Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

An analysis of cybersecurity in Dutch annual reports of listed companies

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

Erasmus University Rotterdam, the Netherlands

ARTICLE INFO

Keywords:
Cybersecurity
Financial law
Annual report
Information sharing
Security regulation

ABSTRACT

In this paper we study the disclosure of cybersecurity information in Dutch annual reports, such as cybersecurity measures and cyber incidents, from a financial law and economics perspective. We start our discussion with an analysis of the requirements in financial law to disclose cybersecurity information in annual reports. Hereafter, we discuss the incentives for the board regarding disclosing cybersecurity related information and its effect on stakeholders and shareholders. We draft hypotheses regarding the actual disclosure of cybersecurity information and propose a research design of an exploring empirical study. The results of our study show that although there is no strict legal obligation to do so, 87% of the companies mention cybersecurity or similar words in their annual report in 2018. However, only 4 out of 75 companies disclosed more than six specific cybersecurity measures, while openness would generate the highest surplus for society from a social welfare perspective. Some major Dutch banks and employment agencies did not disclose any specific information with regard to their cybersecurity strategy, while those companies are highly vulnerable for cybersecurity incidents. This hampers the protection of creditors, investors and other stakeholders. Our analysis aims to propel the debate on stimulation of self-regulation or possible obligations in financial law concerning cybersecurity in annual reports.

1. Introduction

It is June 2017. The Wannacry and NotPetya cyber-attacks dominate world news and their impact is colossal. Wannacry infects over 300,000 computers (Lawrence and Robertson, 2017). NotPetya disrupts a quarter of the Rotterdam harbour for six days and its total cost estimations exceed €100 million (Verschuren, 2017; Sedee, 2017). The world sees, more than ever before, that cybercriminals can relentlessly punish suboptimal security. Consequently, scholars and academics urge that cybersecurity either is or should be 'a board-level topic' (Olcott, 2018; Schneider et al., 2016; Deloitte, 2016). 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. This study aims to contribute to this question by providing an exploring empirical analysis of the disclosure of cybersecurity information through the annual reports of listed companies in the Netherlands in 2018.

We will study the annual report in relation to the disclosure of cybersecurity information from a financial

* Corresponding author: B.F.H. Nieuwesteeg, Erasmus University Rotterdam, Burgermeester Oudlaan 50, 3062PA, Rotterdam, the Netherlands.
E-mail addresses: eijkelenboom@law.eur.nl (E.V.A. Eijkelenboom), nieuwesteeg@law.eur.nl (B.F.H. Nieuwesteeg).

https://doi.org/10.1016/j.clsr.2020.105513
0267-3649/

law and economics perspective. Hence, we first discuss in Section 2 whether there are requirements in financial law to disclose cybersecurity information in annual reports. Hereafter, in Section 3, we discuss 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.

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

This section briefly discusses the current requirements regarding disclosing cybersecurity information in annual reports. If requirements for the disclosure of cybersecurity information are in place, one would logically expect more information to be disclosed. This section starts with discussing the objectives of annual financial reports and subsequently discusses the requirements that result from these objectives. Hereafter, we discuss the mandatory disclosure of cyber incidents.

2.1. *Objectives of annual financial reports*

Annual financial 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".[1] The objectives of annual financial reporting are discussed in legislative history, case law and literature. For the board of management and the supervisory board, the annual financial report is a means to account for the management of the listed company. Disclosure of annual reports aims to contribute to efficient and accurate prices on the stock markets. The legal requirements regarding the disclosure of information aim to protect creditors, investors, and shareholders. Another objective of annual financial reporting is that disclosing information acts as a warrant of trust in the performance of the securities market for investors. Furthermore, disclosing information in annual financial reports contributes to corporate governance because it enables investors to make use of the rights to which they are entitled. From a law and economics perspective annual financial reports aim to mitigate agency-problems between management and shareholders by the disclosure requirements (Hijink, 2010; Chang et al., 1983).

2.2. *Requirements for annual financial reports of Dutch listed companies*

European legislation relating to financial reporting requirements is found in the EU Directive 2013/34/EU on the annual financial statements, consolidated financial statements, and related reports of certain types of undertakings, amending Directive 2006/43/EC and repealing the Fourth and Seventh EC Directives on Company Law. Dutch legislation relating to financial reporting requirements for listed companies is part of the Dutch Civil Code and the Dutch Financial Supervision Act. The EU Directive 2013/34/EU is transposed into Dutch national law. The implementation of EU Directive 2013/34/EU in the Dutch Civil Code became effective from financial years beginning on or after 1 January 2016. The Netherlands makes use of some member state options provided by Directive 2013/34/EU or its predecessors. Three examples of member state options the Netherlands uses can be found in Article 3(12) Directive 2013/34/EU on the calculation of thresholds on consolidated basis, Article 19(3) Directive 2013/34/EU on drawn up exemption for the managing directors' report for small legal entities and Article 23(1) Directive 2013/34/EU on consolidation exemptions for small groups.

Furthermore EU Directive 2014/95 EU – amending Directive 2013/34/EU – on the disclosure of non-financial and diversity information by certain large undertakings and groups affects the annual financial reporting by certain (large) listed companies. In the Netherlands, Directive 2014/95 EU is transposed in the Dutch Civil Code, by means of a 'Besluit bekendmaking diversiteitsbeleid' and 'Besluit bekendmaking niet-financiële informatie'. Legislation became effective from financial years beginning on or after 1 January 2017.

The annual financial reports are divided into three parts: the managing directors' report, the financial statements – consisting of a balance sheet, the profit and loss account with notes thereon and, if applicable, the consolidated financial statements – and additional data, consisting of other publication requirements referring to amongst others, the auditor's report[2] and 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.[3] Under European legislation[4] listed companies must prepare their consolidated financial statements in accordance with the International Financial Reporting Standards (IFRS). The annual financial report, including the financial statements of listed companies must be drawn up by the managing directors within four months after the end of the financial year.[5] Notably, reporting requirements on cybersecurity are absent, both in the European as well in the Dutch specific legislation relating to annual financial reporting.

[1] Preamble (4) Directive 2013/34/EU.

[2] Article 35 Directive 2013/34/EU and the implementation in the Dutch law Article 2:392 Dutch Civil Code.

[3] Article 41 Directive 2013/34/EU and the implementation in the Dutch law in Article 2:392a Dutch Civil Code.

[4] 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.

[5] 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.

In addition to the legal requirements, Dutch listed companies[6] are also required to report on compliance with the Dutch Corporate Governance Code (hereafter: the Code) in their annual financial report (Dutch Corporate Governance Code, 2016). The Code contains principles and best practice provisions that are aimed at defining the responsibilities for, amongst others, risk control. With regard to cybersecurity, the audit committee focuses on monitoring the management board concerning the application of information and communication technology by the company, including risks relating to cybersecurity.[7]

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.[8] The Guidelines of the Dutch Accounting Standard Board have widespread use. The Guidelines 400.110a and 400.110b provide guidance on disclosure requirements related to risk control which could include cybersecurity risk.

However, Guideline 400.129 guides on the compulsory nature of the disclosure requirements applicable to the management report.[9] 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.)

2.3. *Cybersecurity incident disclosure requirements*

Apart from requirements in financial law regarding disclosing cybersecurity information in annual reports, there is also mandated disclosure of cybersecurity incidents in cybersecurity and privacy law, being the General Data Protection Regulation (GDPR)[10] and the Directive on security of network and information systems (NIS Directive).[11] These types of cybersecurity incident disclosure do not specifically mandate an incorporation in the annual financial report. However, the data incident disclosure obligations from a cybersecurity law perspective could provide incentives for the board to also disclose cybersecurity information in the annual financial report. For instance, in many cases a data breach incident has to be notified to the data subject (this is often the consumer) according to Article 34 GDPR. Thus, the board might want, as part of its communication strategy, to further clarify the public incident in the annual report together with information on measures to prevent future data breaches. In Section 3, we will further discuss the costs and benefits of disclosing cybersecurity information in annual reports.

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).

The GDPR, which applies to almost all organisations that process personal data, mandates the communication of data breaches to the data protection authority and in most cases also to the data subject. The GDPR introduces public disclosure of data breaches by means of its data breach notification obligation (DBNO) in Articles 2(2), 4(7), 4(12), 33, 34 and 83(4) GDPR. Article 33 GDPR regulates disclosure to the DPA and Article 34 GDPR regulates public disclosure through informing data subjects. The NIS Directive[12] 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.[13] Article 1 (2) (d) NIS Directive states that the NIS Directive 'establishes security and notification requirements for operators of essential services and for digital service providers'. Article 14 (3) NIS Directive regulates the security breach notification for operators

[6] 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).

[7] Bpp 1.5.1 Dutch Corporate Governance Code.

[8] Supreme court of the Netherlands 10-02-2006 (KPN/Sobi), ECLI:NL:HR:2006:AU7473.

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

[10] 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).

[11] 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.

[12] 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'.

[13] 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 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).

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.[14] Article 16 (3) NIS Directive regulates the security breach notification for digital service providers. These incidents, such as for instance a cyberattack on a power grid, could also entail personal data breaches. These companies should however disclose personal data breaches under the GDPR regime. Vice versa, a data breach under GDPR does not automatically constitute a security incident under the NIS Directive. The DBNO in the GDPR covers (privacy) breaches of personal data, while the NIS Directive encompasses the confidentiality of services covered and the underlying data. Moreover, the threshold for notification regarding the cybersecurity incidents under the NIS Directive is much higher than according to the GDPR. We will discuss the ramifications of the notification obligations in the GDPR and NIS-directive for our research objective in more depth in Section 3.

Another obligation regarding companies that fall under the NIS directive is the fact that they should 'take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed' (Article 14 NIS Directive). Also, the competent authority has the power to mandate a security audit at the organisations that fall under the NIS-Directive (Article 15(2) NIS Directive).[15] The additional requirements in the NIS directive form the basis for the second hypothesis in Section 4.

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

This section discusses the potential costs and benefits of cybersecurity related information diffusion in annual reports. First, we will discuss the 'private' costs and benefits of disclosing cybersecurity information in annual reports. These are the negative and positive incentives for the board of directors and the supervisory board, which are the actors that have the decision-making and supervisory authority about whether cybersecurity information should be included in the annual report. Second, we will discuss costs and benefits for society, the so-called social benefit and costs. The society includes actors that directly or indirectly can benefit or get harm from the disclosure of cybersecurity information excluding the actors with decision-making authority.

3.1. *Private benefits*

Mentioning cybersecurity by the board of directors and the supervisory board (hereafter: the board) in the annual report has benefits regarding their relation to:

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

Signal board level priority. Regarding market actors, the board could use cybersecurity information in the annual report to disclose the current status of the resilience of the firm towards the cybersecurity risk. This could raise its attractiveness towards investors or creditors. One could argue that nowadays, every company is essentially an IT company. Without an appropriate IT system, it would be impossible for any listed company to operate its services. Hence, the breach of confidentiality, integrity or availability of IT systems could severely impact growth, revenue, and profit.[16] For instance, Maersk encountered a severe security breach in 2017 resulting from the not-Petya attack with an estimated cost between USD 250 million and USD 300 million (Maersk, 2017, p. 12).

Signal compliance with regulation. There is also a regulatory incentive for the board to increase transparency with regards to (compliance with) cybersecurity regulations. This is related to the increasing pace in which the regulator adopts legal instruments to induce organisations to increase their cybersecurity, such as the GDPR,[17] PSD2,[18] and the NIS directive.[19] The GDPR, for instance, specifies requirements for reasonable security: Article 25 GDPR requires data controllers to take 'appropriate technical and organisational measures'. The regulatory incentive is closely connected to the market incentive because there is an actual risk of penalties that could reach a level that impacts the financial performance of a company. For instance, the UK's data privacy authority (Information Commissioner's Office (ICO) has announced it intends to fine airline British Airways for failing to protect its customers' data. The airline will have to pay £183.39 million (€200 million) (ICO, 2019).

Trickledown effect in internal organisation. Lastly, by explicitly discussing cybersecurity, for instance through summarizing and validating the IT security investments in the annual report, the board stresses the importance of cybersecurity. This could stimulate awareness and change of cybersecurity of the internal organisation of the company. For instance,

[14] 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.

[15] As said, in the Netherlands, the Directive has been transposed into national regulation by a law called 'Wet beveiliging netwerken informatiesystemen', hereafter Wbni. Article 7(1) of the Wbni specifies that organisations should take appropriate and proportionate technical and organisational measures and hence transposes the requirements of the NIS directive. Also, Article 7(2) further specifies that the measures of the digital service provider referred to in the first paragraph should in any case take into account the following aspects: the security of systems and facilities; the handling of incidents; business continuity management; supervision, control and testing; and compliance with international standards.

[16] Pfleeger (2003) defines Confidentiality, Integrity and Availability (CIA).

[17] Regulation (EU) 2016/679, *OJ* 2016L 119

[18] Directive (EU) 2015/2366, *OJ* L 337

[19] Directive (EU) 2016/1148, *OJ* 2016L 194.

in the process of drafting the annual report, departments responsible for providing the relevant cybersecurity data are induced to cooperate and share knowledge with the department in charge of drafting the annual report. This fosters processes to prioritize, structure and synthesize this information. However, this benefit depends on the amount of detail regarding the cybersecurity policy that is requested. Research has shown the existence of internal benefits of prioritizing other pressing issues in annual reports, such as diversity, sustainability, and corporate social responsibility (Shabana et al., 2017).

3.2. *Private costs*

There are also costs involved in disclosing cybersecurity information in annual reports. We distinguish two types of information. On the one hand, we distinguish information regarding security investments such as SOAR (Security Orchestration, Automation and Response) measures and security awareness training. On the other hand, there is information that signals vulnerabilities, such as (potential) cybersecurity incidents.

Administrative cost. There is the internal administrative cost of the aggregation of information regarding cybersecurity measures and the process of selecting these measures.

Reputation damage. Insofar cyber incidents, such as data breaches or business interruptions are disclosed, this could lead to (perceived) reputation damage. Scholarly publications regarding the effects of reputation damage in cybersecurity show that data breaches could have some reputation damage in the short term, while effects in the long term are hard to disentangle from exogenous variables such as the growing demand for E-commerce (Bisogni et al., 2017; Nieuwesteeg and Faure, 2018). In practice, it is largely perceived reputation damage that provides negative incentives for organisations to disclose data breaches. One should also be aware that there is a significant time of delay between the publication of the annual report and the date of the incident, which mitigates the risk of reputation damage even further.

Providing information to the attacker. Extended disclosure of cybersecurity information can also have a negative impact on system security as such. For instance, when a company discloses information on the cybersecurity measures and policies it implemented, a perpetrator could use this information to adapt its attack strategy. There is anecdotal evidence from the US that companies that have publicly stated that they purchased cyber insurance are being attacked more by ransomware often because the attackers know that these companies will pay the ransom (Dudley, 2019). In the case of incident reporting, there would be a risk that the incident could reveal other connected vulnerabilities in the IT system of the company (or other companies, in this case it could be a social cost), when the company does not adopt the best practices for responsible disclosure (National Cyber Security Center, 2018a, 2018b).

Enhanced liability risk for cybersecurity incidents. This mainly applies to the publication of specific information regarding cybersecurity incidents, such as data breaches. The general logic is that the opportunity arises for the public to sue organisations when a data breach becomes public (Nieuwesteeg and Faure, 2018). Publication of data breaches is already mandatory according to Article 33 and 34 GDPR, and it would be unreasonable to assume that companies would mention data breaches in their annual reports without disclosing those data breaches according to the data breach notification obligation. Therefore, it is expected that cybersecurity information in annual reports only slightly raises the likelihood of liability costs. However, companies might have the perception that they need to take a proactive stance, being 'in the lead', concerning future class actions or other liability cases and therefore these companies might refrain from publishing cybersecurity information for which they could potentially be held liable.

3.3. *Social benefits*

There is a wide body of research that addresses information asymmetry in cybersecurity and hence stresses the societal need to enhance incentives for organisations to engage in cybersecurity information diffusion (Anderson, 2001; Anderson et al., 2008; De Fuentes, 2017; Nieuwesteeg, 2018).[20] In general, disclosure of cybersecurity information in annual reports can be seen as an instrument of an organisation to engage in such information diffusion. We discuss the benefits for two groups. First, we will discuss the social benefits for actors that have a direct relationship with the company, mostly investors and creditors. Second, we will discuss the indirect social benefits: the development of knowledge regarding the nature of cybersecurity risk and the return on investment of cybersecurity investments.

Direct social benefits for investors and creditors. With regards to the direct social benefits, investors (potential and actual shareholders) and creditors have a benefit of access to information about the cybersecurity incidents, resilience of the organisation, and the companies' strategy with regards to cyber risk management. However, it is currently unclear to what extent investors and creditors base their judgement on the information regarding cybersecurity provided in annual reports.[21] This connects to one of the main economic objectives of the financial law of annual reports, namely to overcome agency problems between management and shareholders. (Reference made to our discussion in Section 2.)

Indirect social benefits for society. With regards to the indirect social benefits, we should bear in mind that the marginal social benefits of information disclosure should be set against existing cybersecurity information disclosure. Currently, cybersecurity data is disclosed through data breach notification laws, surveys, qualitative and quantitative research, cyber insurance or norms and standardization of cybersecurity maturity levels. Also, various public organisations aggregate cybersecurity in the Netherlands. We name three examples. Statistics Netherlands (CBS) publishes an annual cyber-

[20] Nieuwesteeg (2018) defines information diffusion as 'the continuous circulation of information related to the return on cybersecurity investments and the nature of cybersecurity risk.' The diffusion of information is needed to determine strategies for companies to attain so called 'optimal' or 'reasonable' cybersecurity, which is stimulated from both a market and a regulatory pull.

[21] The market for cybersecurity rating agencies such as for instance the company BitSight or Cyrating is evolving, hence one could argue that there at least is an interest for information about the level of cybersecurity of organisations.

security monitor, which discloses an aggregated overview of various cybersecurity measures that different sizes of companies take (CBS, 2019). The Dutch National Cybersecurity centre provides a yearly update about recent cybersecurity threats (Cybersecurity Beeld Nederland). The Dutch Data Protection authority provides aggregated statistics regarding data breach notifications (Dutch DPA, 2019).[22] Companies such as Bitsight provide security ratings of organisations by scanning the outside network environment of the organisation.[23] The overarching pattern is that currently, information on an aggregated level is provided, while there is also a societal demand for more detailed information of individual companies to reach the benefits of cybersecurity information diffusion. In that sense, public disclosure of cybersecurity information by listed companies could complement the data that is already being provided by the institutions. Currently, there is a wide consensus among academic scholars in cybersecurity that there is insufficient objective cybersecurity data. (See for instance: Anderson, 2001; Moore, 2010; Böhme and Schwartz, 2010; Biener et al., 2015; Eling and Schnell, 2016.) Hence, information regarding cybersecurity in annual reports could lead to:

1.) Increased efficiency and effective cybersecurity investments, because organisations can utilize information from other organisations and do not have to reinvent the wheel.[24]
2.) Enhanced understanding of threat levels and incident rates at listed companies.
3.) Better cybersecurity products, such as cyber insurance.[25]

Naturally, in our case of cybersecurity information in annual reports, the benefits for other organisations to utilize this information strongly depends on the information that is diffused. For instance, when listed companies solely state their awareness regarding cybersecurity threats, there is little to be learnt from. But, when companies provide a detailed overview of cybersecurity measures, their respective cost relative to IT size and quality, their level of compliance with standards and the number of incidents, other organisations could use this information to benchmark their efforts and this information can be aggregated.

3.4. Social costs

There are also social costs involved in the disclosure of cybersecurity information in annual reports.

Notification fatigue. There is a risk that increased awareness regarding cybersecurity incidents (flowing from the information in annual reports) can lead to a decrease in the positive effects of disclosing this information. An information overflow reduces that meaningfulness of information diffusion and eventually all cybersecurity information could just be perceived as irrelevant information (Mulligan, 2007, p.33). This effect is labelled as 'notification fatigue' (Ablon et al., 2016; Nieuwesteeg and Faure, 2018). This effect is expected to be small, since annual reports are not widely read by the general public.

Reduction of trust. When more cybersecurity incidents become public, the increased awareness might lead to avoidance of digital services which would otherwise bring a net benefit to the consumer.[26] Although a negative effect could not be ruled out entirely, the effect is likely to be small because in general consumers do not tend to change from organisations when data breaches occur and more importantly, in general do not read annual reports of listed companies.

3.5. Synthesis

We briefly summarize the results of the analysis in Section 3. We display the private and social effects of alternative ways of mentioning cybersecurity in annual reports. One should note that the estimations of the effects are made for the indicative purpose of the overview and aim to reflect the insights of the literature. However, it is not a strict quantification of these effects.

Table 1 shows that we do not observe any private cost or benefit when an organisation decides not to disclose any information regarding cybersecurity in the annual report. Likewise, there is also no social benefit or cost, other than opportunity costs, which can be observed as the difference with the benefits of the two other scenarios. Mentioning cybersecurity has clear benefits and only little cost for the organisation that publishes it in the annual report. Consider, for instance, the benefit of signalling board-level priority and the trickledown effect. Arguably, the administrative cost of mentioning cybersecurity is low and the risk of reputation damage and transferring information to the attacker is non-existent. Mentioning cybersecurity has social benefits. Shareholders and stakeholders can

[22] See for instance: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/meldplicht_datalekken_feiten_en_cijfers_eerste_helft_2019.pdf

[23] BitSight: https://www.bitsight.com (Accessed: 22 January 2020).

[24] However, the cost of information diffusion should not be higher than the benefits of not reinventing the wheel (Nieuwesteeg, 2018).

[25] A frequently observed barrier for growth in the cyber insurance market is the fact that the impact of cyber risks theoretically operationalizes simultaneously among actors. Insurers are hesitant to insure risks which are strongly correlated because in such a situation the average pay out does not approach the average risk. This is caused by the fact that information technology is based on identical underlying technological principles combined with the observation many organisations use similar pieces of software such as Microsoft, Adobe or SaaS platforms. Hence, the IT infrastructure companies are vulnerable to the same treats. In theory, one could model cases of heavy risk correlation: a zero-day exploit in a Microsoft, a vulnerability in accounting software, or a vulnerability in a widely used file viewer. We have seen this in the 2017 Wannacry and NotPetya attacks. Although, also regarding these attacks, solely 3% of organisations that had that vulnerability were hit. Still, I would consider this as a large number since many organisations used the system that contained that vulnerability. Nevertheless, there is little empirical evidence about the extent of correlation for various types of cyber risk. Disclosure of cybersecurity information in annual reports could verify or falsify the assumption of correlative risks and potentially propel the market for cyber insurance products.

[26] For instance, Hussain et al. (2018) state that "elderly people are anxious about Internet security, as they believe they can be victimised, hence the reason why the generation avoids the technology as much as possible".

Table 1 – Benefits and costs of alternative ways of mentioning cybersecurity in annual reports.

	Private benefit	Private cost	Social benefit	Social cost
Not mentioning cybersecurity	0	0	0	0
Mentioning cybersecurity	+ +	−	+	0
Mentioning specific information such as measures or incidents	+ +	− −	+ + +	0/-

for instance observe that a company pays (some) attention towards cybersecurity risk. Publishing extended cybersecurity information has a relatively high private cost related to reputation damage and potential future liability claims, but also the highest social benefits since it capitalizes on the stimulation of information diffusion regarding the nature of cybersecurity risk and the type of cybersecurity investments that companies make.

4. Research design, hypotheses, and 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 financial reporting. In principle, companies are allowed to disclose their cybersecurity information in their financial reporting. In our empirical research design, we observe whether public companies pay attention to cybersecurity in their annual reporting; and therein:

- the amount of attention companies dedicate to cybersecurity;
- the part(s) of the annual report that include(s) cybersecurity information; and
- the type of cybersecurity information companies include.

The empirical study investigates the 2018 annual reports published by companies listed on Euronext Amsterdam that are part of the AEX, AMX and AScX Indices.[27] The indices contain 75 public companies. Some of these public companies fall within the scope of the NIS Directive. The NIS Directive is transposed in Dutch national legislation (the aforementioned Wbni). We categorized the public companies by analysing the Wbni and the Dutch decree (in Dutch: Algemene Maatregel van Bestuur) that specifies organisations that fall within the scope of the Wbni. However, the Dutch Cyber Security Centre that plays a role in the execution of the Wbni, does not publish nor confirm which companies fall under the scope of the Wbni. Moreover, according to the Wbni some digital service provides have to identify themselves as part of the scope of the Wbni. Due to the openness of the standard and a missing overview of companies that fall within the scope of the NIS Directive, we identified, to the best of our knowledge, the public companies for which we assume that they fall within the scope. The Appendix contains the details. First, we searched the annual reports for the selection of the following words:

- Cyber (including the more specific terms cybersecurity and cyber risk)
- Information security
- Data protection

Secondly, we checked for information about specific cybersecurity measures by searching for the following selection of keywords:

- Two-factor or multi-factor authentication[28]
- Penetration test[29]
- Network monitoring[30]
- Network compartmentalization[31]
- Cyber insurance[32]

[27] The composition of the indices is derived from aex.nl in October 2019.

[28] Proper authentication is one of the core principles of cybersecurity, and two or multifactor authentication is quickly become the new standard, also driven by regulation, such as PSD2, which demands strong customer authentication (Article 91 PSD2), which is two or multifactor authentication.

[29] Penetration testing is (category of) security activities to review the status of your network ex ante and is widely offered by cybersecurity companies such as Fox It, Deloitte and Qbit.

[30] Network monitoring is becoming an increasingly important building block in a cybersecurity strategy, since it continuously provides a certain level of security instead of a one-time action. Parties such as Guardian 360 fully specialize in network monitoring.

[31] While, penetration testing and network monitoring are in essence outside actions that can for instance be performed by a cybersecurity provider, network compartmentalization is an inherent structural element of a secure IT system. For instance, during the 2017 NotPetya, Maersk failed to compartmentalize its network, it essentially treated its IT system as one homogeneous network with no internal boundaries and controls. This resulted in the spread of the ransomware. Albeit a slightly more detailed security measure, given the fact that a listed company experienced a major cyber attack precisely because of the lack of compartmentalization, we include it as a key word to search for.

[32] Cyber insurance is a risk management technique to provide cover for risk aversion through the (partial) transfer of cyber risks (those which are low probability, high impact risks) to a third party in return for a premium (Mukhopadhyay et al., 2013; Shackelford, 2012).This transfer is a remedy for risk aversion when firms are more risk averse than insurers, and the costs of the transfer do not outweigh the benefits (Kesan and Majuca, 2004). There is a growing demand for cyber insurance as a risk management technique in cybersecurity, although its development is hindered by highly interrelated losses, lack of data, and severe information asymmetries (Biener et al., 2015).

The words were selected based on a technical analysis of cybersecurity measures. We included a variety of cybersecurity measures which are commonplace when defining a cybersecurity strategy. Hence, we reviewed several technical documents of public and private industry leaders such as the Ponemon Institute, Fox IT, AON and the European Union Agency for Cybersecurity, to gain an overview. We selected those measures that have a level of generality that would be suitable for publication in a general report. Typically, we would not expect very specific cybersecurity measures such as for instance observed by Haller et al. (2013). In addition to the predefined measures, we also counted the number of other specific cybersecurity measures that companies included in their annual report, such as the appointment of a data protection officer, collaboration with specific institutes and an awareness program. Our count of other specific measures did not include unspecified measures such as 'controls' or 'policies' which did not point out further details.

Lastly, we searched for information about data breaches. We used the following key words[33]:

- Data breach
- Incident

The amount and the location of the search hit(s) are included in a database and categorized into the following categories:

- Awareness
- Data protection
- Incidents
- Other

Although the total selection of search terms seems limited, the broad scope of the words covers the vast majority of information related to cybersecurity in the annual financial report. At the start of our research we tested the bag of words by randomly selecting five annual reports and verifying by hand if our search terms covered all the information related to cybersecurity in those annual reports. After this initial search we added the words 'data breach' and 'incident' to the search terms because those words also revealed paragraphs related to cybersecurity that had a small change of being overlooked when using the original bag of words. Furthermore, during testing each search hit was verified by hand in the sense that the information presented around the search hit was read and interpreted by means of professional judgement by the research team. Only the relevant information related to cybersecurity was included in the research.

Despite our research method, a chance exists that information relating to cybersecurity in the annual financial report does not correspond to the search terms resulting in absence in the search results. However, the probability of this kind of non-correspondence is small due to the fact that legal reporting requirements on cybersecurity are absent for annual financial reporting (par. 2.2). The main focus of the annual financial report is not only to provide information for investors in capital markets but also give an account of past transactions and enhance corporate governance (par. 2.1.). Stated differently, traditionally the focus of the annual financial report is on financial information. If information on cybersecurity is provided, indicating that additional information is voluntarily provided, it is most likely that the focus is on transparent disclosure on cybersecurity indicating use of direct language.

4.2. *Hypotheses*

In this brief section, we draft hypotheses based on the research design on whether there will be spontaneous disclosure of cybersecurity information in annual reports. Since there is no direct regulatory obligation to do so, as observed in our legal analysis in Section 2, we based our hypotheses purely on our cost and benefit framework in Sections 3.1 and 3.2 that outlines incentives of the board to disclose cybersecurity information.

H_1: We expect that companies mention cybersecurity in their annual reports since private benefits of mentioning cybersecurity outweigh the cost, but do not provide extended cybersecurity information because here the comparative cost is higher than solely mentioning cybersecurity.

H_2: We expect that companies that fall under the NIS Directive, which are digital service providers and operators of essential services, disclose more information on cybersecurity in their annual reports than companies that do not fall under the NIS Directive because this directive imposes additional requirements for cybersecurity.[34]

4.3. *Results*

The results, visualized in Table 2, show that 10 of the total population of 75 companies (˜ 13%) do not include information on cybersecurity in their annual report of 2018.[35] These ten companies represent 7 of the total of 22 sectors of the population.[36] Furthermore, AEX-companies perform better than AMX and AScX companies with attention for cybersecurity in 23 and 21 annual reports respectively.

Table 3 provides a more in-depth insight into the annual reports that contain information on cybersecurity. Our research shows that information on cybersecurity can be found

[33] We are aware that a regulatory incentive for including the disclosure of cyber incident (depending on whether it potentially would fall within the NIS Directive), could differ from a data breach, which is more likely to be connected to obligations in the GDPR, as discussed in Section 2.3.

[34] https://zoek.officielebekendmakingen.nl/stb-2018-388.html ; Digital Service providers are providers such as online marketplaces, online search engines and cloud computing services which are to the best of our knowledge not present in the AEX/AMX. Furthermore, the by the Dutch competent supervisory authority – De Nederlandsche Bank N.V. – appointed credit institutions as referred to in Article 4(1) Regulation (EU) no 575/2013 fall within the scope of the NIS Directive.

[35] Attention for cybersecurity is lacking in the annual reports 2018 of AEX companies: Arcelormittal and Galapagos; AMX companies: AMG, Eurocommercial, Fagron and WDP; and AScX companies: ACCSYS, Kiadis, SIF Holding and Vastned.

[36] These sectors are Basic Resources, Biotechnology, Construction & Materials, Energy, Health care, Industrial Goods & Services and Real Estate.

Table 2 – Presence of cybersecurity information in annual reports 2018.

		AEX	AMX	AScX
Attention for cybersecurity in annual report 2018	YES	23*	21	21
	NO	2	4	4

* The annual report of Takeaway does not include the word 'cyber' but mentions 'IT security' therefore Takeaway is included in this result.

Table 3 – Appearance of cybersecurity information in annual reports in 2018.

		AEX	AMX	AScX
Appearance of 'cyber' in annual report	Financial statements	5	2	3
	Managing directors' report	23*	20	9
	Supervisory report	16	11	10
	Additional data	6	1	11

* The annual report of Takeaway does not include the word 'cyber' but mentions 'IT security' therefore Takeaway is included in this result.

Table 4 – Information on specific cybersecurity measures in annual reports 2018.

	AEX	AMX	AScX
Two-factor or multifactor authentication	1	2	–
Penetration test	1	2	3
Network monitoring	1	1	–
Network compartmentalization	2	1	–
Cyber insurance	5	2	2
Total number of companies mentioning at least one specific measure	5	4	5

throughout the entire annual report. However, the managing director's report and supervisory report are relatively used most. Specifically, all AEX companies and all except one AMX company use the managing directors' report to disseminate cybersecurity information. The supervisory report is used by 16 AEX and 11 AMX companies. Similar to the information in the managing directors' and supervisory report, the information on cybersecurity in the financial statements are qualitative descriptions. For example, ASR refers to cybersecurity in the notes to the operation risk. Information on cybersecurity in the annual reports of AScX companies is more widespread than in the annual reports of AEX and AMX companies. Especially the section in the annual report that contains 'additional data' is used more often by AScX companies.

Table 4 contains details regarding five predefined specific cybersecurity measures. Granted most annual reports contain information on cybersecurity measures, the five specific measures[37] we searched for were represented less often. We discovered 31 measures that fall under the five specific measures that we predefined and 93 other specific measures that we did not predefine. Hence, in total, 124 specific cybersecurity measures were disclosed in the 75 annual reports we investigated. Information on the five predefined specific cybersecurity measures in the annual reports is provided by 14 companies. Five AEX companies mention at least one specific measure.[38] Information on the specific cybersecurity measures is presented in the annual report of four[39] of the AMX companies and five[40] of the AScX companies. Notable is that all the AEX companies mention cyber insurance. Besides information on cyber insurance, two companies also add information on other of the five predefined specific measures. For example, AEX company Unibail-Rodamco-We provides details on all of the specific cybersecurity measures that are part of this research. Although a reference to all specific cybersecurity measures can be found in the annual reports of the AMX companies – different than the AEX companies – not one of the AMX companies mentions all five predefined specific measures. However, two of the companies mention more than one measure.[41] Each of the five AScX companies refer to one specific cybersecurity measure, namely penetration test[42] or cyber insurance.[43]

As reflected in Table 2 approximately 87% (65 out of 75) of the listed companies refer to cybersecurity in their annual reports. Specifically, fourteen companies refer to specific cy-

[37] Those are two-factor or multifactor authentication, penetration test, network monitoring, network compartmentalization and cyber insurance.

[38] Aalberts NV, Adyen, Aegon, Ahold Delhaize and Unibail-Rodamco-We.

[39] Corbion, Fugro, OCI and KLM.

[40] Alfen, Ordina, Nedap and NSI and Van Lanschot.

[41] KLM and OCI refer to cyber insurance, Corbion and Fugro refer to implementation of multifactor authentication and penetration tests. Furthermore, Corbion adds, in a more implicit way, information on network monitoring and network compartmentalization.

[42] Ordina, Nedap and NSI.

[43] Alfen and Van Lanschot.

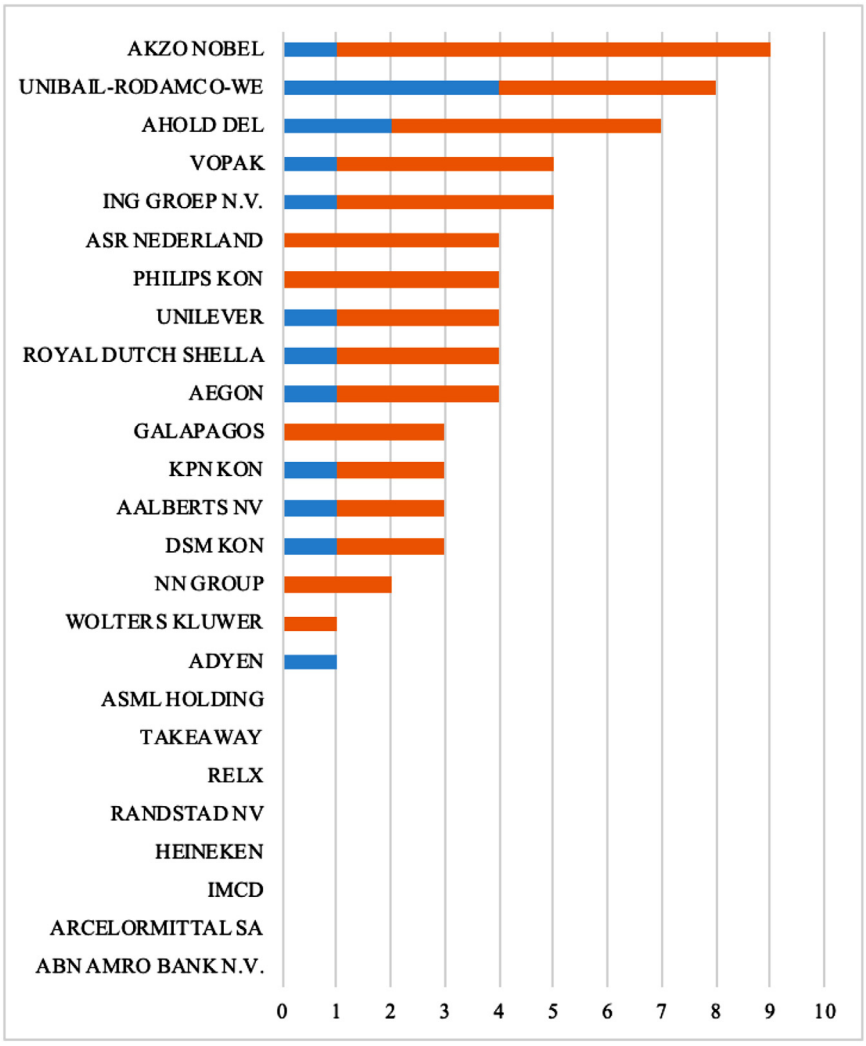

Fig. 1 – Sum predefined and other specific measures (AEX companies).

Table 5 – Information on other cybersecurity measures in annual reports 2018.

	AEX	AMX	AScX
Total number of companies mentioning other than the specific measures	19	19	15

bersecurity measures, see Table 4. Consequently, as depicted in Table 5, most companies mention cybersecurity measures other than the specific measures.

Other cybersecurity measures companies report on are, amongst others, the appointment of information security officers,[44] formulating specific internal policies,[45] and organisation of security awareness campaigns and/or workshops.[46] In the Figs. 1-3, we display the sum of the number of predefined specific measures per annual report (in blue) with the number of these other specific cybersecurity measures (in red).

Besides mentioning cybersecurity measures, one company in our sample reported on experienced data breaches and/or incidents.[47] Fig. 4 shows the disclosure of specific measures by companies, for which we assume that they fall under the

[44] Companies that mention the appointment of information security officers or other dedicated information security personnel are ING Groep N.V., Akzo Nobel, Philips Kon, NN Group, KPN Kon, Fugro, V Lanschot Kempen, Brunel International, Heijmans, Forfarmers and ICT Group.

[45] Companies that mention (re)formulating security policies are Randstad N.V., Wolters Kluwer, Unilever, Takeaway, Boskalis, Corbion, TKH Group, Basic-Fit, Alfen and NSI N.V.

[46] Companies that mention raising awareness by campaigns or workshops are DSM Kon, Vopak, ASR Nederland, NN Group, Boskalis, Arcadis, Air France – KLM, Volker Wessels, B&S Group, ForFarmers, Wessanen, NSI N.V., ICT Group.

[47] The 2018 Annual report of Philips (p.56) states: "Philips has experienced cyber attacks but to date has not incurred any signifi-

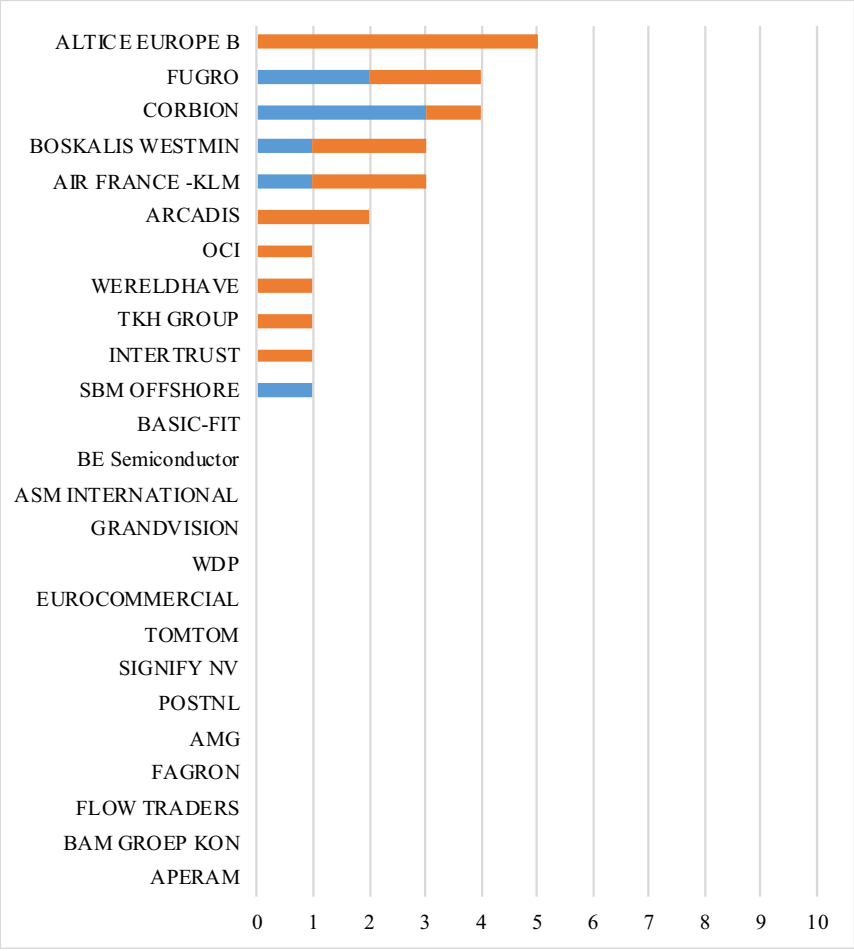

Fig. 2 – Sum predefined and other specific measures (AMX companies).

NIS Directive.[48] While KPN and Air France – KLM disclose three specific measures, Adyen, BinckBank and ABN-AMRO do disclose below average or not at all. Kas Bank discloses two specific measures.

To summarize, roughly 13% of (10 out of 75) of listed companies in the Netherlands do not mention cybersecurity at all in their annual reports. Forty of the listed companies provide specific information regarding cybersecurity strategy, incidents or investments, although this information is not very detailed. Only four companies, Akzo-Nobel, Unibail-Rodamco-We, Van Lanschot Kempen and Ahold provide more than six specific measures. Two listed companies that assumedly fall under the scope of the NIS directive, being ING Bank and KLM, describe their cybersecurity measures relative extensively. However, ABN AMRO only mentions the importance of cybersecurity, without describing any cybersecurity measure. Adyen mentions the importance of cybersecurity and describes that they implemented cyber insurance.

5. Discussion

From a financial law and economics perspective, our results show that, on average, about half of the listed companies share specific cybersecurity measures and hence share more information than just mentioning cybersecurity as an important topic. From a cost and benefits point of view, this implicates that these companies, at least to some extent, are willing to take some of the negative private costs associated with disclosing cybersecurity information. For example, nine companies mention the purchase of cyber insurance. However, only four companies provide more than six specific cybersecurity measures. The exploratory nature of the research prohibits us to make strong implications, but this observation tends to be in line with the expected reluctance of companies to strive for extensive disclosure of cybersecurity measures. None of the companies disclosed a data breach in the annual report. This also means that there currently is no overlap with the data breach notification obligation in the GPDR.

This leads to our prudent conclusion that the first hypothesis is confirmed. Most companies indeed disclose minor information on cybersecurity. However, extensive openness is not yet common practice, although this could be beneficial

cant damage as a result, or incurred significant monetary cost in taking corrective action."

[48] The Appendix contains the details.

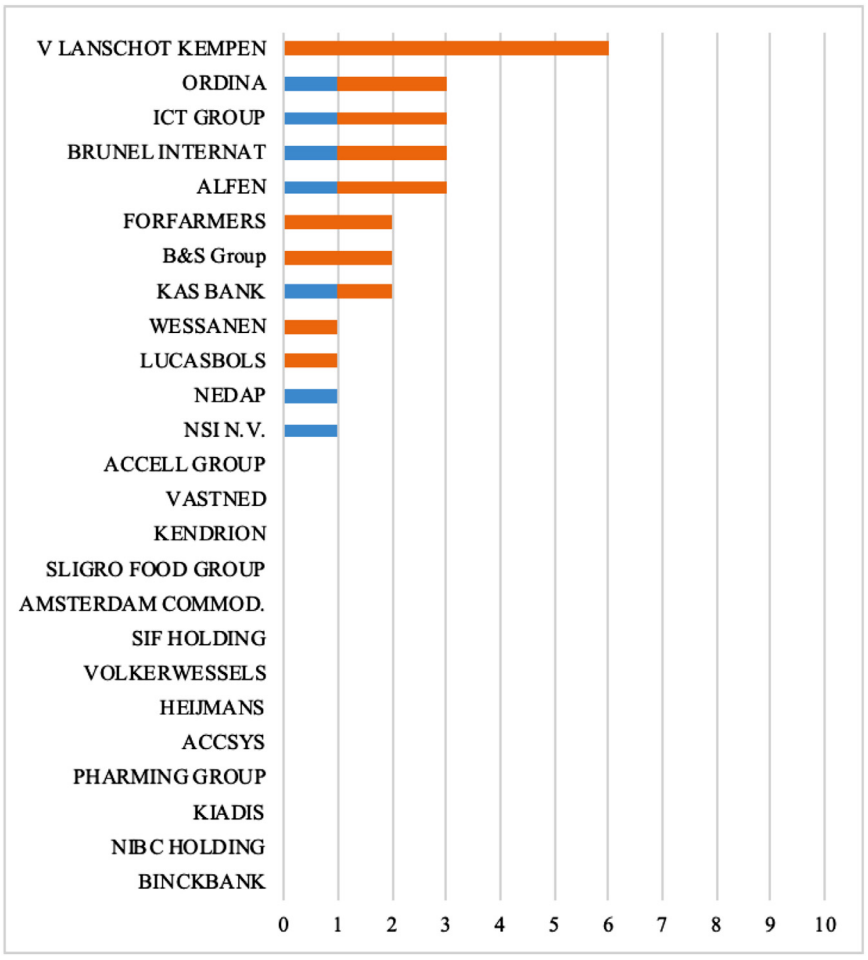

Fig. 3 – Sum predefined and other specific measures (AScX companies).

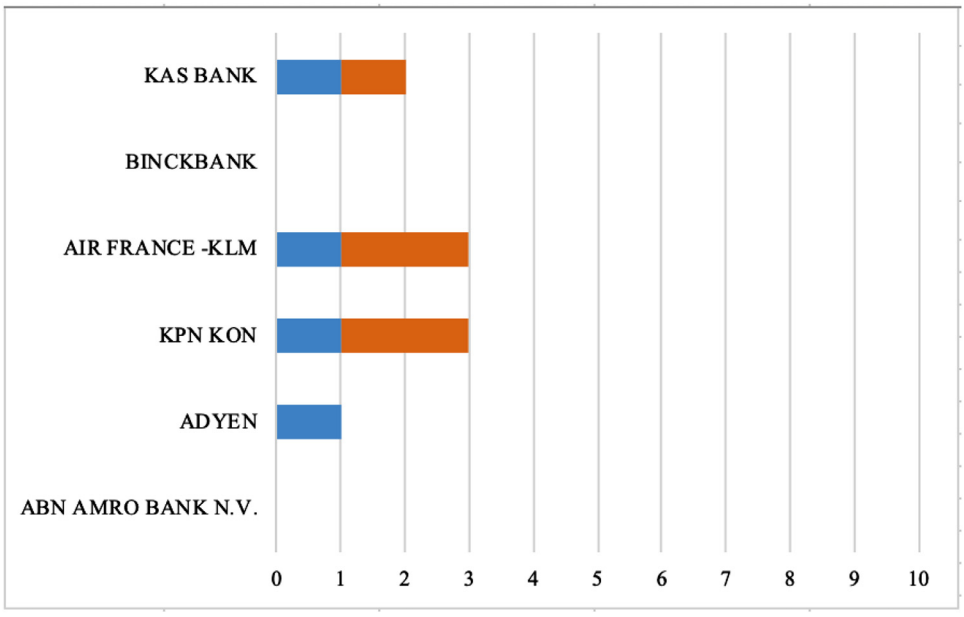

Fig. 4 – Sum predefined and other specific measures for companies for which we assume that they fall under the NIS directive.

for society. Hence, we observed the characteristics of a possible market failure, but more research is definitely needed to further strengthen this observation. When the presence of a market failure could be established, the status quo yields suboptimal spontaneous diffusion of information in annual reports. A social surplus of extended disclosure of cybersecurity information in annual reports is likely to remain, even when net private costs are taken into account as observed in Section 3.5. The legislator could induce listed companies to disclosing extended cybersecurity related information by drafting new or adjusting current legislation. An example of the latter could be an adjustment of the Non-financial reporting Directive (2014/95/EU) which requires listed companies, amongst others, to disclose information on policies they implement on for example diversity, environmental protection, anti-corruption and bribery. Extending the scope of this Directive with disclosure requirements for cybersecurity information could be a policy option. The national legislator could implement the requirements in national law. In the Netherlands, this could be done in for example the Dutch Civil Code. A less invasive option might be the implementation of disclosure requirements regarding cybersecurity in a Code with comply or explain requirements such as the Dutch Corporate Governance Code.

The second hypothesis is not confirmed. Companies for which we assume that they fall under the NIS directive, and have higher regulatory cybersecurity duties, do not disclose more specific cybersecurity information in their annual reports. However, more research is needed regarding the correlation between disclosing extensive cybersecurity information in the annual report and the actual level of cybersecurity. We know from studies regarding diversity, sustainability, and corporate social responsibility that priority in the annual report can have a trickledown effect in the company, but currently such research is lacking in the field of cybersecurity.

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. We discussed whether there are requirements in financial law to disclose cybersecurity information in annual reports and observed that there is no requirement in financial law that induces listed firms to disclose any cybersecurity related information. Hereafter, we discussed the incentives for the board of disclosing cybersecurity related information in the absence of the law. We discussed private incentives and social effects on third parties such as stakeholders and shareholders from a law and economics perspective.

We used financial law and economics perspective to draft hypotheses regarding the disclosure of cybersecurity information. We found these hypotheses largely confirmed in the sense that the majority of the listed firms in the Netherlands (94%) only mentioned cybersecurity or only disclosed less than six specific cybersecurity measures such as performing a security awareness training. 13% of the listed companies did not mention cybersecurity (or similar words) at all. Significant openness would, according to our analysis of incentives, generate the highest surplus for society and companies themselves. Although we would like to stress the exploratory character of our research and the lack of research on this topic, there could be a case for regulation if the amount of cybersecurity information diffusion by listed companies does not improve in the upcoming years.

Declaration of Competing Interest

No conflict of interest identified.

Appendix A

This research is based on the 2018 annual reports published by companies listed on Euronext Amsterdam that are part of the AEX, AMX and AScX Indices. The composition of the indices is derived from aex.nl in October 2019. Table A1 contains the total population of the 75 public companies that are part of this research. The companies we assume that fall within the scope of the NIS Directive are indicated with an *.

In order to identify companies that fall under the NIS Directive, we first scrutinized the Wbni. Article 5 (1) (a) Wbni states that the 'operators of essential services' will be defined by governmental decree. On 30 October 2018, the Dutch government issued such a decree called 'besluit beveiliging netwerk en informatiesystemen' (Bbni) (Stb. 2018,388).[49] As a background check, we reached out to the Dutch National Cyber Security Centre (NCSC), which falls under the Dutch ministry of Justice and Security. Companies that fall within the scope of the Wbni have to notify security incidents within the scope of the Wbni to the NCSC. Unfortunately, the Wbni does not share information with third parties which companies fall within the scope of either operators of essential services or digital service providers, even if the companies are transparent about that fact themselves.

Hence, we can only provide an assumption based on the NIS-Directive, Wbni and Bbni about which listed companies fall within the scope of the NIS-Directive.

We scrutinized the Bbni and came to the conclusion that Dutch listed companies with a banking license (which is a criterium in the decree, see Article 2 Bbni) fall within the scope of the NIS Directive. The Dutch Central Bank (DNB) holds a public register containing all Dutch licensed banks (DNB, 2020). Dutch listed companies with a banking license are ABN Amro Bank N.V., Adyen N.V., Binckbank N.V. and KAS BANK N.V. It should be noted that the licensed bank does not have to be the listed company, see for example ING Groep N.V, which does not have a banking license, while its subsidiaries (could)

[49] There are a few differences between the list of types of essential services in Annex II of the NIS Directive and the list of types of essential operators in the Dutch governmental decree. For instance, the Dutch decree includes telecommunication services. Because of the fact that the NIS Directive is a directive and hence requires national implementation, we will use the governmental decree to identify which companies fall within the scope of the NIS Directive in the sense that they can be classified as operators of essential services.

Table A1 – Overview of Euronext companies.

AEX	AMX	AScX
AALBERTS NV	AIR FRANCE –KLM *	ACCELL GROUP
ABN AMRO BANK N.V. *	ALTICE EUROPE B	ACCSYS
ADYEN *	AMG	ALFEN
AEGON	APERAM	AMSTERDAM COMMOD.
AHOLD DEL	ARCADIS	B&S GROUP
AKZO NOBEL	ASM INTERNATIONAL	BINCKBANK*
ARCELORMITTAL SA	BAM GROEP KON	BRUNEL INTERNAT
ASML HOLDING	BASIC-FIT	FORFARMERS
ASR NEDERLAND	BE SEMICONDUCTOR	HEIJMANS
DSM KON	BOSKALIS WESTMIN	ICT GROUP
GALAPAGOS	CORBION	KAS BANK*
HEINEKEN	EUROCOMMERCIAL	KENDRION
IMCD	FAGRON	KIADIS
ING GROEP N.V.	FLOW TRADERS	LUCASBOLS
KPN KON*	FUGRO	NEDAP
NN GROUP	GRANDVISION	NIBC HOLDING
PHILIPS KON	INTERTRUST	NSI N.V.
RANDSTAD NV	OCI	ORDINA
RELX	POSTNL	PHARMING GROUP
ROYAL DUTCH SHELLA	SBM OFFSHORE	SIF HOLDING
TAKEAWAY	SIGNIFY NV	SLIGRO FOOD GROUP
UNIBAIL-RODAMCO-WE	TKH GROUP	V LANSCHOT KEMPEN
UNILEVER	TOMTOM	VASTNED
VOPAK	WDP	VOLKERWESSELS
WOLTERS KLUWER	WERELDHAVE	WESSANEN

have. The reporting requirements are applicable to the licensed bank, so for the analysis we take into account whether the (report of) the listed company falls within the scope of the NIS directive. That means that we assume the listed company as such needs to have a banking license.

Also, Air France-KLM falls within the scope of the Directive, since this company has more than 25% of the total amount of flight movements on Schiphol airport, which is also a criterium in the decree (Article 2 Bbni). Moreover, we believe that KPN falls within the scope of the NIS directive, since this is 'a provider of an electronic communication network.' (Article 3 Bbni).

Annex III of the NIS directive determines the scope of Digital Service Providers. There are no companies that primarily operate an online market place or an online search engines among the 75 listed companies that are investigated and displayed in Table 1. With regards to cloud computing service, there is some more uncertainty whether listed companies are delivering cloud computing services. Article 4 (19) NIS directive defines a cloud computing service as a 'digital service that enables access to a scalable and elastic pool of shareable computing resources'. To the best of our knowledge,we did not observe companies that deliver cloud computing services as a primary activity. Hence, we made the decision not to label any listed company as a cloud computing service provider. However, it should be noted that it that could be a margin of error when labelling DSPs, since DSPs have to identify themselves as DSPs and the NCSC does not give a confirmation whether a company could be identified as a DSP.

Table A2 contains an overview of sectors represented in the research sample. Furthermore, the sector division per index is visualized.

Table A2 – Overview of amount of companies per sector.

Sector	AEX	AMX	AScX
Banks	2		4
Basic resources	1	1	
Biotechnology			2
Business services			1
Chemicals	3		
Construction and materials		3	3
Distribution services			1
Energy			1
Financial services		2	
Food and beverage	1	1	5
Health care	2	1	
Industrial goods and services	4	5	2
Insurance	3		
Media	2		
Oil and gas	1	2	
Personal and household goods	1	1	
Real estate	1	3	2
Retail	2	1	
Sporting goods			1
Technology	1	2	3
Telecommunications	1	1	
Travel and leisure		2	

REFERENCES

Ablon, L. et al. (2016) Consumer attitudes toward data breach notifications and loss of personal information. doi: 10.7249/rr1187

Anderson R. Why information security is hard – an economic perspective. Proceedings of the annual computer security applications conference, ACSAC; 2001. p. 358–65 2001-Janua.
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, Wirfs JH. Insurability of cyber risk: an empirical analysis. Geneva Pap Risk Insur: Issues Pract 2015;40(1):131–58. doi:10.1057/gpp.2014.19.
Bisogni F, Asghari H, van Eeten M. Delft University of Technology Estimating the size of the iceberg from its tip: an investigation into unreported data breach notifications. Proceedings of the 16th annual workshop on the economics of information security; 2017 2017 citation, 54.
Böhme R, Schwartz G. Modeling cyber-insurance: towards a unifying framework. Proceedings of the ninth annual workshop on the economics of information; 2010. p. 1–36. https://pdfs.semanticscholar.org/7768/84d844f406fbfd82ad67b85ebaabd2b0e360.pdf.
CBS (2019) 'Cybersecuritymonitor 2019', Available at: https://www.cbs.nl/-/media/_pdf/2019/37/cybersecuritymonitor-2019.pdf (Accessed: 26 February 2020, Dutch).
Chang LS, Most KS, Brain CW. The Utility of annual reports: an international study. J Int Bus Stud 1983:p.63–p.84 spring/summer.
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. The extortion economy: how insurance companies are fueling a rise in Ransomware attacks. Pro Publica; 2019 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, Schnell W. What do we know about cyber risk and cyber risk insurance? J Risk Finance 2016;17(5):474–91. doi:10.1108/JRF-09-2016-0122.
de Fuentes JM, et al. PRACIS: privacy-preserving and aggregatable cybersecurity information sharing. Comput Secur 2017;69:127–41 Elsevier Ltd. doi:10.1016/j.cose.2016.12.011.
Haller I, et al. Dowser: a guided fuzzer for finding buffer overflow vulnerabilities. Login: Mag USENIX SAGE 2013;38(6):16–19.
Hijink JBS. Publicatieverplichtingen voor beursvennootschappen. Dutch: Wolters Kluwer; 2010 dissertation University of Amsterdam2010 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 D.P.A. (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, Bednar P. 'The perception of the benefits and drawbacks of internet usage by the elderly people. Lect Notes Inf Syst Org 2018;23:199–212. 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 JP, Majuca RP. University of Illinois college of law the economic case for cyberinsurance. IL: University of Illinois; 2004 Working paper.
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. The economics of cybersecurity: principles and policy options. Int J Crit Infrastruct Protect 2010;3(3–4):103–17 Elsevier B.V.. doi:10.1016/j.ijcip.2010.10.002.
Mukhopadhyay A, et al. Cyber-risk decision models: to insure IT or not? Decis Supp Syst 2013;56(1):11–26 Elsevier B.V.. doi:10.1016/j.dss.2013.04.004.
Mulligan DK. Security breach notification laws : views from chief security officers, Samuelson law, technology & public policy clinic. Univ. of California, Berkeley School of Law; 2007. p. 1–52. (December)Available at. https://www.law.berkeley.edu/files/cso_study.pdf .
National Cyber Security Center (2018a) '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 (2018b) '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 BFH, Faure M. An analysis of the effectiveness of the EU data breach notification obligation. Comput Law Secur Rev 2018;34(6):1232–46 Elsevier Ltd. doi:10.1016/j.clsr.2018.05.026.
Olcott J. 4 Cybersecurity factors every board member must consider for 2019 planning. BitSight; 2018 Available at https://www.bitsight.com/blog/4-cybersecurity-factors-board-members-2019-planning (Accessed: 20 February 2020).
Pfleeger C. Data security. In: Ralston A, Reilly Ed, Hemmendinger D, editors. Encyclopedia of computer science. Wiley; 2003.
Shabana KM, Buchholtz AK, Caroll AB. The institutionalization of corporate social responsibility reporting. Bus Soc 2017;56(8):1107–35 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 SJ. Kelley School of Business, Indiana University; 2012. p. 349–56 Business Horizons.
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).