European Journal of Risk Regulation (2022), **13**, 443–463
doi:10.1017/err.2022.10

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

A Corporate Governance Approach to Cybersecurity Risk Disclosure

Elif Kiesow Cortez[1]* and Martijn Dekker[2]

[1]Senior Lecturer, The Hague University of Applied Sciences, The Hague, The Netherlands and [2]Visiting Professor, University of Amsterdam, Amsterdam, The Netherlands
*Corresponding author. E-mail: elifkiesowcortez@gmail.com

Abstract

This article sheds light on cybersecurity risk disclosure practices, offering explanations based on the corporate governance literature. We argue that cybersecurity risk management poses particular challenges for corporations due to amplified agency problems. Cybersecurity risks are increasing in number and growing in complexity for companies worldwide. The financial sector in the Benelux region was already digitalising rapidly when, in 2020, enhanced remote-working requirements due to the COVID-19 pandemic further contributed to risk exposure. Substantiating our theoretical discussion, we present and discuss insights as to the most pressing cybersecurity risk management issues in the financial sector based on evidence from semi-structured interviews with Chief Information Security Officers/Chief Security Officers from financial sector leads in the Benelux region. We discuss contemporary factors that might induce management to dedicate more attention to cybersecurity. This apparent shift in companies' approaches regarding cybersecurity is likely to encounter obstacles and should not be expected to be an even and linear process, given the challenges of processing and communicating information in an environment featuring high uncertainty and technical complexity as well as potentially misaligned incentives.

Keywords: Chief Information Security Officer; corporate governance; cybersecurity risk disclosure; information asymmetry

I. Introduction

Cybersecurity compliance risks are increasing in number and growing in complexity for business organisations worldwide. Indeed, institutional investors representing US$35 trillion in assets ranked data privacy and cybersecurity third amongst threats to portfolio companies' strategic success in the next three to five years in a recent survey.[1] Shareholder class actions connected to privacy law infringements have become more prevalent in recent years, which may indicate that information asymmetries exist between shareholders and the management of corporations regarding the assessment of cybersecurity compliance risks. Meanwhile, enhanced remote-working requirements due to the COVID-19 pandemic have contributed to companies' exposure to risk. This article provides an overview of the available literature and professional reports on this issue in light of the legal requirements of cybersecurity risk disclosure in the European Union (EU) and

[1] SW Klemash, JC Smith and C Seets, "What Companies Are Disclosing about Cybersecurity Risk and Oversight" (*Harvard Law School Forum on Corporate Governance*, 2020) <https://corpgov.law.harvard.edu/2020/08/25/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight/> (last accessed 3 January 2022).

the USA. We will utilise economic analysis in order to explain why companies are likely to underinvest in cybersecurity practices, given the risk environment.

Large corporations with dispersed ownership models often rely on the existence of sufficient incentives to exercise appropriate control over managerial actions, also taking into account the disciplining function played by capital markets.[2] However, agency problems can be pervasive and augment the challenge of overseeing managers, especially in complex domains such as cybersecurity risk management. Distinctive mechanisms have evolved in different jurisdictions for ameliorating agency problems that arise due to the separation of ownership and control and the related information asymmetries between management and shareholders.[3] In addition, the degree to which managers are afforded latitude to decide matters can differ between the USA and certain civil law countries in Europe. Irrespective of differences across capitalist economies with regard to financial market peculiarities and organisational firm characteristics, underinvestment in cybersecurity risk management may be posing problems for corporations everywhere, and the evidence suggests that shareholders are taking notice of their failures in this regard.

The present article aims at providing insights into cybersecurity risk management practices and at delineating how these can be explained from the vantage point of corporate governance theories. Cybersecurity risks are increasing in number and growing in complexity for business organisations worldwide and mandatory data protection risk-reporting requirements opened up possibilities for stakeholders to sue companies after major data breaches. The financial sector in the Benelux region was already digitalising rapidly when, in 2020, enhanced remote-working requirements due to the COVID-19 pandemic further contributed to the new cybersecurity risk exposure in the financial sector. This article presents insights as to the most pressing cybersecurity risk management issues in the financial sector based on evidence from semi-structured interviews conducted in October 2021 with eleven Chief Information Security Officers (CISOs)/ Chief Security Officers (CSOs) from financial sector leads in the Benelux region.

The article first lays out how the corporate governance approach relates to cybersecurity risk (Section II) and continues to discuss the proposition that cybersecurity risk management poses particular challenges for corporations due to amplified agency problems (Sections II and III). One of the arguments here is that if it is difficult to accurately gauge the effectiveness of management's cybersecurity efforts, then management can more easily deflect responsibility in case of breaches, whereas concomitantly the ability of stakeholders to monitor management performance suffers. Next, the article discusses cybersecurity risk reporting in the US and European contexts, which helps to briefly elucidate the regulatory context of the major markets in which companies operate and clarifies the respective legal requirements (Section IV). After having briefly stated the regulatory demands, it is useful to consider another aspect that might be of relevance to companies' decisions to invest in cybersecurity, namely the costs that security breaches might cause. Thus, an accounting of the possible economic fallout for companies in the event of non-compliance with data protection laws is provided (Section V). Lastly, the most pressing cybersecurity risk management issues in the financial sector are presented, based on insights collected through semi-structured interviews conducted with CISOs from major companies in Benelux region (Section VI). The interviews also aimed at obtaining insights from these company insiders at an extraordinary moment where adjustments had to be made by companies due to the COVID-19 pandemic, which then created new cybersecurity

[2] EF Fama, "Efficient Capital Markets: A Review of Theory and Empirical Work" (1970) 25(2) Journal of Finance 383.

[3] JC Coffee, "The Rise of Dispersed Ownership: The Roles of Law and the State in the Separation of Ownership and Control" (2001) 111(1) Yale Law Journal 1.

vulnerabilities. In the conclusion (Section VII), the main factors behind a potential shift in companies' approaches towards cybersecurity risk disclosure are briefly discussed.

II. Information asymmetry: shareholders versus management

Jensen and Meckling succinctly described the corporation as an entity representing "a nexus of contracting relationships".[4] They defined corporate governance essentially as a problem involving the manager of a corporation and multiple potential principals: the shareholders, creditors, employees and other parties with whom the manager transacts on behalf of the firm. Corporate governance rules emerge out of contracting efforts between the different principals or constituencies and the management of the corporation. With the increased information technology (IT) intensity of companies and the increased cyber threat, proper management of cybersecurity risk has become of significant interest to all corporate stakeholders. Boards and external auditors function as intermediaries or represent some of the constituencies with whom the manager transacts, and hence cybersecurity has increasingly become part of the conversation with these actors.[5]

In the same article, Jensen and Meckling provided the foundations of principal–agent theory as applied to the firm, which is concerned with the implications of asymmetric information between parties regarding a contract (eg a contract between the principal and an agent). In line with this, the challenge facing corporate governance can also be described as a "common agency problem" that involves one agent – the manager – interacting with multiple potential principals, including shareholders and employees.[6] In the case of cybersecurity, the relationship between management and shareholders has posed distinctive challenges. As cybersecurity risks can have a significant impact on the value of the company for stakeholders, cybersecurity professionals are pressed to find ways to effectively communicate with these – often non-technical – stakeholders.

An important issue in corporate governance is estimating the likely outcomes of the contracting efforts between agent and principal and how, in practice, corporate governance can deviate from a theoretically formulated efficient contracting benchmark. This article aims at offering an initial discussion of how the realm of compliance with cybersecurity requirements can pose new challenges for corporations, which can interfere with the nature of some of the corporations' agency relationships.

The information asymmetry that characterises the principal–agent relationship between shareholders and management can generate moral hazard, encouraging excessive risk-taking by shielding the risk taker from the full consequences of the action. Moral hazard can stem from hidden information or hidden action.[7] Hidden information occurs when the principal does not have the expertise to properly assess the agent's actions. Hidden action occurs when the principal cannot even observe the agent's actions. In both cases, asymmetric information gives the agent room to act in ways that are not in line with the principal's expectations and in ways that may undermine the principal's interests. Thus, when, for example, a bad outcome materialises (eg the firm is caught mishandling personal data), the principal (the shareholders) cannot refute a claim by the agent (the management of the firm) that it happened due to a random exogenous shock and

[4] MJ Jensen and WH Meckling, "Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure" (1976) 3(4) Journal of Financial Economics 305.

[5] M Becht, P Bolton and A Röell, "Corporate Law and Governance" in AM Polinsky and S Shavell (eds.), *Handbook of Law and Economics – Volume 2* (Amsterdam, Elsevier 2007).

[6] BD Bernheim and MD Whinston, "Common Agency" (1986) 54(4) Econometrica 923.

[7] BE Hermalin and MS Weisbach, "The Study of Corporate Governance" in BE Hermalin and MS Weisbach (eds.), *Handbook of the Economics of Corporate Governance – Volume 1* (Amsterdam, Elsevier 2017).

not because of faulty behaviour by the agent. Both types of moral hazard problems (hidden information and hidden action) may apply to a significant degree with regard to corporations' cybersecurity practices.

The literature on the economics of agency emphasises how the extent and the ease with which the agent can conceal actions becomes very important for the agency relationship and the possibilities of employing contractual solutions. In this vein, Hermalin observes:

> Although it is hard to dispute that a key driver of corporate governance problems is asymmetric information, knowing what is asymmetrically known and by whom is critical. Does the agent possess payoff relevant information unknown to the principal? Does he take an action that the principal cannot observe? Or perhaps he takes an action that the principal can observe, but which is difficult for her to verify. . . . [T]he nature of the contractual solution can vary tremendously depending on these issues . . .[8]

Managers can have many opportunities to conceal data-handling practices from external oversight. Cybersecurity may be particularly open to such obfuscation, as it may involve IT solutions that are difficult for non-experts to understand. One consequence of this exacerbated agency problem can be managers underinvesting in compliance with data protection regulations or other cybersecurity requirements.[9]

Park argues that the threat stemming from data breach litigation could in principle attenuate the agency problem and the related misaligned incentives to invest in robust security measures. However, for such a litigation threat to have the desired effect of inducing managers to shore up precautionary investment, it has to happen in a context where the plaintiff has a reasonable chance of winning. Park argues that in the US context, California courts' reluctance to grant Article III standing impaired this type of solution based on a mechanism of private enforcement.[10] Similarly, Chatterjee and Sokol point out that firms spend much less on data breach-related compliance than on other traditional areas of compliance such as anti-bribery and audit fraud.[11] Our interview findings also show that, in recent years, CISOs/CSOs are more frequently invited to report their risk assessments directly to the board. Furthermore, in light of the acceleration of such trends due to COVID-19 measures, CISOs/CSOs are more frequently invited to add statements to companies' annual reports directed at external stakeholders.

Anderson and Moore point out another relationship that is fraught with information asymmetries: namely, the one between management and software providers.[12] When buying software, firms cannot verify the claims that software vendors make about the security of their products and thus firms have no reason to trust those claims. Buying firms lacking the information needed to assess software have no reason to pay more for protection, and consequently vendors are disinclined to invest in it.[13] Thus, only lower-quality

[8] BE Hermalin, "Aspects of the Economics of Organization with Application to Corporate Governance" in BE Hermalin and MS Weisbach (eds.), *Handbook of the Economics of Corporate Governance – Volume 1* (Amsterdam, Elsevier 2017), p 76f.

[9] S Park, "Why Information Security Law Has Been Ineffective in Addressing Security Vulnerabilities: Evidence from California Data Breach Notifications and Relevant Court and Government Records" (2019) 58 International Review of Law and Economics 132.

[10] ibid.

[11] C Chatterjee and DD Sokol, "Data Security, Data Breaches, and Compliance" in B van Rooij and DD Sokol (eds.), *Cambridge Handbook on Compliance* (Cambridge, Cambridge University Press 2021).

[12] RJ Anderson and T Moore, "The Economics of Information Security" (2006) 314 Science 610.

[13] ibid.

software remains available for sale.[14] This also leads to suboptimal preparedness against data breach risk, which is also pointed out in a recent report released in 2021 for the Dutch Safety Board ("Onderzoeksraad voor Veiligheid").[15]

In terms of the regulatory response to the issue of corporate agency problems due to information asymmetry and the effect on companies' privacy policies, there are indications that regulators in the EU and the USA differ in how they perceive the severity of the problem and which solutions they deem most appropriate. Indeed, the California Consumer Privacy Act (CCPA) provides for a lighter and less demanding regulatory approach than the General Data Protection Regulation (GDPR) at the intra-firm operational and institutional level. For example, GDPR requires that larger firms put in place a Data Protection Officer, who acts independently and conducts data protection impact assessments (DPIAs).[16] This suggests that regulators doubt that firms will reorganise internally to accommodate cybersecurity risk challenges without such intervening measures.

III. Organisational vulnerabilities and cybersecurity risks

The first two subsections below will consider corporations' vulnerabilities to data breach incidents, review ways to assess the magnitude of the risks and discuss corporations' underinvestment in cybersecurity despite evidence of exposure. Additionally, evidence as to the risk of attack according to firm type in the USA will be reviewed and the underlying theoretical underpinnings discussed.

1. Corporations' cybersecurity vulnerabilities and data breach

Organizations are vulnerable to data breaches due to human-induced errors and misperception of risks, in addition to vulnerabilities stemming from the technical setup of their systems.[17] Addressing these vulnerabilities effectively is difficult and requires sustained commitment from management. However, this commitment might be insufficient, as described in Section II. Phishing and ransomware are two common forms of cybercrime that can lead to these breaches.

Phishing is a cybercrime in which multiple users receive bulk e-mails designed to steal data that appear to be from a legitimate source (such as a bank or a commercial firm).[18] Personal data collected in this manner is used for criminal offences such as identity theft or for duplicating credit cards. Similar schemes directed at companies can allow cybercriminals access to their data, such as trade secrets or intellectual property, when an employee clicks on a phishing link.[19] One cybersecurity approach focuses solely on raising awareness among insiders in the belief that training everyone with access to a company's systems not to click on phishing links provides adequate protection from attacks.[20]

Ransomware is malware that encrypts the data in the victim's computer. Cybercriminals then ransom the data by offering the decryption key for cash or, more commonly, bitcoin. In 2017, the WannaCry ransomware affected many users globally,

[14] GA Akerlof, "The Market for Lemons: Quality Uncertainty and the Market Mechanism" (1970) 84(3) Quarterly Journal of Economics 488.

[15] Dutch Safety Board (2021) Kwetsbaar door software <https://www.onderzoeksraad.nl/nl/page/17171/kwetsbaar-door-software—lessen-naar-aanleiding-van> (last accessed 3 January 2022).

[16] See Recital 97 of GDPR: "Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner".

[17] See E Kiesow Cortez, "Cybersecurity Risk for Companies" (2018) 4 Strafblad 12.

[18] G Kostopoulos, *Cyberspace and Cybersecurity*, 2nd edn (London, Taylor & Francis 2017).

[19] SANS Institute, *2017 Threat Landscape Survey: Users on the Front Line* (White Paper, 2017) <https://www.qualys.com/forms/whitepapers/sans-2017-threat-landscape-survey-users-front-line/> (last accessed 3 January 2022).

[20] SL Garfinkel, "The Cybersecurity Risk" (2012) 55(6) Communications of the ACM 29–32.

bringing the attention of the general public to this significant cybersecurity risk.[21] The World Economic Forum's 2018 Global Risks report notes that the NotPetya ransomware attack caused estimated harm to businesses of up to $300 million worldwide.[22] Petya and NotPetya attacks affected many global firms such as Maersk, Merck and DLA Piper, among many others.[23]

The exploitation of judgment errors by customers and employees provides a strong indication that calculations of cybersecurity risk should include the human factor. A study based on data collected from 10,316 cybercrime victims shows that neither personal background nor financial status predicted susceptibility to phishing attacks.[24] Indeed, research has yet to identify what factors make individuals more likely to fall for cyber traps. Bruijn and Janssen discuss the reasons for this as well as some reasons why companies do not invest in cybersecurity, such as limited visibility, the ambiguous impact of attacks and victims' propensity to hide that they experienced an attack.[25]

Companies that have a dominant market position are behaving as if they are not afraid to lose their customers in response to an attack.[26] The Cisco Annual Cybersecurity Report sheds light on this: while 49% of participating organisations reported that they experienced public scrutiny after a data breach became public, most organisations ignore 44% of the security alerts they receive.[27] As Cisco's CSO notes in the report, paying attention to such alerts could readily bear fruit in blocking cybercrime.[28]

A recent Cybersecurity Cultures in Organizations report by the European Union Agency for Cybersecurity (ENISA) reveals the economic costs of cyberattacks and breaches.[29] These include direct costs such as loss of intellectual property and indirect costs such as loss of reputation (and market share due to reputation loss).[30] Citing several professional sources,[31] the report documents that occurrence of phishing and ransomware attacks is increasing in frequency and that the average ransom demanded from firms is increasing.[32]

[21] D Palmer, "Ransomware: Not Dead, Just Getting a Lot Sneakier" (*ZDNet*, 2018) <https://www.zdnet.com/article/ransomware-not-dead-just-getting-a-lot-sneakier/> (last accessed 3 January 2022).

[22] World Economic Forum (2018) *The Global Risks Landscape 2018* <http://reports.weforum.org/global-risks-2018/global-risks-landscape-2018/#landscape> (last accessed 3 January 2022).

[23] A Hern, "WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017" (*The Guardian*, 2017) <https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware> (last accessed 3 January 2022).

[24] ER Leukfeldt, "Phishing for Suitable Targets in the Netherlands: Routine Activity Theory and Phishing Victimization" (2014) 17(8) Cyberpsychology, Behavior, and Social Networking 551.

[25] H de Bruijn and M Janssen, "Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies" (2017) 34(1) Government Information Quarterly 1.

[26] On the "public good" approach to cybersecurity and its potential consequence being underinvestment in cybersecurity by companies, see CJ Coyne and PT Leeson, "Who's to Protect Cyberspace?" (2005) 1(2) Journal of Law, Economics & Policy 473. For more on economics of cybersecurity and a "cybersecurity as a public good" approach, see DK Mulligan and FB Schneider, "Doctrine for Cybersecurity" (2011) 140(4) Daedalus 70; T Moore and RJ Anderson, "Internet Security" in M Peitz and J Waldfogel (eds.), *The Oxford Handbook of the Digital Economy* (Oxford, Oxford University Press 2012). On the analysis of regulatory strategies, see B van den Berg, "Coping with Information Underload" in M Hildebrandt and B van den Berg (eds.), *Information, Freedom and Property* (London, Routledge 2016).

[27] *Cisco Annual Cyber Security Report 2017* <https://www.cisco.com/c/dam/en/us/solutions/collateral/security/annual-reports/acr-infographic-2017.pdf> (last accessed 3 January 2022).

[28] ibid.

[29] *ENISA Cybersecurity Cultures in Organisations 2018* <https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations> (last accessed 3 January 2022).

[30] ibid.

[31] *IBM X-Force Threat Intelligence Index 2017* <https://www.ibm.com/security/data-breach/threat-intelligence> (last accessed 3 January 2022).

[32] *ENISA Cybersecurity Cultures in Organisations 2018* <https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations> (last accessed 3 January 2022).

The report also emphasises that the pervasiveness of global value chains is exposing an increasing number of firms to cybersecurity vulnerabilities.[33] Similarly, ENISA's threat landscape report for 2020 shows that phishing, ransomware, insider threat, identity theft and information leakage were on the rise.[34] The report admonishes organisations to update their cyber threat intelligence schemes with more training via cyber-ranges (virtual environments that make use of real network equipment and are frequently used for cybersecurity preparedness training) and calls for cybersecurity research and development to focus their research initiatives on high-risk points of vulnerability.[35]

2. *Quantification of cybersecurity risk and underinvestment in cybersecurity*

Ralston et al focus on analysing cybersecurity threats and risks for supervisory control and data acquisition and distributed control systems.[36] Their paper states that protecting critical US infrastructure from cyberattack and assessing the risk of such attacks have become priority concerns for the Department of Homeland Security.[37] Once considered isolated systems not subject to the network threats companies faced, supervisory control and data acquisition systems have become increasingly vulnerable due to greater connectivity and other technological developments.[38] The departments' assessments would be more accurate if companies were willing to provide data on the attacks they have suffered and their consequences, but companies fear damage to their reputation[39] and that they might reveal the vulnerabilities of their systems to additional attackers.[40]

Companies could also benefit from greater information on the probability and frequency of cyberattacks, as this could help them better prioritise their investments in cybersecurity through better risk calculations.[41] In their paper, Kaplan and Garrick differentiate "absolute risk" (a clear risk for people with full information) from "perceived risk" (an incorrectly assessed risk due to lack of information).[42] They explain that multiplying the probability of an event by its consequences provides insufficient information because it groups high-probability attacks with low harm and low-probability attacks with high harm.[43] They propose that companies should approach risk more holistically, including all possible (probable) attacks.[44] Relatedly, it became apparent from the semi-structured interviews conducted for this article that the security professionals themselves

[33] ibid.

[34] *ENISA Threat Landscape Report 2020* <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends> (last accessed 3 January 2022).

[35] ibid.

[36] PA Ralston, JH Graham and JL Hieb, "Cyber Security Risk Assessment for SCADA and DCS Networks" (2007) 46(4) ISA transactions 583.

[37] ibid.

[38] ibid.

[39] On how investors react to information security breaches of companies, see LA Gordon, MP Loeb and L Zhou, "The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?" (2011) 19(1) Journal of Computer Security 33.

[40] On the risk of creating a roadmap for future cybercriminals by disclosing vulnerabilities, see MF Ferraro, "Groundbreaking or Broken; An Analysis of SEC Cybersecurity Disclosure Guidance, Its Effectiveness, and Implications" (2013) 77 Albany Law Review 297.

[41] S Kaplan and BJ Garrick, "On the Quantitative Definition of Risk" (1981) 1(1) Risk Analysis 11.

[42] ibid, p 12. The authors do not include the definition of the absolute risk and perceived risk, but they differentiate by referring to a hypothetical scenario. In this scenario, they imagine a person puts a rattlesnake in another person's mailbox. They explain that if the mailbox owner were asked whether he would be taking a risk if he put his hand into his mailbox, he would say "no". However, this response would only reflect the perceived risk, as the mailbox owner lacks information regarding the placement of the snake, not the absolute risk.

[43] ibid.

[44] ibid.

possess imperfect information about how to appropriately determine the probability of breaches. This would suggest that when analysing cybersecurity through a corporate governance lens one should take into account that inherent uncertainty might pervade cyber risk calculations.

Further research by Kasperson et al has analysed perceived risk from a cognitive perspective, reporting that who informs the public about the risk and what kind of signal the public receives (ie whether the information is coming from a high-quality source) can affect the public's perception of risk.[45] Kasperson et al also provide a model explaining the misperception of risk among the general public, which can also be used to shed light on how stakeholders of companies might misperceive the risk of cyberattacks.[46] The model delineates four channels that contribute to individuals' misconception of risk: (1) *heuristics and values* – individuals use simplifying mechanisms to handle complexity, which then can introduce biases when deciphering information; (2) *social group relationships* – the interests of a social group affects risk perception and group alignment hampers updating based on new information; (3) *signal value* – new, uncommon accidents, even if they are of smaller magnitude, connote lack of control and therefore trigger stronger reactions and amplify perceived risk; and (4) *stigmatisation* – individuals avoid environments associated with risk to prevent potential stigma.[47]

Companies may be the victim of cyberattacks without even knowing it, as phishing attacks only come to light if the attacker chooses to inform the company of their illegitimate access to companies' systems. Therefore, perceived risk may be far lower than absolute risk in this area. Similarly, the economic impact of cybersecurity breaches is not easy to calculate, which can also increase the underestimation of the consequences of a cyberattack.[48]

In cybersecurity research, cyber threats are typically analysed together with attack vectors. Attack vectors are defined in the ENISA report as "a means by which a threat agent can abuse weaknesses or vulnerabilities on assets (including human) to achieve a specific outcome".[49] The report categorises attack vectors as follows: attacking the human element; web- and browser-based attacks; Internet-exposed attacks; exploitation of vulnerabilities; and supply-chain attacks. The first includes tactics such as phishing, customer support scams and social media information gathering. Web- and browser-based attacks include malvertising, SQL injection and drive-by downloads. In Internet-exposed attacks, Internet-exposed services are used to deliver malware or perform ransom attacks. A recent exploitation of such vulnerabilities was the WannaCry attack, which used previously leaked National Security Agency information to exploit a Microsoft Windows Server Message Block (SMB) vulnerability. In addition, the NotPetya malware is an example of a supply-chain attack. It exploited a compromise of the systems of the legitimate accounting software *M.E.Doc* to attack users of the software.[50]

Confronted with cyber threats, companies are likely to underinvest in security measures. Given their basic profit motive, companies try to avoid paying for things that they

[45] RE Kasperson, O Renn, P Slovic, HS Brown, J Emel, R Goble, JX Kasperson and S Ratick, "The Social Amplification of Risk: A Conceptual Framework" (1988) 8(2) Risk Analysis 177.

[46] For a recent study analysing whether the news media amplifies the data protection risk, see T Reijmer and M Spruit, "Cybersecurity in the News: A Grounded Theory Approach to Better Understand Its Emerging Prominence" (2014) Technical Report Series (UU-CS-2014-006).

[47] ibid, pp 185–86.

[48] Regarding suggestions about cybersecurity awareness investments, see H de Bruijn and M Janssen, "Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies" (2017) 34(1) Government Information Quarterly 1.

[49] *ENISA Threat Landscape Report 2020* <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends> (last accessed 3 January 2022).

[50] *ENISA Threat Landscape Report 2017*, pp 100–04.

consider non-essential, such as investment in cybersecurity. If many companies behave in this manner, this only increases the perception that cyberattacks are rare. Indeed, research indicates that group decisions and group behaviour can lead to flawed risk assessment.[51]

The semi-structured interviews conducted with eleven CISOs/CSOs in the Benelux region for this article reveal that companies' approaches might be changing, at least at the margins. The acceleration of digitalisation due to COVID-19 and the increased awareness amongst corporate stakeholders that cybersecurity is a key enabler (and disabler) of business continuity and resilience are drawing more attention to the issue of cybersecurity. However, the level of engagement between cybersecurity professionals and company stakeholders remains suboptimal and communication challenges are still being overcome.

Kamiya et al provide information as to what types of firms are likely to experience data breach attacks based on a Privacy Rights Clearinghouse study of such attacks on US firms from 2005 to 2017.[52] Their findings indicate that 30% of attacks occurred in the service industry, 27% in the financial sector, 18% in manufacturing industries and 15% in wholesale and retail trade. From a theoretical point of view, it is not clear what types of firms hackers are likely to target. Hackers are expected to attack firms where benefits surpass costs. On the one hand, more visible, larger firms might provide more personal customer data that can be misused and exploited for greater gain. On the other hand, smaller firms might be more vulnerable because their IT security systems are likely to be less sophisticated. Kamiya et al's empirical model shows that larger firms are more likely to suffer attacks. In addition to sheer size, visibility increases risk, including being part of the Fortune 500 list, being financially less constrained, being more highly valued and possessing more intangible assets.

3. Boards' reported cybersecurity preparedness

Cheng and Groysberg and Cheng et al discuss the results of surveys that they conducted that also covered the issue of cybersecurity awareness and preparedness among boards of corporations.[53] One of the reported findings is that one source of cybersecurity vulnerabilities for corporations is that boards do not have appropriate processes in place or sufficient (access to) expertise to identify, assess and handle cyber threats.

Regarding the question of whether firms have established processes to promote cybersecurity, only 24% of directors indicated that their processes for the cybersecurity domain are "above average" or "excellent". Of all domains, they deemed cybersecurity to be the one equipped with the least effective processes. Cybersecurity processes are established activities such as regular discussions about cyber risks (with or without the presence of cybersecurity specialists) and management reviews of contingency plans for the event of a data breach. The second factor leading to boards' poor handling of cybersecurity is

[51] Kasperson et al, supra, note 45.

[52] S Kamiya, J-K Kang, J Kim, A Milidonis and RM Stulz, "What Is the Impact of Successful Cyberattacks on Target Firms?" NBER Working Paper No. 24409. Kamiya et al also found that firms that facing less competition in their respective market segment are more likely to experience an attack. They measure market competitiveness using the Herfindahl index as a measurement of the "uniqueness" of the firm's product, assessed using the ratio of selling expense to sales. This might suggest that firms that do not fear losing market share to a competitor after an attack becomes public might be investing less in securing their IT systems against attacks. They may assume that losses in revenue due to a publicised cyberattack would not merit such investment.

[53] JY-J Cheng and B Groysberg, "Why Boards Aren't Dealing with Cyberthreats" (*Harvard Business Review*, 2017) <https://hbr.org/2017/02/why-boards-arent-dealing-with-cyberthreats> (last accessed 3 January 2022); JY-J Cheng, B Groysberg, PM Healy and R Vijayaraghavan, "Directors' Perceptions of Board Effectiveness and Internal Operations" (2021) 67(10) Management Science 6399.

insufficient expertise according to the survey findings of Cheng and Groysberg. Directors reported that risk and security are the issues that they find most challenging in their role as board directors. They also reported not having the necessary expertise to handle these issues.

Kamiya et al tested whether firms that have what they call a "risk committee" on their boards effectively lower their risk. According to BoardEx, firms may term these committees in a variety of ways, such as the "Risk Management Committee", the "Audit and Risk Committee" or the "Enterprise Risk Management Committee". Controlling for the total number of board committees a firm possesses, Kamiya et al's regression results show that risk committees lower the risk of a cyberattack. This may suggest that such committees have both a direct impact and an indirect one. Having an organisation structure that is attentive to risk may increase firm awareness of cybersecurity risk, leading to the implementation of effective cybersecurity measures.[54]

For example, even if a few firms reported that their cybersecurity risk management is effective, Cheng et al report several ways in which some firms improved oversight effectiveness in the cybersecurity domain:

> One risk committee chair explained that his committee had created a separate board of advisors, comprising experts in cyber risk, who worked with management and the risk committee to provide advice on the area. Others noted that their boards had appointed a new member with experience in cybersecurity to supplement the board's risk management capabilities. Still others explained that the audit/risk committee had engaged consultants to work with the committee and management to help inform the board and ensure that appropriate actions were being taken to protect against cyberattacks.[55]

These differences between firms in the level of precautionary engagement to improve cybersecurity suggest that, instead of alleged practical hurdles imposing insurmountable constraints, underinvestment in cybersecurity risk management reflects choices by the responsible actors within corporations, some of whom have postponed dealing with the issue despite mounting evidence of need. Information asymmetry is certainly a major cause of this widespread inaction: if it is not known *ex ante* what precise measures are actually effective at increasing cybersecurity or whether such measures are difficult to observe, especially for actors on the outside such as shareholders, then the board might have little incentive to be proactive.

Our findings from the semi-structured interviews conducted with eleven CISOs/CSOs in the Benelux region for this article reveal that, in the financial industry, the companies' lead cybersecurity specialists are increasingly given a seat at the table at the board level, which is in line with the fact that cybersecurity risk disclosure are being included in the statements to companies' annual reports directed at external stakeholders.

IV. Cybersecurity and privacy risk reporting

Regulation 2016/679, GDPR, introduced the concept of the DPIA as an essential tool to ensure data controllers demonstrate compliance. The CCPA does not directly reference a risk-based approach or an impact assessment. However, the US National Institute of Standards and Technology (NIST) Privacy Framework includes references to cybersecurity risk. A recent NIST report introduces a privacy risk model that is designed to provide

[54] Kamiya et al, supra, note 52.
[55] Cheng et al, supra, note 53, 6404.

coherent privacy risk assessment evaluating the likelihood of problematic scenarios regarding the processing of personally identifiable information to be included as a cybersecurity risk.[56] Thus, data protection and privacy risk assessment requirements applicable to compliance apply to the US and EU contexts. Company reporting practices increasingly reflect a recognition of data protection and privacy risk. A 2020 study shows that 89% of Fortune 100 companies disclosed that the oversight section of their proxy statement included a focus on cybersecurity risk and 99% of the companies listed data privacy in their risk factor disclosures.[57]

Less visible and smaller-magnitude data breaches that do not attract a lot of public attention might not lead to shareholders starting class action litigation.[58] However, high-visibility data breaches have led to many instances of such shareholder class action suits being put forward. Companies targeted by such suits occasionally succeeded at navigating and reacting to the challenge by responding with motions to dismiss and through settlement. But as the stakes are getting higher in the case of large-scale data breaches, lawyers hired by the shareholders are improving their strategies and refining their pleadings to overcome the deficiencies of their earlier legal strategies. Given recent cases, corporations are becoming increasingly aware of the possibility of being targeted with shareholder class action suits after data breaches. It remains to be seen moving forward whether the threat of such litigation affects corporations' level of commitment to robust cybersecurity risk management practices.

1. Cybersecurity and privacy risk reporting for corporations in the USA: Securities and Exchange Commission rules

The Division of Corporate Finance of the US Securities and Exchange Commission (SEC) first published a cybersecurity disclosure guidance on 13 October 2011, and the latest version of the guidance is applicable starting 26 February 2018.[59] The guidance highlights that cybersecurity is essential given that "the investing public and the U.S. economy depend on the security and reliability of information and communications technology, systems, and networks".[60] It also prohibits company insiders who have access to information regarding a cybersecurity incident from trading the companies' securities before this information becomes public.[61] It requires companies to disclose the material data protection risks that they face in a timely and periodic manner, clarifying that such risks occur when a reasonable investor would consider the information relevant for making an investment decision and include the possibility of harm (due to that incident) on the company's reputation, financial performance and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions.[62]

In the 2011 version of the guidance, the SEC emphasised that companies should "avoid generic 'boilerplate' disclosure", but also that the companies should not compromise their

[56] *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management* (2020) <https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf> (last accessed 3 January 2022).

[57] Klemash et al, supra, note 1.

[58] M Hooker and J Pill, "You've Been Hacked, and Now You're being Sued: The Developing World of Cybersecurity Litigation" (2016) 90 Florida Bar Journal 30.

[59] Securities and Exchange Commission, 17 CFR Parts 229 and 249, [Release Nos. 33-10459; 34-82746] Commission Statement and Guidance on Public Company Cybersecurity Disclosures <https://www.sec.gov/rules/interp/2018/33-10459.pdf> (last accessed 3 January 2022).

[60] ibid.

[61] ibid.

[62] ibid.

cybersecurity through disclosure.[63] Empirical research shows that data protection risk disclosures give investors an indication of companies' cybersecurity awareness and that the market reacts to the level of such awareness.[64] However, research also suggests that the SEC requirement might be incentivising companies to report insignificant risks as well as significant ones and that therefore the requirement might be creating a less reliable information environment.[65] Critics argue that the regulation places an additional procedural burden on companies without effectively mitigating investor risk.[66] They also state that forcing companies to disclose their vulnerabilities places them at a disadvantage vis-à-vis cybercriminals.[67]

In addition to risk-reporting requirements, given recent cases, corporations are becoming increasingly aware of the possibility of being targeted with shareholder class action suits after data breaches. Shareholder class actions in the privacy domain are an example of the emerging pervasiveness of so-called event-driven securities litigation, in which investors sue when a corporation's share price falls in response to a corporate shock, such as a product liability crisis, oil spill or, in line with the focus of our article, a data breach.

It can be argued whether the threat of such litigation affects corporations'level of commitment to robust cybersecurity risk management practices. One concern is that these class action suits are plagued by standing problems because the circuit is split on what constitutes injury from a data breach.[68] Certain difficulties arise for shareholders who wish to pursue legal action via securities fraud class action suits in response to sudden declines in stock prices after a data breach gets revealed. These shareholders face the challenge of making the case that their prior actions were taken, to their disadvantage, based on a firm's material misrepresentations as reflected in their public statements and 10-K filings. Furthermore, legal hurdles also exist for derivative shareholder lawsuits wishing to demonstrate that directors and boards breached their fiduciary duties. For instance, the influence of the business judgment rule in Delaware courts should be taken into account, as well as the non-trivial task of successfully pleading demand futility.[69]

A shareholder class action lawsuit was filed against SolarWinds regarding the fall in the price of shares observed after a hack was disclosed in December 2020. Shareholders alleged that they were damaged because SolarWinds failed to rapidly disclose the vulnerabilities that could lead to the exposure of thousands of customers. The plaintiffs argue that SolarWinds, including previous Chief Executive Office Kevin Thompson and Chief Financial Office J. Barton Kalsu, "failed to employ adequate cybersecurity safeguards

[63] Division of Corporation Finance, Securities and Exchange Commission, "CF Disclosure Guidance: Topic No. 2 Cybersecurity" (2011) <https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm> (last accessed 3 January 2022).

[64] H Berkman, J Jona, G Lee and N Soderstrom, "Cybersecurity Awareness and Market Valuations" (2018) 37(6) Journal of Accounting and Public Policy 508.

[65] H Li, WG No and T Wang, "SEC's Cybersecurity Disclosure Guidance and Disclosed Cybersecurity Risk Factors" (2018) 30 International Journal of Accounting Information Systems 40. For example, it would be interesting to pinpoint how far a company needs to go in order to identify all potential data protection risks. A recent study refers to a complex methodology for identifying cyberattacks early using a machine learning methodology with information retrieval techniques for analysing the content of hacker forums as well as Internet relay chat (IRC) channels. See V Benjamin, W Li, T Holt and H Chen, "Exploring Threats and Vulnerabilities in Hacker Web: Forums, IRC and Carding Shops" presented at *Intelligence and Security Informatics (ISI)*, 2015 IEEE International Conference.

[66] MF Ferraro, "Groundbreaking or Broken; An Analysis of SEC Cybersecurity Disclosure Guidance, Its Effectiveness, and Implications" (2013) 77 Albany Law Review 297.

[67] SJ Hughes and RL Trope, "The SEC Staff's Cybersecurity Disclosure Guidance: Will It Help Investors or Cyber-Thieves More" (2011) Business Law Today 1.

[68] M Dowty, "Life Is Short. Go to Court: Establishing Article III Standing in Data Breach Cases" (2017) 90 Southern California Law Review 683

[69] DJ Marcus, "The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information" (2018) 68 Duke Law Journal 555

and did not maintain effective monitoring systems to detect and neutralize security breaches", and that these failures left the company and its customers "particularly susceptible to cyber-attacks".[70]

Another recent instance is a data breach concerning a provider of Internet of Things and networking equipment devices that services across industries and goes under the name of Ubiquiti. Ubiquiti produces and sells wireless data communication equipment as well as wired products for homes and enterprises. A shareholder class action complaint was filed alleging that Ubiquiti made materially false and/or misleading declarations. Shareholders claimed that Ubiquiti's previously made positive statements about the corporation's operations, business and future prospects were materially misleading and/or lacked a reasonable basis.[71]

2. *Cybersecurity and privacy risk reporting for corporations in the EU*

The EU GDPR[72] attempts to avoid the investment risk emphasised by the SEC as it requires companies to have their data protection risk factors assessed through DPIAs, therefore obliging firms to complete an internal risk assessment document that usually is audited by experts to test their compliance with the regulation.[73] EU Market Abuse Regulation also requires companies to disclose any insider information if the information would have a significant effect on the share price of the company, and some cybersecurity incidents might fall within this definition.[74]

The European Commission proposed the draft regulation on the Digital Operational Resilience Act (DORA) for financial services on 24 September 2020.[75] In the proposal, it is declared that, based on Article 114 of the Treaty on the Functioning of the European Union, DORA aims to improve "the establishment and functioning of the internal market for financial services by harmonising the rules applicable in the area of ICT [information and communications technology] risk management, reporting, testing and ICT third-party risk".[76] The new expectations under DORA also aim at lowering information asymmetries regarding cybersecurity risk in the financial sector, as the proposed act envisions that the management body should have an active role in cybersecurity risk management, including an implementation of a full range of approval and control processes and appropriate allocation of ICT investment and training. As per Article 4.2.g of DORA, the management body

[70] Scmagazine, "SolarWinds lawsuits merge as stockholders begin documenting financial losses" (2021) <https://www.scmagazine.com/news/breach/solarwinds-lawsuits-merge-as-stockholders-begin-documenting-financial-losses> (last accessed 3 January 2022).

[71] M Clark, "Ubiquiti Is Accused of Covering Up a 'Catastrophic' Data Breach – And It's Not Denying It" (*The Verge*, 2021) <https://www.theverge.com/2021/3/31/22360409/ubiquiti-networking-data-breach-response-whistleblower-cybersecurity-incident> (last accessed 3 January 2022); and Businesswire, "Ubiquiti Investors: July 19, 2021 Filing Deadline in Class Action" (2021) <https://www.businesswire.com/news/home/20210611005074/en/UBIQUITI-INVESTORS-July-19-2021-Filing-Deadline-in-Class-Action-%E2%80%93-Contact-Lieff-Cabraser> (last accessed 3 January 2022).

[72] 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).

[73] PL Marcogliese and R Mukhi, "Untangling the Tangled Web of Cybersecurity Disclosure Requirements: A Practical Guide" (*Harvard Law School Forum on Corporate Governance*, 2018) <https://corpgov.law.harvard.edu/2018/06/17/untangling-the-tangled-web-of-cybersecurity-disclosure-requirements-a-practical-guide/> (last accessed 3 January 2022).

[74] ibid.

[75] Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014.

[76] ibid.

shall "allocate and periodically review appropriate budget to fulfil the financial entity's digital operational resilience needs in respect of all types of resources, including training on ICT risks and skills for all relevant staff".

Environmental, social and governance (ESG) reporting has also gained international attention, and it is addressed in a comprehensive manner in the proposal of the European Commission on the Corporate Sustainability Reporting Directive (CSRD) on 21 April 2021.[77] CSRD is expected to be added onto the existing reporting requirements of the EU's Non-Financial Reporting Directive (NFRD). A 2017 Guideline of the Commission focuses on NFRD and states that "companies should consider making material disclosures on human rights due diligence", and that the companies "may consider disclosing material information and KPIs [key performance indicators] on occurrences of severe impacts on human rights relating to its activities or decisions".[78] It would be important to observe whether data breaches that cause harm to the rights and freedoms of natural persons could be classified as operational risks that could be subject to NFRD or the new CSRD. The proposed CSRD states is Article 19b.2.b.iii that the sustainability reporting by companies should specify the information that undertakings are to disclose about social factors, including "respect for the human rights ... established in the ... Charter of Fundamental Rights of the European Union". Article 8 of the EU Charter of Fundamental Rights focuses on the protection of personal data; therefore, cybersecurity risks that put personal data protection at risk might be expected to be covered by this new directive. Empirical data were collected on whether privacy is included in ESG reporting in the SEC disclosure requirement context.[79] Bloomberg Law analysed date obtained from publicly filed Form 8-Ks and Form 10-Ks and their research revealed that "a record number of companies will be classifying their data-privacy actions as ESG matters by early 2022".[80]

Article 33 and Recital 85 of GDPR refer to the data breach notification requirements, stating that reports of personal data breaches to the supervisory authority should be prompt, typically within seventy-two hours of detection, "unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons". GDPR requires controllers to carry out DPIAs to evaluate "the origin, nature, particularity and severity of [cyber] risk" as a way "to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons" as per Recital 84.[81] Working Party 29 issued guidelines on determining high-risk activities in order to facilitate the decision-making process for companies.[82]

[77] For a critical discussion of CSRD, see K Ramanna, "Friedman at 50: Is It Still the Social Responsibility of Business to Increase Profits?" (2020) 62(3) California Management Review 28.

[78] European Commission, Communication from the Commission Guidelines on non-financial reporting (methodology for reporting non-financial information) (2017/C 215/01) and 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.

[79] P Karalis, "Analysis: Is Privacy an ESG Win? SEC Filing Trend Says Yes" (*Bloomberg Law Analysis*, 2021) <https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-is-privacy-an-esg-win-sec-filing-trend-says-yes> (last accessed 5 January 2022).

[80] ibid. For a debate on ESG ratings, see DM Christensen, G Serafeim and A Sikochi, "Why Is Corporate Virtue in the Eye of the Beholder? The Case of ESG Ratings" (2022) 97(1) The Accounting Review 147. For a discussion on the possible use of privacy ratings, see E Erdemoglu, "A Law and Economics Approach to the New EU Privacy Regulation: Analysing the European General Data Protection Regulation" in J de Zwaan, M Lak, A Makinwa and P Willems (eds.), *Governance and Security Issues of the European Union* (The Hague, TMC Asser Press 2016).

[81] Regulation (EU) 2016/679 GDPR.

[82] Art 29 Data Protection Working Party Guidelines on DPIA and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. See also: OneTrust Blog, "WP29 Issues Revised Guidelines on Data Protection Impact Assessment (DPIA)" (2017) <https://www.onetrust.com/blog/article-29-working-party-issues-revised-guidelines-data-protection-impact-assessment-dpia/> (last accessed 3 January 2022).

GDPR Recital 85 describes the risks associated with a personal data breach as follows: "[P]hysical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymization, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned." GDPR Article 35 states that if a type of data processing is likely to result in a high risk to the rights and freedoms of natural persons, the data controller entity shall carry out a DPIA before processing the personal data. DPIAs are an essential part of risk assessment in several organisations. Among Fortune 100 companies, 24% reported data privacy as an individual risk factor in their Form 10-K filings, as well as frequently citing the rapidly evolving data protection regulations that create not only financial and legal exposure but also reputational risks.[83]

Working Party 29 guidelines analyse the personal data breach definition under GDPR. Article 4/12 defines a data breach as a breach of security leading to accidental or unlawful destruction, loss, alteration and/or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed. Destruction of data means that the data no longer exist, while loss of personal data could refer to instances where data still exist but the controller has lost access to them. The latter occurs when cybercriminals use ransomware to encrypt data if the company does not have a copy of the data that they can access.[84]

Regarding the role of lawsuits brought forward on the basis of the cybersecurity risk disclosures of companies, in the USA the discussion is centred on class action lawsuits brought by shareholders. In the European setting, group actions brought against firms in the aftermath of data breaches rest on consumer initiatives. The class action model originated in the USA and continues to be predominantly a US occurrence; however, Canada, as well as several European countries relying on civil law, have introduced some changes in recent years allowing consumer organisations representing groups of consumers to bring claims on their behalf. While we cannot speak of US-style class actions in a strict sense, in Europe new forms of collective redress are emerging in the privacy domain and in connection with GDPR.

A recently disclosed significant fine levied by a European regulator against Amazon could open up a discussion of how the European and US privacy regimes might potentially serve as a disciplining tool for corporate actors. The price of Amazon shares dropped by as much as 8% on 30 July 2021 after the e-commerce company disclosed a significant fine issued by the Luxembourg National Commission for Data Protection for allegedly failing to comply with European privacy laws and after it posted less than expected second-quarter earnings.[85] The disclosure occurred via a SEC filing. The revealed fine amounts to $885 million (746 million euros) and was imposed on 16 July on the grounds that Amazon's processing of personal data was non-compliant with GDPR.[86] It remains to be seen whether the ultimately levied fine will remain at such a high figure.

[83] Klemash et al, supra, note 1.

[84] Art 29 Data Protection Working Party 29, 18/EN, Guidelines on Personal data breach notification under Regulation 2016/679, Adopted 3 October 2017, Revised and Adopted on 6 February 2018.

[85] J Ponciano, "Amazon Stock Loses $130 Billion in Market Value After $885 Million Fine and Disappointing Earnings Report" (*Forbes*, 2021) <https://www-forbes-com.cdn.ampproject.org/c/s/www.forbes.com/sites/jonathanponciano/2021/07/30/amazon-stock-loses-130-billion-in-market-value-after-885-million-fine-and-dismal-earnings-report/amp/> (last accessed 3 January 2022).

[86] T Leggett, "Amazon Hit with $886m Fine for Alleged Data Law Breach" (*BBC News*, 2021) <https://www.bbc.com/news/business-58024116> (last accessed 3 January 2022).

V. Economic risk from non-compliance

Industry reports indicate that corporations are highly vulnerable to cyber risk.[87] The losses imposed via exposure to such risks will likely continue to increase if corporations do not change their approach to this issue. Kaspersky Lab, a technological consultancy, surveyed almost 6,000 firms across twenty-nine countries in 2018 regarding privacy risks in the business environment. According to this survey, 42% of large enterprises and 46% of small and medium-sized companies had experienced at least one data breach at some point in their company history.[88] The researchers also found that personal data from customers had been stolen in 40% of those data breach cases.

The Ponemon Institute and IBM Security surveyed over 400 corporations from thirteen countries in 2017. The results indicated that the average organisational cost of a data breach was US$7.35 million among US companies and US$3.62 million across the sample.[89] In some jurisdictions, firms may face class action lawsuits on top of these costs. For large breaches, settlements can reach over US$100 million.[90] Furthermore, the price of stocks of affected companies declines by 5% on average following the disclosure of data breach events.[91] Besides these financial costs, the Kaspersky Lab survey found that 31% of corporations that faced a data breach had laid off staff as a consequence.

At the same time, observers noted that the economic fallout of non-compliance with privacy rules due to regulatory fines and sanctions was much less than companies had initially anticipated because of the enforcement difficulties that privacy laws create. Companies could have gotten the impression that GDPR's level of enforcement was low. This may have reflected low enforcement commonly expected in the early years of a law's adoption. Indeed, there are indications that enforcement is increasing as the law's principles gradually are translated into more precise requirements throughout the European legal system.

Furthermore, Jang and Newman observed that transnational civil society groups are emerging across Europe.[92] They argued that these groups may create what they called a "transnational fire alarm" system that will spur and support litigation against corporations' infringements of privacy rights. Individual consumers are often ill-positioned to bargain for privacy *ex ante* or to react to privacy harms. Civil society organisations may be able to address this limitation, thereby deterring corporate abuses.

On the other hand, other scholars think that privacy laws in their current form are insufficient for deterring corporations from underinvesting in privacy risk management, which means that firms will find the overall costs due to privacy law enforcement manageable and the field will remain tilted against individuals concerned about their privacy, despite the hype surrounding the new privacy laws. For example, Helman argued that

[87] HJ Lehuedé, "Corporate Governance and Data Protection in Latin America and the Caribbean" (2019) Production Development series, No. 223 (LC/TS.2019/38), Santiago, Economic Commission for Latin America and the Caribbean (ECLAC) <https://repositorio.cepal.org/bitstream/handle/11362/44629/1/S1900395_en.pdf> (last accessed 3 January 2022).

[88] Kaspersky Lab, "From Data Boom to Data Doom – The Risks and Rewards of Protecting Personal Data" (2018) <https://go.kaspersky.com/rs/802-IJN-240/images/Kaspersky_Lab_Business%20in%20a%20data%20boom.pdf> (last accessed 3 January 2022).

[89] Ponemon Institute and IBM Security, "Cost of Data Breach Study – Global Overview" (2017) <https://www.securityupdate.net/SU/IBMSecurity/IBM-Security-Cost-of-Data-Breach-Study.pdf> (last accessed 3 January 2022).

[90] AH Southwell, E Vandevelde, R Bergsieker and JB Maute, "Gibson Dunn Reviews U.S. Cybersecurity and Data Privacy" (*Columbia Law School Blue Sky Blog*, 2017) <https://clsbluesky.law.columbia.edu/2017/02/03/gibson-dunnreviews-u-s-cybersecurity-and-data-privacy/> (last accessed 3 January 2022).

[91] Ponemon Institute, "The Impact of Data Breaches on Reputation and Share Value" (2017) <www.centrify.com/media/4772757/ponemon_data_breach_impact_study_uk.pdf> (last accessed 3 January 2022).

[92] W Jang and AL Newman, "Enforcing European Privacy Regulations from Below: Transnational Fire Alarms and the General Data Protection Regulation" (2022) 60(2) Journal of Common Market Studies 283.

consent mechanisms, which are typically part of newly emerging privacy laws, are insufficient and that market failures reduce corporations' incentives to internalise privacy concerns.[93] The same article argues that data use imposes externalities on others, implying that privacy infringements can burden individuals irrespective of their conscious choice. Helman, as well as Hartzog and Richards,[94] have proposed that social network executives should be held accountable for breaches in data privacy protection, thus effectively demanding a fundamental reform of traditional corporate law tenets in order to better control the privacy practices of companies with business models that rely on handling significant amounts of (sensitive) private data.

In earlier literature that empirically assessed the impacts of data breaches on firm fundamentals, Cavusoglu et al found that there is a negative correlation between the size of a data breach and stock market response.[95] Cavusoglu et al and Hovav and D'Arcy[96] found that data breach costs are higher for Internet firms. Garg et al reported that security attacks result in overall losses of 5.3% of value over a three-day event window and that Internet security vendors experience positive returns of 10.3% over the same window when security attacks are reported.[97] Campbell et al showed that breaches involving unauthorised access to customer personal data or firm proprietary data result in an average loss of firm value of 5.5%.[98] Gatzlaff and McCullough demonstrated that: (1) for firms that are less forthcoming about the details of a breach, market reaction and the breach are negatively associated; (2) a data breach is associated with greater negative abnormal returns when firms have higher market-to-book ratios; (3) features such as firm size and subsidiary status mitigate the negative effects of a data breach on the stock price; and (4) the negative market reaction to a data breach is stronger for the most recent time periods of their sample.[99]

VI. The view of the CISOs

The World Economic Forum recognises that systemic cyber risk is one of the most likely and potentially impactful risks facing firms.[100] The COVID-19 pandemic has significantly sped up the adoption of cloud and remote-working technologies.[101] These developments have led to a transformation of the attack surface and added complexity

[93] I Helman, "Pay For (Privacy) Performance: Holding Social Network Executives Accountable for Breaches in Data Privacy Protection" (2019) 84(2) Brooklyn Law Review 523.

[94] W Hartzog and N Richards, "Privacy's Constitutional Moment and the Limits of Data Protection" (2020) 61(5) Boston College Law Review 1687.

[95] H Cavusoglu, B Mishra and S Raghunathan "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers" (2004) 9(1) International Journal of Electronic Commerce 70.

[96] ibid; A Hovav and J D'Arcy, "The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms" (2003) 6(2) Risk Management and Insurance Review 97.

[97] A Garg, J Curtis and H Halper, "Quantifying the Financial Impact of IT Security Breaches" (2003) 11(2) Information Management & Computer Security 74.

[98] K Campbell, LA Gordon, MP Loeb and L Zhou, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market" (2003) 11(3) Journal of Computer Security 431.

[99] KM Gatzlaff and KA McCullough, "The Effect of Data Breaches on Shareholder Wealth" (2010) 13(1) Risk Management and Insurance Review 61.

[100] WEF, "Understanding Systemic Cyber Risk" (*World Economic Forum: Global Agenda Council on Risk and Resilience*, 2016) <https://www.weforum.org/whitepapers/understanding-systemic-cyber-risk> (last accessed 3 January 2022).

[101] B Al-Ruwaii and G De Moura, "Why the Time Has Come to Embrace the Zero-Trust Model of Cybersecurity" (*World Economic Forum*, 2021) <https://www.weforum.org/agenda/2021/10/why-the-time-has-come-for-the-zero-trust-model-of-cybersecurity/> (last accessed 3 January 2022).

and interdependency across the digital supply chain. Thus, the previous castle-and-moat approach focused on guarding the perimeter is becoming obsolete.[102]

The move to remote working since March 2020 has been linked to a substantial rise in cyberattack incidents.[103] ENISA's threat landscape report focused on the period between April 2020 and July 2021 found a spike in non-malicious incidents due to human error and system misconfigurations and that COVID-19 was the dominant luring subject for e-mail attacks.

The World Economic Forum reported that the number of accounted for global cyber-attacks was up by 22% in 2020.[104] In addition, phishing attacks were 600% more frequent in 2020 relative to the preceding year. An increase in the number of attacks targeting the Microsoft Remote Desktop protocol was also reported. In line with intuitive expectations, the highest increase in attacks was in the healthcare sector, which witnessed a 45% increase in attacks compared to 2019. A scholarly paper found that ransoms had increased as well, with the average ransom amount being 60% higher in the latter six months of 2020 than it had been in 2019, at US$170,000.[105] All in all, the aggregate economic cost to the global economy stemming from additional cyberattacks linked to the COVID-19 pandemic is more than US$1 trillion.

To obtain empirical evidence on current trends, the present study further assesses cyber-security risk governance through interviews with eleven CISOs/CSOs from financial-sector leads in the Benelux region. Through these interviews, we also gained insights into the impact of the COVID-19 pandemic on the risk management of cybersecurity.[106]

When CISOs/CSOs were asked which tasks related to cybersecurity risk management and cyber resilience domains take the greatest amount of their time on a daily basis, the most common answers were, in order of popularity: (1) cybersecurity awareness training; (2) demonstrating the operational effectiveness of cyber hygiene capabilities; and (3) third-party risk management. Respondents also emphasised various other cyber-security challenges such as concerns about state–actor intrusion, the need for decentral-ising security decision-making into DevOps teams (a combination of software development and IT operations) and business alignment regarding the implementation of cybersecurity practices in the full operation chain of the company.

We also asked the eleven CISOs/CSOs about their current best practices in cybersecurity risk management and cyber resilience. Communicating with senior management on applied examples of incidents from other financial-sector firms, execution of security by design principles, sharing threat intelligence, a zero-trust approach, making central decisions and explaining the reasoning behind certain security rules to the team were the most frequently reported answers.

When asked about the pandemic's impact on cybersecurity best practices to deal with the change to remote working, several survey participants reported that hybrid working increased the importance of best practices and led to a further focus on the acceleration of cybersecurity threats. They said that hybrid working had increased cybersecurity awareness among senior management and had decreased their willingness to tolerate

[102] ibid.

[103] R Jamilov, H Rey and A Tahoun, "The Anatomy of Cyber Risk" (2021) National Bureau of Economic Research WP No. 28906.

[104] I Greenberg, "Fifth-Generation Cyberattacks Are Here. How Can the IT Industry Adapt?" (*World Economic Forum*, 2021) <https://www.weforum.org/agenda/2021/02/fifth-generation-cyberattacks/> (last accessed 3 January 2022).

[105] HS Lallie, LA Shepherd, JRC Nurse, A Erola, G Epiphaniou, C Maple and X Bellekens, "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks During the Pandemic" (2021) 105 Computers & Security 102248.

[106] For an extended version of the collected insights, see E Kiesow Cortez and M Dekker, "Cybersecurity in Finance" (2022) HCL Whitepaper, forthcoming.

cybersecurity risk. In line with ENISA's threat landscape report stating that the pandemic multiplied incidents stemming from human errors and system misconfigurations,[107] respondents said that remote working during the COVID-19 pandemic had significantly increased cyberattacks targeted at the workforce and that the company had to improve their awareness campaigns as hybrid working is becoming standard. All of them said that they expect remote working to become more prominent in their company's future and that they were still using a hybrid work model in which employees continue to work from home and come into the office only when it is required.

Regarding which parameters are becoming increasingly important in cybersecurity management in the financial services, our CISO/CSO participants responded that they expect investments to increase in the domains of data integrity, data quality and operational effectiveness. They also stated that cybersecurity-related events had received much more attention from regulators during the COVID-19 pandemic than previously. In line with this, when asked which regulatory frameworks impacted or would impact their cybersecurity strategies most, the majority of participants referenced DORA, which the EU is expected to adopt in 2022, and future data transfer regulatory frameworks they anticipate will emerge after the Schrems II decision[108] of the Court of Justice of the European Union.

Jamilov et al's comprehensive study of data gathered four times a year from over 12,000 firms located in eighty-five countries since 2002 reveals several clear facts on global cyber risk.[109] First, the industrial composition of global cyber risk exposure is shifting towards the financial sector. The finance industry exhibited very little exposure before 2014, but it is now the third most affected sector after IT professional services, which includes cyber-sensitive IT consulting firms, and after manufacturing.

In our interviews, we also asked participants what kind of changes they foresee encountering in their tasks in the next two to five years. CISOs realise that they need to engage significant principals on the topic and learn how to articulate relevant cyber risk exposure details to stakeholders. They foresee a need for more transparency regarding the cyber risk originating from the supply chains of their companies. In addition, as supply chains are becoming more symmetrical, they expect to be required to provide information about cybersecurity strength to the suppliers of their companies, as well as to their boards and investors. As more and more security controls are crossing legal or corporate boundaries, CISOs in the Benelux region realise that they need to recognise information gaps and strengthen their teams with more diverse skills and expertise, including knowledge of psychology to better analyse human factors in attack vectors and legal expertise given that security controls in the supply chain are increasingly enforced through legal clauses.

Many interviewees highlighted a greater need for cybersecurity awareness and self-service capabilities, the need to increase the "consumability" of security measures such that each individual employee can understand and employ them, the need for acceleration of business and the need to move towards 100% coverage for security services triggered by increased reliance on cloud environments. Now that the general public recognises information security as an existential business risk, it seems likely that boards will expect CISOs to be prepared to be much more transparent about the cybersecurity strength of their companies and to be able to better articulate the return of investments in security. As one interviewee explained to us, "with the experiences of the COVID-19 pandemic, cybersecurity is now seen as a business enabler also in light of the much more frequent uses of the cloud environments for collaborative working on sensitive documents".

[107] *ENISA Threat Landscape Report 2020* <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends> (last accessed 3 January 2022).

[108] Case C-311/18, ECLI:EU:C:2020:559 (2020).

[109] Jamilov et al, supra, note 103.

VII. Conclusion

We argue in this article that information asymmetries and related agency problems between management and other corporate stakeholders represent important explanations of companies' underinvestment in cybersecurity measures. Management efforts at privacy compliance are difficult to observe and monitor, which opens up opportunities for firm management to act in ways that are not in line with the preferences of shareholders and other stakeholders. High-profile class action suits initiated after the detection of privacy violations by firms and the imposition of significant penalties by regulatory authorities are signs of the potentially fraught management–shareholder relationship with regards to firms' cybersecurity practices.

We collected insights through semi-structured interviews with eleven CISOs/CSOs in the Benelux region on the most up-to-date cybersecurity risk management strategies in the financial sector. Relying on classic principal–agent theory, the expectation would be that managers underinvest in cybersecurity given the information asymmetry between stakeholders and management, especially in this domain. It is difficult for stakeholders to appropriately monitor the efforts by management to make the company more cybersecure, and it is also difficult for stakeholders to quantify and assess the effectiveness of any measures taken by management. This means that, from the perspective of corporate governance theories, management can get away with underinvesting in precautionary measures while at the same time deflecting blame for accidents and attributing the occurrence of data breaches to chance or residual risk.

Although the semi-structured interviews revealed a series of more nuanced findings, overall the CISOs pointed out that cyber threats are beginning to be taken more seriously and that a more proactive approach towards cybersecurity is emerging.

Given the theoretical predictions just mentioned, how should the stated intentions by these company representatives to take cyber risk seriously be interpreted? Are they mere pronunciations of intentions that will not be followed through with concrete steps, or do they indicate a genuine shift and so the theoretical predictions should be reconsidered or at least refined? If we assume for a moment that the shift is *de facto* happening and attention to cybersecurity will significantly increase, one can think of ways in which the principal–agent model could accommodate the occurrence of such a shift. For instance, the magnitude of the costs from security breaches over the last decade or so provided stakeholders with new information that would make it rational for them to accept incurring higher monitoring costs in order to more closely control managers' actions and performance regarding cybersecurity. Some of the increased monitoring costs would include stakeholders making themselves more familiar with cybersecurity risks and opportunities for them to exert control, thereby adjusting their information base and putting themselves in a better position to oversee management behaviour in this domain. Furthermore, the regulatory landscape in this domain has also evolved, and increasingly firms are obliged to disclose possible cybersecurity risks and expected costs related to their operations within their financial reporting. These disclosure requirements have introduced new demands on management regarding their focus on cybersecurity risks in addition to facilitating monitoring by stakeholders.

The prediction of underinvestment in cybersecurity relates to the assumption that monitoring by stakeholders is costly and challenging. The monitoring possibilities seem to be improving with new disclosure requirements, and there is also an increasing number of shareholder lawsuits that question managements' cybersecurity risk governance. These two developments might have added to the more recent management-level attention to cybersecurity operations, which is also shown in our interview results, indicating that there has been a shift in managements' approaches to assessing cybersecurity risks,

leading them to assess such risks more carefully. However, according to our findings, we should not expect this to be a swift and linear process given the evolving nature of both technological development and parallel cyber threats, the technical details of which might remain, at least to some extent, obscure to company stakeholders and their narrow circles of experts.

Acknowledgments. The authors would like to thank The Hague Security Delta for their support in facilitating the CISO interviews.

Competing interests. The authors declare none.

Cite this article: E Kiesow Cortez and M Dekker (2022). "A Corporate Governance Approach to Cybersecurity Risk Disclosure". *European Journal of Risk Regulation* **13**, 443–463. https://doi.org/10.1017/err.2022.10