELL GROUP
ACCSYS
ALFEN
ACOMO
B&S GROUP
BINCKBANK
BRUNEL
FORFARMERS
HEIJMANS
ICT GROUP
KAS BANK
KENDRION
KIADIS
LUCASBOLS
NEDAP
NIBC HOLDING
NSI
ORDINA
PHARMING GROUP
VAN LANSCHOT
VASTNED
VOLKERWESSELS
WESSANEN
Z- NEWAYS ELECTRONICS

2019 ANNUAL REPORTS

ABN AMRO BANK
ADYEN
AEGON

AHOLD DELHAIZE
AKZO NOBEL
ARCELORMITTAL SA
ASML HOLDING
ASR NEDERLAND
ROYAL DSM
GALAPAGOS
HEINEKEN
IMCD
ING GROUP
JUST EAT TAKEAWAY
KPN KON
NN GROUP
PROSUS
RANDSTAD
RELX GROUP
ROYAL PHILIPS
SHELL
UNIBAIL-RODAMCO-WESTFIELD
UNILEVER
WOLTERSKLUWER
AALBERTS
AIR-FRANCE – KLM
ALTICE EUROPE
APERAM
ARCADIS
BASIC-FIT
BE SEMICONDUCTOR
BOSKALIS WESTMINSTER
CORBION
EUROCOMMERCIAL
FAGRON
FLOW TRADERS
FUGRO
GRANDVISION
INTERTRUST
NSI N.V.
OCI
PHARMING GROUP
POSTNL
ROYAL BAM GROUP
SBM OFFSHORE

SIGNIFY
TKH GROUP
VOPAK
WDP
ACCELL GROUP
ACCSYS
AFC AJAX
ALFEN
AMG
ACOMO
AVANTIUM
B&S GROUP
BRUNEL INTERNATIONAL
FORFARMERS
HEIJMANS
ICT GROUP
KENDRION
LUCASBOLS
NEDAP
NEWAYS ELECTRONICS
NIBC HOLDING
ORDINA
SIF HOLDING
SLIGRO FOOD GROUP
TOMTOM
VAN LANSCHOT
VASTNED
VIVORYON
WERELDHAVE

2020 ANNUAL REPORTS

ADYEN
AEGON
AHOLD DELHAIZE
AKZO NOBEL
ARCELORMITTAL
ASM INTERNATIONAL
ASML
ASR
BE SEMICONDUCTOR
HEINEKEN

IMCD
ING
JUST EAT TAKEAWAY
KPN
NN GROUP
PROSUS
RANDSTAD
RELX
ROYAL DSM
ROYAL PHILIPS
SHELL
SIGNIFY
UNIBAIL- RODAMCO- WESTFIELD
UNILEVER
WOLTERSKLUWER
AALBERTS
ABN AMRO
ALFEN
AMG
APERAM
ARCADIS
BASIC-FIT
BOSKALIS WESTMINSTER
CORBION
EUROCOMMERCIAL
FAGRON
FLOW TRADERS
FUGRO
GALAPAGOS
GRANDVISION
INTERTRUST
JDE PEET'S
KLM
OCI
PHARMING GROUP
POSTNL
SBM OFFSHORE
TKH GROUP
VOPAK
WDP
ACOMO
ACCELL

ACCSYS
AJAX
AVANTIUM
B&S GROUP
BRUNEL
CM.COM
FORFARMERS
HEIJMANS
HUNTER DOUGLAS
KENDRION
LUCASBOLS
NEDAP
NSI
ORDINA
ROYAL BAM GROUP
SIF
SLIGRO
TOMTOM
VAN LANSCHOT
VASTNED
VIVORYON
WERELDHAVE

2021 ANNUAL REPORTS

ADYEN
AEGON
AHOLD DELHAIZE
AKZO NOBEL
ARCELORMITTAL
ASM INTERNATIONAL
ASML
BE SEMICONDUCTOR
HEINEKEN
IMCD
ING
JUST EAT TAKEAWAY
KPN
NN GROUP
PROSUS
RANDSTAD
RELX

ROYAL DSM
ROYAL PHILIPS
SHELL
SIGNIFY
UMG
UNIBAIL
UNILEVER
WOLTERSKLUWER
AALBERTS
ABN AMRO
ACCELL
ALFEN
AMG
APERAM
ARCADIS
ASR
BASIC-FIT
BOSKALIS WESTMINSTER
CORBION
CTP
FAGRON
FLOW TRADERS GALAPAGOS
INPOST
INTERTRUST
JDE PEET'S
KLM
OCI
POSTNL
SBM OFFSHORE
TKH GROUP
VOPAK
WDP
ACOMO
ACCSYS
AZERION
B&S GROUP
BRUNEL
CM.COM
EBUSCO
EUROCOMMERCIAL
FASTNED
FORFARMERS

FUGRO
HEIJMANS
KENDRION
LUCAS BOLS
NEDAP
NSI
ORDINA
ROYAL BAM GROUP
SIF
SLIGRO
TOMTOM
VAN LANSCHOT
VASTNED
VIVORYON
WERELDHAVE