“Cyber-risk and Director’s Liability: Exploring the Dutch Legal Framework”

A study on derivative liability in the wake of a cyber-incident

Author: Bibi Lalisang

Student number: 2031894

Date: 27 January 2020

Word count: 21.524

Supervisor: Aaron Martin

Second Supervisor: Magdalena Brewczyńska

LLM Law & Technology, Tilburg Institute for Law, Technology, and Society (TILT)

Table of Contents

1. Introduction

1.1 Background

The rise of the internet and recent technological developments mean that companies are increasingly dependent on digital processes. This increasing dependence has led to cybercrime becoming a worldwide problem and therewith to cyber-attacks having an ever-stronger impact on companies. Cyber-attacks may occur in various forms, such as ransomware, phishing, malware, denial of service (DoS) and distributed denial of service (DDoS).

According to a report of the National Coordinator for Security and Counterterrorism (henceforth "NCTV"), the number of cyber-attacks has risen sharply in recent years.[1] This report of 2019 specifically states that the Netherlands is vulnerable to cyber-attacks due to the fact that the resilience of Dutch government institutions and companies is still not in place and is therefore insufficient.[2] A very recent example, published in a Dutch newspaper on 14 January 2020, stated that hundreds of Dutch companies can be hacked easily due to a vulnerability in Citrix servers.[3] These servers run on Citrix software, which allows employees to work remotely. This vulnerability in Citrix servers came to the fore, because NCTV issued a warning about these servers on 13 January 2020. The vulnerability of Citrix servers is assessed in terms of severity on a 9.8 on a scale of 1 to 10. This finding of the NCTV shows, again, that companies are still successfully being attacked with simple methods and some companies even fail to take the most basic precautionary measures, while incidents could have been prevented and damage could have been more limited.[4] The vulnerability in Citrix software and the NCTV report of 2019 indicate it is not surprising that, relying on Deloitte's figures, cybercrime would cost Dutch companies €10 billion per year.[5] Because of this, cyber-risks are one of the five most important concerns for companies.[6] These statistics imply that investing in cyber-security is no longer a choice, but a necessity and decision-making regarding Information Technology (henceforth "IT") and therewith cyber-security management plays an increasingly important role within a company. Therefore, it becomes all the more important for companies to manage these damaging cyber-risks.

---

[1] National Coordinator for Security and Counterterrorism, 'Cybersecuritybeeld Nederland CSBN 2019' (2019) <https://www.rijksoverheid.nl/documenten/rapporten/2019/06/12/tk-bijlage-cybersecuritybeeld-nederland-csbn-2019> accessed 28 December 2019.

[2] ibid 33; Karel Berkhout, 'Nederland Is Kwetsbaar Voor Cyberaanvallen' *NRC Handelsblad* (Rotterdam, 12 June 2019) <https://www.nrc.nl/nieuws/2019/06/12/nederland-is-kwetsbaar-voor-cyberaanvallen-a3963381> accessed 28 December 2019.

[3] Hella Hueck and Stijn Van Gils, 'Honderden Nederlandse Bedrijven Met Citrix-Servers Vatbaar Voor Hack' *Financieel Dagblad* (Amsterdam, 2020) <https://fd.nl/ondernemen/1330985/honderden-nederlandse-bedrijven-met-citrix-servers-vatbaar-voor-hack#> accessed 17 January 2020.

[4] National Coordinator for Security and Counterterrorism (n 1) 34.

[5] Maarten Van Wieren and others, 'Cyber Value at Risk in the Netherlands' (2016) <https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-cyber-value-at-risk.pdf> accessed 28 December 2019.

[6] AON Risk Solutions, 'Global Risk Management Survey' (2019) <https://www.aon.com/2019-top-global-risks-management-economics-geopolitics-brand-damage-insights/index.html> accessed 20 December 2019.

If a company does not adequately protect itself against cyber-risks, considerable financial damage can occur, such as: a decline in share price[7] and revenues[8], loss of customers[9], time to recover decrease productivity, costs involving cyber-infrastructure upgrade, regulatory fines and legal fees arising from lawsuits[10]. In addition, the interests of third parties, such as creditors, shareholders and customers, may also be at stake.

Barely a week goes by without news of a major cyber-incident being reported. Looking back at December 2019 alone, several companies have fallen victim to ransomware-attacks. Examples of these kinds of attacks occurred at Maastricht University and GWK Travelex, a money exchange company.[11] At Maastricht University mostly students and employees were hit by this ransomware-attack.[12] Almost all Windows systems have been hit and email could not be used.[13] GWK Travelex, which was also affected by ransomware, seems to have ignored a major update.[14] In case of a ransomware-attack, files are made inaccessible until the victim pays. The hackers of GWK Travelex demand €4.6 million.[15] Maastricht University already paid several hundred thousand euros to the hackers who broke into its computer system.[16] This shows that these types of attacks are becoming larger and more ingenious, with companies and organizations being consciously attacked.

Cyber-risks are all the more pressing for companies with knowingly outdated and/or weakened IT systems. Withholding or insufficient recognition of such risks can lead to costs running sky-high for a company. Hence, the ever-increasing array of cyber-risks requires on-going involvement in cyber-security management of the board of directors (henceforth "board"). The reason for this is that these risks are by no means limited and illusory. As a result, directors should increasingly be aware that these risks can have a negative impact on their company, i.e. on growth expectations and shareholders'

---

[7] Paul Bischoff, 'How Data Breaches Affect Stock Market Share Prices' (*Comparitech*, 6 November 2019) <https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/#Long_term_effects_of_data_breach_on_share_price> accessed 31 December 2019.
[8] Ponemon Institute, '2019 Cost of a Data Breach Report' (2019) 12, 34 <https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf> accessed 30 December 2019.
[9] ibid 5, 36.
[10] Dan Swinhoe, 'The Biggest Data Breach Fines, Penalties and Settlements so Far' (*CSO*, 20 December 2019) <https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html> accessed 29 December 2019.
[11] Marcel Van Den Bergh, 'Universiteit Maastricht Kampt Met Ransomware-Aanval' (*NOS Nieuws*, 24 December 2019) <https://nos.nl/artikel/2316120-universiteit-maastricht-kampt-met-ransomware-aanval.html> accessed 27 December 2019; Rupert Jones, 'Travelex Forced to Take down Website after Cyber-Attack' *The Guardian* (London, 2 January 2020) <https://www.theguardian.com/technology/2020/jan/02/travelex-forced-to-take-down-website-after-cyber-attack> accessed 14 January 2020.
[12] Marcel Van Den Bergh, 'Universiteit Maastricht Kampt Met Ransomware-Aanval' (*NOS Nieuws*, 24 December 2019) <https://nos.nl/artikel/2316120-universiteit-maastricht-kampt-met-ransomware-aanval.html> accessed 27 December 2019.
[13] ibid.
[14] Stijn Van Gils, 'Door Ransomware Getroffen Travelex Negeerde Belangrijke Update' *Financieel Dagblad* (Amsterdam, 8 January 2020) <https://fd.nl/ondernemen/1330410/door-ransomware-getroffen-geldwisselbedrijf-travelex-negeerde-belangrijke-update#> accessed 14 January 2020.
[15] Rupert Jones, 'Travelex Services Begin Again after Ransomware Cyber-Attack' *The Guardian* (London, 13 January 2020) <https://www.theguardian.com/business/2020/jan/13/travelex-services-begin-again-after-ransomware-cyber-attack> accessed 14 January 2020.
[16] 'Maastricht University Paid Hackers to Get Back System Access' (*DutchNews.nl*, 2 January 2020) <https://www.dutchnews.nl/news/2020/01/maastricht-university-paid-hackers-to-get-back-system-access/> accessed 14 January 2020.

confidence. It is therefore remarkable that a recent survey among listed companies shows that only 40% of directors in the Netherlands consider cyber-security as a responsibility of the board.[17] Hence, cyber-security management is not considered part of daily business, i.e. it is characterized as a burden, difficult and not providing direct financial benefits.[18] It requires financial investments, time and people and is an attractive first target for budget cuts of companies.[19] Even though warranting cyber-security in a company might seem unnecessary and is not considered a top priority for the board, managing cyber-risks has become the inevitable cost of doing business today. Because of this, directors are expected to ensure cyber-security, despite the fact that most boards are unaware of and therewith unprepared for this role.[20]

This lack of knowledge and awareness regarding these new and complex cyber-risks poses potential problems for companies and its directors. To cover this, the board should demonstrate an insight into cyber-risks and take adequate measures against it. The Cyber Security Council (henceforth "CSR") expects that, in the near future, damage due to the absence of cyber-security management or poor cyber-security management will be recovered from directors.[21] The CSR is a national and independent advisory body of the government and consists of representatives from public and private organizations and science. The CSR is – at a strategic level – committed to increasing cyber-security in the Netherlands. The task of the CSR is to provide solicited and unsolicited advice to the government on timely and effective response to new technological developments and on the roles and responsibilities in the cyber-domain. The CSR also sets the agenda for research regarding priority themes in the field of cyber-security. In addition, the CSR ensures public-private cooperation at a strategic level in the cyber-security domain and contributes to awareness about cyber-security within the government and industry.[22]

The board, which consists of directors, is responsible for the daily management of the company.[23] The role of the board and therewith of the directors regarding cyber-security management is likely to become increasingly important in the near future.[24] A recent case, which is described below, illustrates that the personal consequences for directors can be far-reaching with respect to falling short in cyber-security management.

---

[17] KPMG, 'Cyber Security Benchmark' (2017) <https://assets.kpmg/content/dam/kpmg/pdf/2015/05/Cyber-Security-Benchmark.pdf> accessed 18 January 2020.

[18] Rene M Stulz, 'Six Ways Companies Mismanage Risk' [2009] Harvard Business Review <https://hbr.org/2009/03/six-ways-companies-mismanage-risk> accessed on 27 December.

[19] Ray A Rothrock, James Kaplan and Friso Van der Oord, 'The Board's Role in Managing Cybersecurity Risks' [2018] MITSloan Management Review <https://sloanreview.mit.edu/article/the-boards-role-in-managing-cybersecurity-risks/> accessed 27 December 2019.

[20] 'Hiscox Cyber Readiness Report' (2019) <https://www.hiscox.co.uk/sites/uk/files/documents/2019-04/Hiscox_Cyber_Readiness_Report_2019.PDF> accessed 17 January 2020.

[21] 'Bedrijven Doen Nog Te Weinig Aan Digitale Veiligheid' (*Cyber Security Raad*, 2017) <https://www.cybersecurityraad.nl/010_Actueel/bedrijven-doen-nog-te-weinig-aan-digitale-veiligheid.aspx> accessed 28 December 2019.

[22] 'Cyber Security Raad' <https://www.cybersecurityraad.nl/binaries/CSR_Flyer_NED_20191125_tcm107-314456.pdf> accessed 18 January 2020.

[23] Article 2:9(2) of the Dutch Civil Code (henceforth "DCC"); see Appendix A.

[24] Wim Weterings, 'Persoonlijke Aansprakelijkheid Bestuurders Voor Onvoldoende IT-Governance' [2016] Aansprakelijkheid, verzekering en schade 209, 210.

This recent case concerned a phishing attack at Pathé Theatres established in the Netherlands. The Chief Executive Officer (henceforth "CEO") and Chief Financial Officer received fake e-mails of the mother company in France with regard to a strictly confidential acquisition. Pathé the Netherlands mistakenly transferred €19 million to cyber adversaries.[25] Both directors have been fired after this cyber-incident. Although they were not involved in the fraud, Pathé said they could – and should – have noticed the "red flags". They did not, and there was no safety net in place, so the phishing attack was devastatingly successful.[26]

1.2 Problem statement

Nowadays, companies face the dependency of using IT systems for supporting their business processes. However, this creates a borderless and complex digital environment. There are two sides to this phenomenon. On the one hand, digitization provides companies with greater speed and convenience in their processes, decision-making and services. Information becomes more accessible, easier to exchange and share and is less costly. Hence, stakeholders are enabled to access the information whenever, wherever and however at their personal convenience. On the other hand, digitization also introduces new risks, i.e. mainly cyber-risks, to those companies. An example is a computer malfunction that disrupts railroad traffic, breaks down the administrative process of a hospital, or makes mobile telephony impossible or unsafe. The sources of cyber-risks are diverse and complex and could lead to undesirable financial consequences.

The cyber-risk landscape has evolved rapidly over the past decades. Cyber-risk is a broad concept that encompasses all risks that arise from the use of technology and data. Cyber-risks have recently undergone a surge in prominence. This is in part because of a number of high-profile adverse cyber-incidents that have brought the issue of cyber-risk to the forefront of public attention around the world.[27] At a corporate level, most people are now aware that an adverse cyber-incident can have significant consequences for an affected company.[28] National and international newspapers are frequently reporting that companies have incurred regulatory fines and penalties for failing to manage cyber-risks adequately.[29]

What is less well known is the liability risk that individual directors may face in relation to cyber-risks. It is clear that, although cyber-risks are growing in prominence, not all companies and directors are well informed about this issue. However, since cyber-security has become a subject of much interest and business processes are – to a considerable extent – conducted digitally and/or online, one could argue that a director is responsible for adequate and appropriate security of these business processes. Therefore, the role of the board comes into play.

---

[25] Christopher Boyd, 'Business Email Compromise Scam Costs Pathé $21.5 Million' (*Malwarebytes labs*, 19 November 2018) <https://blog.malwarebytes.com/cybercrime/2018/11/business-email-compromise-scam-costs-pathe-21-5-million/> accessed 23 December 2019.
[26] ibid.
[27] Lily Hay Newman, 'The Biggest Cybersecurity Crises of 2019 So Far' (*Wired*, 7 May 2019) <https://www.wired.com/story/biggest-cybersecurity-crises-2019-so-far/> accessed 29 December 2019.
[28] Simon Bushell and Gail Crawford, 'Cyber Security: Litigation Risk and Liability' [2014] *Thomas Reuters Practical Law*.
[29] Laura Stocks, 'Panama Papers: Time to Firm up on Cyber Security?' [2016] *Thomas Reuters Practical Law*.

With the increasing dependence on IT processes and the associated cyber-risks, the question arises as to whether the board and therewith the directors should become more involved in cyber-security management and, in turn, in preventing a cyber-incident. If the answer is yes, the question can be raised as to whether they can be held personally liable for failing to do so and, by extension, which circumstances are required for such a liability. If damage has occurred to a third party, one could question whether he can recover this damage by bringing proceedings against the director who acted negligently regarding cyber-security management.

In my research, this third party is a shareholder. The reason why I have chosen for this delineation is that a shareholder can suffer damage due to a depreciation of his shares as a result of damage caused to the company.[30] This is called derivative damage.[31] This derivative damage should, in my research, stem from an occurred cyber-risk. While in the Netherlands no claims have been raised yet regarding derivative damage as a result of an occurred cyber-risk, in the US there is a considerable amount of cases with respect to these kinds of claims.[32] Although I will not make a comparative analysis with the US, it is interesting to look into some of these cases. The reason for this is that in these US cases shareholders have claimed derivative damage due to an occurred cyber-risk.[33] Since cyber-incidents are becoming commonplace, it seems unavoidable that cyber-related claims against directors will also follow in the Netherlands. This will most likely happen when disadvantaged shareholders seek compensation for their suffered damage, i.e. derivative damage, as a result of poor cyber-security management.

Because of this delineation of the scope to shareholders, I will only focus on both public- and private limited liability companies (henceforth "companies").[34] The reason for this is that these companies have share capital and I am focusing on the perspective of the shareholder in this research. Only public-and private limited liability companies that are established in the Netherlands, and are therefore governed by Dutch corporate law, fall within the scope of my research. As per 1 January 2013, the one-tier board structure was formally introduced in Dutch law. This one-tier board system can be used in both a public-and private limited liability company. Before 2013, Dutch corporate law only allowed the customary two-tier board structure in the Netherlands. As I expect this possibility for a one-tier board structure will be used more frequently in the future, I will examine whether there is a distinction in liability of directors between these two board systems. The reason why this may be of relevance is that in case there is a substantial difference in the liability regime of directors, a company could decide to choose for the most beneficial regime.

---

[30] Daan Ballegeer, 'Cyberdief neemt ook beurswaarde mee' *Financieel Dagblad* (Amsterdam, 14 April 2019) <https://fd.nl/beurs/1296909/cyberdief-neemt-ook-beurswaarde-mee#> accessed 22 December 2019.

[31] Maarten Kroeze, 'Afgeleide Schade En Afgeleide Actie' (thesis, University of Groningen 2004) 17.

[32] Benjamin Dynkin and Barry Dynkin, 'Derivative Liability in the Wake of a Cyber Attack' (2018) 28 Albany Law Journal of Science and Technology 23 <http://www.albanylawjournal.org/Documents/Articles/28.3.23_Dynkin.pdf> accessed 13 January 2020; Benjamin P Edwards, 'Cybersecurity Oversight Liability' (2019) 35 Georgia State University Law Review 663 <http://www.albanylawjournal.org/Documents/Articles/28.3.23_Dynkin.pdf> accessed 13 January 2020.

[33] ibid.

[34] Article 2:129 et seq. DCC for public limited liability companies, article. 2:175 et seq. DCC for private limited liability companies.

1.3 Research questions

The following central research question follows from the above:

'To what extent can a director of a Dutch company be held liable by a shareholder when a cyber-risk resulting in derivative damage has occurred within the current legal framework?'

The central research question is answered on the basis of a number of sub-questions. These are as follows:

1. What is the current legal liability framework of a director of a Dutch company?
2. What are the possibilities for a shareholder to claim derivative damage from a director?
3. What are the duties of a director regarding a cyber-risk?
4. Under which circumstances can a director be held liable by a shareholder in case a cyber-risk resulting in derivative damage has occurred?

An occurred cyber-risk can be the result of various factors. In my research, the starting point is that a cyber-risk occurs due to poor cyber-security management. The reason for this is that it is most likely that a director will be held personally liable by a shareholder in case an occurred cyber-risk, which has led to derivative damage, is the (in)direct consequence of poor cyber-security management. Hence, the assumption of poor cyber-security management is embedded in the research question.

1.4 Research methodology

The objective of this research is to gain insight into the relationship between the liability of directors established in the Netherlands in case of a cyber-incident and shareholders derivative damage. In this legal research, a descriptive method is used. It is descriptive in a way that this research will come to a conclusion as to whether, and under which circumstances, directors can be held liable by a shareholder for an occurred cyber-risk under the Dutch legal liability framework of directors. Literature and document research, including case law and legal scientific literature, was used to answer the research questions.

To answer the first sub-question, I had to review extensive case law and literature regarding the Dutch liability framework of directors. With respect to the second sub-question about claiming derivative damage, I again carefully analyzed Dutch case law and literature on this doctrine. Regarding my third sub-question, I examined the specific duties of directors regarding cyber-risks. When researching literature on cyber-risks in relation to liability of directors, which concerns my fourth sub-question, it became apparent that this is yet uncultivated territory in the Netherlands. Cyber-risks and related liability issues of directors are, particularly in the Netherlands, a relatively new phenomenon. Currently, I am not aware of any Dutch judgments that address the liability of directors regarding poor cyber-security management, and therewith regarding a cyber-incident.[35] The same holds for case law in which a shareholder claims derivative damage, as a result of a cyber-incident, from a director. Due to the lack of this kind of case law, the fourth sub-question has been

[35] However, there is one exception: the DigiNotar case. In this case it concerned liability of directors as a result of breaching a warranty. This warranty contained a general obligation to ensure adequate cyber-security management. See District Court Amsterdam 30 July 2014, ECLI:NL:RBAMS:2014:4888.

answered by analyzing two US cases and one Dutch case (which has not been brought before a court). All three cases had to deal with a cyber-incident. I hypothetically applied the facts of these cases to the Dutch legal context and assessed whether the directors in these cases could (hypothetically) be held liable.

It is important to note that most discussed case law is only relevant to the extent that it has been used to support the interpretation of the Dutch liability framework of directors on which it can be determined whether there is liability in general terms.[36] In line with this absence of Dutch case law regarding liability of directors with respect to a cyber-incident, literature on liability of directors pertaining to poor cyber-security management or a cyber-incident is also scarce. Therefore, throughout this research, reference will usually be made to literature regarding liability of directors in a general sense as there is quite some literature on liability of directors in general.

Hence, the aim of this research is to get a better understanding of managing cyber-risks in relation to liability of directors by reviewing (scientific) literature, case law, the current Dutch legal liability framework of directors and the specific duties of directors regarding cyber-risks.

Lastly, Appendix C contains a glossary of the – for my research – relevant cyber-related terms. The reason why I have chosen to leave them out of the body of my research is that it would interrupt the narrative flow.

1.5 Demarcation of the research

Firstly, directors may be held liable for actions that they performed as directors of the legal entity. This research focuses on liability of directors regarding an occurred cyber-risk. In the context of liability of directors, both internal liability of directors towards the legal entity[37], i.e. the company itself, and external liability of directors towards a third party[38], including a shareholder, are dealt with. Initially, a disadvantaged party will, as a rule, turn to the legal entity in question. The reason for this is that a stricter threshold applies to the liability of directors. In order to delimit the scope of this research, I will not discuss the liability of the legal entity itself.

Secondly, a liability claim towards a director as a result of a cyber-incident could theoretically lead to bankruptcy of the company. However, liability claims which lead to insolvency are beyond the scope of this research.

Thirdly, this research does not concern the product liability with an information and communications technology application and therewith the possibility to be subjected to a cyber-attack. This would involve product liability. The scope of my research does not lend itself to address these issues.

Fourthly, the two-tier board system consists of a Supervisory Board and a board of directors. This Supervisory Board is a separate body and has less influence on the decision-making process of the board. Because of this, I will only focus on liability of directors of the board.

Fifthly, although data protection is a significant part of cyber-security, it will be left outside the scope of this research. The reason for this is that discussing data protection provisions, which are laid down in the General Data Protection Regulation[39]

[36] Article 2:9 DCC.
[37] Article 2:9 DCC; see Appendix A.
[38] Article 6:162 DCC; see Appendix B.
[39] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data on the free movement of such data and repealing Directive 95/46 (General Data Protection Regulation) [2016], L 119/1.

(GDPR), would require an extensive analysis. This research does not lend itself to such an analysis, and therefore goes beyond the scope of my research.

Sixthly, in order to delimit the scope of my research, I will not discuss the way in which shareholders should *demonstrate* derivative damage.

Lastly, cyber-insurance falls outside the scope of my research, because this will only come into play when the liability of a director has been established.

1.6 Overview of the chapters

This research consists of six chapters, chapter 1 being the introduction. In chapter 2, I will outline the current Dutch legal framework regarding the liability of directors. This involves the legal principles of internal liability of directors towards the legal entity, i.e. the company itself, as well as the external liability of directors towards third parties, which include shareholders. In chapter 3, the possibilities for a shareholder to claim derivative damage from a director will be discussed. Chapter 4 will go into the duties of directors arising from cyber-risks. In chapter 5, I will set out two American cases and one Dutch case, which all three had to deal with a cyber-incident. I will use the facts of these cases and apply them to the Dutch legal liability framework of directors. Therefore, examining whether the directors of these cases would be liable under Dutch law will be a purely hypothetical assessment. The central research question will be answered in chapter 6. In this chapter a final conclusion will be reached, and I will give some recommendations with regard to my research.

2. Dutch legal liability framework of directors

2.1 Introduction

In this chapter I will set out the Dutch legal framework regarding liability of directors. This includes the board structure, the legal bases of internal liability of directors towards the legal entity, as well as external liability of directors towards shareholders. I will also discuss some recent developments regarding exculpation possibilities for internal liability of directors. It is important to note that the two-tier board structure is my starting point in this chapter. However, in one paragraph I will make a passing reference to the one-tier board structure with regard to exculpation.

2.2 Internal liability of directors

2.2.1 Board structure

In the Netherlands, each company needs a board of directors, consisting of appointed board members. For a long time, Dutch law provided only for the so-called two-tier board structure, in which the supervisory directors are organized in a separate board, supervising the board of directors. Since 1 January 2013, Dutch law facilitates the creation of a one-tier board structure for companies.[40] Hence, in the one-tier board, the board of directors and the Supervisory Board are combined in one body[41], while in the customary two-tier system the board of directors and the Supervisory Board are two separate bodies. In order to create a one-tier board structure, the articles of association must provide that the tasks of the board be divided among one or more non-executive directors and one or more executive directors. This means that non-executive directors are collectively responsible together with the executive directors for the general course of affairs of the company. While the executive members are responsible for the company's daily management, the non-executive members have at least the statutory task of supervising the board in the performance of its duties.[42] In this research, I will discuss both the two-tier board structure and the one-tier board structure. The two-tier structure is relevant to address, because it is the most widely used regime in the Netherlands.[43] However, since the one-tier structure is introduced in Dutch law in 2013, I will examine whether there is a distinction in the liability regime between executive and non-executive board members. This will be analyzed later in this chapter.

According to article 2:129 paragraph 1 and article 2:239 paragraph 1 DCC, the board is responsible for managing the company.[44] It is generally assumed that "management" within article 2:129 DCC in any case means responsibility for the daily course of

[40] Act of 6 June 2011, *Stb*. 2011, 275 ("The Act on Supervision and Management"). This Act came into effect on 1 January 2013. Since the implementation of this Act, a one-tier board structured was introduced in Dutch corporate law.

[41] This is also reflected in principle 5.1 of the Dutch Corporate Governance Code 2016. On 8 December 2016, the Monitoring Committee Corporate Governance Code has published the new Corporate Governance Code (henceforth "Code"). The Code applies to any financial year starting on or after 1 January 2017. <https://www.mccg.nl/?page=4738> accessed 29 November 2019.

[42] Derk Lemstra, 'Act on Management and Supervision Will Enter into Force on 1 January 2013' (*Stibbe*, 27 September 2012) <https://www.stibbe.com/en/news/2012/september/act-on-management-and-supervision-will-enter-into-force-on-1-january-2013> accessed 17 January 2020.

[43] SpencerStuart, '2018 Netherlands Spencer Stuart Board Index' (2018) 6 <https://www.spencerstuart.com/-/media/2018/december/nlbi2018.pdf> accessed 9 December 2019. This report shows that, out of study of 50 Dutch companies, 44 companies have a two-tier board structure.

[44] Maarten Kroeze, *Mr. C. Assers Handleiding Tot de Beoefening van Het Nederlands Burgerlijk Recht. 2. Rechtspersonenrecht. Deel I. De Rechtspersoon* (Kluwer 2015).

affairs, the objectives, strategy, financial policy and finally risk management.[45] From article 2:141 paragraph 2 and 2:251 paragraph 2 DCC also appears more explicitly that the board is involved in risk management and the establishment of management and control systems.[46] It is important to note that it is widely assumed that risk management is a core task of the board.[47] For my research it is of importance to stress that I assume that cyber-security management falls under risk management.[48] The rationale behind this assumption is that cyber-security should be included in the enterprise risk management of companies in order to improve cyber-security awareness among directors. As a result of this, cyber-risks will be mitigated and (better) managed.

2.2.2 Collective responsibility

Internal liability of directors is based on article 2:9 DCC. Since 1 January 2013 the current legal text states:

"1. Each director is responsible towards the legal entity for a proper performance of his duties. To the duties of all directors belong all duties that have not been assigned by or pursuant to law or the articles of association to one or more other directors.
2. Each director is responsible for the general conduct of affairs. He is fully liable for improper management, unless, also with regard to the tasks assigned to the other directors, serious blame cannot be attributed to him and he also has not been negligent in taking measures to avert the consequences of such improper management."

Hence, on the basis of article 2:9 paragraph 1 DCC each director is responsible towards the legal entity for a proper performance of his duties.[49] A director is fully liable for improper performance of duties towards the legal entity, unless serious blame cannot be attributed to him, as follows from article 2:9 paragraph 2 DCC.

With respect to a board of multiple directors, the starting point of article 2:9 DCC is that these directors are collectively responsible and jointly and severally liable for the improper performance of duties by the board, except for the possibility of exculpation. So, the board as a whole has a collective responsibility to properly perform its tasks. In principle, all directors are jointly and severally liable towards the legal entity in the event of improper performance of duties by one of them.[50] This is a consequence of the principle of collective responsibility. A division of tasks does not release an individual director from that collective responsibility. This is only different if an individual director can exculpate himself from liability.

Despite a possible division of tasks within the board, all the directors have the responsibility to make decisions jointly on important (financial) issues concerning the company and to supervise the performance of each other's duties. The principle of

[45] MM Stolp and W De Nijs Bik, 'De Positie van Bestuurders En Commissarissen Ter Zake van Risicomanagement' in Arie Tervoort, Henk Bruisten and Suzanne Drion (eds), *Be (aware). Legal Risk Management & Compliance* (Sdu juridisch 2015).
[46] This also follows from principle 1.2 Code.
[47] Grant Kirkpatrick, 'The Corporate Governance Lessons from the Financial Crisis' (11 February 2009) 3, 17, 19 <https://www.oecd.org/finance/financial-markets/42229620.pdf> accessed 31 December 2019; 'Corporate Governance and the Financial Crisis: Key Findings and Main Messages' (June 2009) 40 <https://www.oecd.org/corporate/ca/corporategovernanceprinciples/43056196.pdf> accessed 31 December 2019.
[48] This claim is also supported by the report of "Risk and Responsibility in a Hyperconnected World" of the World Economic Forum.
[49] The law does not specify the concept of "proper performance of duties" by directors.
[50] *Parliamentary history I* 2010/11, 31 763, nr. c, p. 5, 6.

collective responsibility entails that, besides the specific tasks assigned to a specific director, each director – whether an executive director or non-executive director – has an individual duty to cooperate with his co-directors, to supervise his co-directors and to take action when he foresees or should foresee possible improper performance of duties by his co-directors.

2.2.3 The "serious blame" standard

In 1997, the Supreme Court rendered its judgment in the case *Staleman/Van de Ven* in which it introduced the serious blame standard for internal liability.[51] It ruled that the liability of directors only occurs if they can be "seriously blamed" which, according to the Supreme Court, must be assessed by taking into account all the relevant circumstances. These circumstances include, according to the Supreme Court:

(i) the nature of the activities carried out by the legal entity;
(ii) the resulting risks generally related to those activities;
(iii) the divisions of tasks within the board;
(iv) any guidelines applicable to the management;
(v) the information that was available to the director or that ought to have been available at the time of his actions; and
(vi) the insight and diligence that may be expected from a director who is capable of his tasks and who fulfills these tasks meticulously.

Hence, as a benchmark for internal liability of directors, the director involved or one of his co-directors must be "seriously blamed". This serious blame standard is considered a subjective criterion. To interpret this criterion, it requires an objective test that is assessed in light of all the circumstances of the case, which are stated above under (i) to (vi). Hence, an objective test is applied to interpret the subjective criterion of "the serious blame standard".[52] Regarding circumstance (vi), the performance of duties of a director is assessed by comparing his actions to how an average reasonable and capable director would have acted under the same circumstances as the circumstances that occurred during the performance that is subject to investigation.[53] This standard of conduct follows both from the parliamentary history[54] and from the Supreme Court in the *Laurus* case.[55] The "average reasonable and capable director" of the *Laurus* case refers to the way in which a director must perform his duties (i.e. "properly"), and not to the subjective serious blame standard.

In legal literature, there has been extensive discussion about the meaning of the term "serious blame" in the context of liability of directors. The different opinions of authors regarding the serious blame standard will be reflected below. However, the fact that there has been so much debate regarding this subject, illustrates that the Supreme Court's choice of the words "serious blame" in *Staleman/Van de Ven* is rather unfortunate. In addition, according to legal scholars, there is no consensus on whether the "serious blame" standard should be used as the applied standard for internal liability

[51] Supreme Court 10 January 1997, ECLI:NL:HR:1997:ZC2243, *NJ* 1997/360 with annotation by J.M.M. Maeijer and *JOR* 1997/29 (*Staleman/Van de Ven*) para 3.3.1.
[52] The application of this objective test is reflected in the parliamentary history to article 2:9 DCC.
[53] De objectieve 'maatman-bestuurder'.
[54] Parliamentary history II 1983/84, 16 631, nr. 9, p. 2 and Parliamentary history II 2008/09, 31 763, nr. 3, p. 9.
[55] Supreme Court 8 April 2005, ECLI:NL:HR:2005:AS5010, *NJ* 2006/443 with annotation by G. van Solinge; *JOR* 2005/119 with annotation by M. Brink (*Laurus*).

of directors.[56] Schild advocates this serious blame standard, since the conclusion of A-G Mok[57] in *Staleman/Van de Ven* states the Supreme Court had to make a deliberate and even fundamental choice.[58] It therewith explicitly chose the words "serious blame". Because of this decision, Schild is of the opinion that the serious blame standard is correctly included in article 2:9 DCC.[59] To the contrary of Schild, Westenbroek believes that the Supreme Court did not make a fundamental choice in *Staleman/Van de Ven*.[60] He is of the opinion that this standard does not fit into the liability framework of directors and it cannot be properly aligned with the parliamentary history.[61] The reason for this is that, according to Westenbroek, a standard for liability is already embedded in the words "(im)proper performance of duties" of article 2:9 DCC.[62] Lastly, according to Strik, the terminology "serious blame" should be used as an attribution standard for the individual director.[63] It should no longer refer to the assessment of the violation of the standard of conduct "proper performance of duties". She argues that the term "serious blame" should indicate a degree of guilt.[64]

While the judgment of *Staleman/Van de Ven* was delivered in 1997, it is only since 1 January 2013 that the legislature has codified the serious blame standard by changing article 2:9 DCC. This was a consequence of the entry into force of the Act on Management and Supervision.[65]

As I mentioned in the introductory chapter, poor cyber-security management is embedded in my research question. In addition, as stated in the second paragraph of this chapter, cyber-security management is covered by risk management. Because of this, it is of importance to discuss significant case law pertaining to failing risk management.

2.2.4 Internal liability of directors regarding failing risk management

As stated above, the DCC does not provide any clarification on what is meant by a "proper performance of duties", since it does not provide any objective standards. Case law, however, may help to acquire some insights to ascertain in what situations improper performance of duties of directors may be established. The cases I will outline

---

[56] WA Westenbroek, 'Het Trustkantoor Als Bestuurder En "Omgaan" in Het Bestuurdersaansprakelijkheidsrecht (HR 30 Maart 2018, ECLI:NL:HR:2018:470)' (2018) 26 Onderneming en Financiering 14 <http://www.bjutijdschriften.nl/doi/10.5553/OenF/157012472018026003003> accessed 30 October 2019.

[57] See the conclusion of A-G Mok of Supreme Court 10 January 1997, ECLI:NL:HR:1997:ZC2243, *NJ* 1997/360 with annotation by J.M.M. Maeijer (*Staleman/Van de Ven*).

[58] AJP Schild, 'Bestuurdersaansprakelijkheid In Theorie: Bespreking Van Het Proefschrift van Mr WA Westenbroek' [2019] Maandblad voor Vermogensrecht 36-39.

[59] ibid.

[60] WA Westenbroek, 'Bestuurdersaansprakelijkheid in Theorie' (2019) 29 Maandblad voor Vermogensrecht 103 <http://www.bjutijdschriften.nl/doi/10.5553/MvV/157457672019029003004> accessed 2 November 2019; WA Westenbroek, 'Metaalmoeheid Na 88 Jaar "Externe" Bestuurdersaansprakelijkheid En Spaanse Villa, Het Is Tijd Voor Herbezinning: Laat de Ernstig Verwijt Maatstaf Los' (2015) 69 Maandblad voor Vermogensrecht 353-66.

[61] ibid.

[62] ibid.

[63] Daniella Strik, 'Grondslagen Bestuurdersaansprakelijk, Een Maatpak Voor de Boardroom' (thesis, Erasmus University Rotterdam 2010) 166-69; Daniella Strik, 'Ernstige Verwijtbaarheid: Tussen Onrechtmatigheid En Toerekenbaarheid - over de "inkleuring" van Art. 6:162 BW Door Art. 2:9 BW' (2009) 156 Ondernemingsrecht 660.

[64] ibid.

[65] Act of 6 June 2011, *Stb*. 2011, 275 (n 40).

below are examples of improper performance of duties with respect to risk management pursuant to article 2:9 DCC.

The *Ceteco* case[66] was about the board taking decisions without investigating possible risks. The District Court of Utrecht in this case considered that there can be no doubt that any reasonable thinking director of an internationally operating listed company should have investigated, in the given circumstances, whether the size of the organization was still in line with the quality of the underlying business processes, including risk-management processes.[67] It follows that a reasonably thinking director knew or should have known in any case that the size of the company had become too large in relation to the quality of the underlying processes and had thus become effectively unmanageable.[68] This led to the establishment of sufficient serious blame for the directors and they had apparently improperly performed their duties towards *Ceteco*.

Another example is the *Vie d'Or* case[69], in which the Enterprise Division ruled that the administrative organization and internal control of Vie d'Or did not comply with the required standards. As a result, the rights and obligations were recorded incompletely or too late and the insight into the financial position and the results was obscured.

Additional vigilance is appropriate in a situation of growth of a company: organic growth of a company can cause the falling short of systems due to the increased or more diversified scale of activities.[70] An example of such a situation was the *Ahold* case in light of its expansion strategy.[71] The Enterprise Division ruled that there were legitimate reasons to doubt Ahold's proper policy with regard to the supervision of its operating companies, insofar as they relate to the organization and operation of internal control, the operating companies and the reporting thereof to Ahold.[72] More or less the same was decided in the *Laurus* case[73] by the Enterprise Division with regard to the expansion strategy of Laurus.

2.2.5 Exculpation

Article 2:9 paragraph 2 DCC states that exculpation is possible if serious blame cannot be attributed to the individual director in relation to the improper performance of duties and if he also has not been negligent in taking measures to avert the consequences of that improper performance of duties. It is important to note that the question as to whether the director concerned has been negligent in taking measures to avert the consequences of improper performance of duties will not always be easy to answer for a judge. The parliamentary history of article 2:9 DCC states that also where individual directors rely upon the possibility of exculpation it is necessary for the director to prove he cannot be seriously blamed in respect of improper performance of duties.[74]

---

[66] District Court of Utrecht 12 December 2007, ECLI:NL:RBUTR:2007:BB9709, *JOR* 2008/10 (*Ceteco*).
[67] ibid para 5.105.
[68] ibid para 5.99.
[69] Enterprise Division of the Court of Appeal of Amsterdam 9 July 1998, *JOR* 1998/122 (*Vie d'Or*).
[70] Strik, 'Grondslagen Bestuurdersaansprakelijk, Een Maatpak Voor de Boardroom' (n 63) 285, 286.
[71] Enterprise Division of the Court of Appeal of Amsterdam 6 January 2005, ECLI:NL:GHAMS:2005:AR8831, *JOR* 2005/6 with annotation by M.W. Josephus Jitta (*Ahold*).
[72] ibid para 3.40.
[73] Enterprise Division of the Court of Appeal of Amsterdam 16 October 2003, ECLI:NL:GHAMS:2003:AM1450, *JOR* 2003/260 (*Laurus*).
[74] *Parliamentary history I* 2010/11, 31 763, nr. c, p. 5.

Since January 2013, the introduction of the revision of article 2:9 DCC, it explicitly envisages the possibility to provide, "by or pursuant to" the articles of association (or the law), a division of tasks for the board.[75] Hence, the revision of article 2:9 DCC has created the possibility to include a division of tasks in the articles of association. Based on the parliamentary history, this division of tasks is a viewpoint as regards the question as to whether or not an individual director can exculpate himself from liability for improper performance of duties.[76] The Supreme Court in the case *Staleman/Van de Ven* had already considered this. To that extent, the legislature only codified existing case law. According to Strik, the division of tasks within the set of relevant circumstances, which were introduced in *Staleman/Van de Ven*, outweighs others.[77] Furthermore, also according to Maeijer and Dortmond, a division of tasks could play a role in individual exculpation.[78] However, Maeijer, Schild and Timmerman did not enter into the question on *how* the division of tasks plays a role in exculpation.[79] Lastly, it is important to note that Van Schilfgaarde and Glasz argue that, according to the wordings of article 2:9 DCC, directors are not severally liable for matters that do not belong to their employment. As a result, the issue of individual exculpation does not need to be addressed according to these two authors.[80]

In addition, Schild and Timmerman state that, despite any division of tasks between the directors, all directors remain responsible for the general affairs, the financial affairs and important issues relating to the legal entity.[81] On top of this, a director can never exculpate himself from "the general affairs".[82] No clear definition of this concept can be found in the parliamentary history. Here one may think of fundamental issues that must always be considered to be the responsibility of all directors. As mentioned earlier, it is important to note that risk management is considered a core task of the directors.[83] The starting point of core tasks is that all directors are collectively responsible for these kinds of tasks.[84] In addition, a director can hardly ever exculpate himself from core tasks.[85] This is of great importance for my research, since cyber-security management fall under risk management, which is

[75] This also ties in with the distinction between executive and non-executive directors that the legislator has introduced to the so-called "one-tier board".
[76] *Parliamentary history I* 2010/11, 31 763, nr. c, p. 5-6.
[77] Daniella Strik, 'One Tier Board En Aansprakelijkheid' (2012) 91 Ondernemingsrecht 496-500.
[78] JM. Maeijer, *Mr. C. Asser's Handleiding Tot de Beoefening van Het Nederlands Burgerlijk Recht. 2. Vertegenwoordiging En Rechtspersoon. Deel III. De Naamloze En de Besloten Vennootschap: Hoofdstuk X, XI, XII En XIV* (Kluwer 2000); District Court Rotterdam 17 June 1999, *JOR* 1999/244 with annotation by F.J.P. Van den Ingh; PJ Dortmond, 'De One-Tier Board in Een Nederlandse Vennootschap' in LJ Hijmans van den Bergh (ed), *Nederlands ondernemingsrecht in grensoverschrijdend perspectief* (Instituut voor Ondernemingsrecht, Kluwer 2003).
[79] G Van Solinge and MP Nieuwe Weme, *Mr. C. Assers Handleiding Tot de Beoefening van Het Nederlands Burgerlijk Recht. 2. Rechtspersonenrecht. Deel II. De Naamloze En Besloten Vennootschap* (Kluwer 2013); AJP Schild and L Timmerman, 'Het Nieuwe Art 2:9 BW, Uitgelegd Voor Gewone Bestuurders' [2014] Weekblad voor Privaatrecht, Notariaat en Registratie 270.
[80] Daniella Strik, 'Aansprakelijkheid van Niet-Uitvoerende Bestuursleden: You Cannot Have Your Cake and Eat It' [2003] Ondernemingsrecht 370.
[81] Schild and Timmerman (n 79) 273.
[82] Article 2:9 paragraph 2 DCC, first sentence.
[83] Heleen Kersten, 'De Rol van de Auditcommissie Bij Het Toezicht Door de Raad van Commissarissen Op Risicobeheer' (2016) 14 Ondernemingsrecht 56.
[84] Strik, 'Grondslagen Bestuurdersaansprakelijk, Een Maatpak Voor de Boardroom' (n 63) 275; This is also reflected in the Code with regard to directors having to issue the so-called "in control"-statement on risk management for the financial reporting process in the annual report.
[85] ibid 343.

considered a core task.[86] As a consequence, according to Schild and Timmerman, other directors cannot exculpate themselves from liability, as a result of collective responsibility, by relying upon their divisions of tasks when it concerns a core task.[87]

The remaining question regarding the issue of exculpation is as to whether a director can also exculpate himself by referring to a division of tasks that is *not* laid down in the articles of association. After all, article 2:9 DCC paragraph 1 DCC requires a division of tasks that is regulated "by or pursuant to the articles of association". If the previous question has to be answered in the positive, a judge should take into account a division of tasks that has taken place on a practical level. Case law shows that a non-formalized division of tasks should be involved in the assessment.[88]

2.2.6 One-tier board and exculpation

As mentioned in the introduction of this chapter, besides the two-tier board option, there is the possibility to choose a one-tier board structure in the Netherlands since 2013. It is important to note that, besides executive directors, non-executive directors directly fall within the scope of article 2:9 DCC. This is due to the usage of the words "*each* director" in paragraph 1 of article 2:9 DCC. Hence, a non-executive director is a full member of the board, and therewith duties within the board also belong to him. As a result of this, a non-executive director can also be liable for the consequences of the performance of duties. A non-executive director can therefore be liable as a director on the basis of article 2:9 DCC. It must be noted, however, that this is only the case if a non-executive director performs executive tasks.[89] In the case he only performs supervisory tasks, a non-executive will fall under the same liability-regime as a Supervisory Board member.[90] As mentioned in the introductory chapter, this liability-regime is beyond the scope of my research. In this paragraph, non-executive directors performing executive tasks are my reference point. Since both executive and non-executive directors are included in article 2:9 DCC, improper performance of duties by a director leads to the liability of *all* executive and non-executive directors. The reason for this can be found in the collective responsibility of directors.

If a non-executive director is part of the board, the question arises as to what extent he can rely on the division of tasks determined within the board to exculpate himself from liability. This division of tasks can be laid down in the articles of association.[91] What has been agreed upon the division of tasks – whether formally or informally – among non-executive directors is therefore of crucial importance for an exculpation possibility.[92] The tasks of non-executive directors, who are not only involved in supervisory tasks, can be compared to the tasks of directors in a two-tier

---

[86] Schild and Timmerman (n 79) 273.
[87] Schild and Timmerman (n 79) 273; M Olaerts, 'Bestuurdersaansprakelijkheid in Het Vernieuwde (BV-)Recht' [2012] Tijdschrift voor Vennootschapsrecht, Rechtspersonenrecht en Ondernemingsbestuur 170.
[88] District Court of Rotterdam 14 July 2010, ECLI:NL:RBROT:2010:BN7874, *JRV* 2011/14; District Court of The Hague 28 April 2016, ECLI:NL:RBDHA:2016:8601, *RO* 2017/17.
[89] Strik, 'Aansprakelijkheid van Niet-Uitvoerende Bestuursleden: You Cannot Have Your Cake and Eat It' (n 80) 6, 7.
[90] CEJM Hanegraaf, 'De One-Tier Board En de Bestuurdersaansprakelijkheid van Niet-Uitvoerende Bestuurders' (2019) 5 Maandblad voor Ondernemingsrecht 18 <http://www.bjutijdschriften.nl/doi/10.5553/MvO/245231352019005102003> accessed 20 December 2019.
[91] Article 2:239a(1) DCC.
[92] District Court Rotterdam 17 June 1999, *JOR* 1999/244 with annotation by F.J.P. van den Ingh, para 3.11.b.

board. Hence, a more extensive range of tasks, by which I mean executive tasks for non-executive directors, requires greater responsibility and, by extension, broader liability: as a director.[93] This implies that also a non-executive director, who performs executive tasks, cannot exculpate himself from core tasks, such as risk management. Hence, non-executive directors should be treated equally to executive directors regarding exculpation possibilities.[94]

2.2.7 Proposal regarding article 2:9 DCC

The Minister of Justice filed a proposal for a bill: the Act on Management and Supervision of Legal Entities[95], containing a new article 2:9 DCC.[96] To the possibilities for a division of tasks does not change anything in substance, according to the parliamentary history.[97] The parliamentary history shows that (i) a division of tasks does not change the joint liability, (ii) the starting point of collective responsibility, in principle, leads to joint and several liability, also in the case of divided tasks and (iii) exculpation is possible, whereby the division of tasks can play a role.[98] This bill is formulated in such a way that it seems that tasks, which are assigned to others, are no longer the responsibility of the remaining directors. Verdam illustrates the consequence of this change in legislative text by stating that when an IT-policy is attributed to director A, the remaining directors are not responsible for the accompanied crucial transition to a new IT-system by director A.[99] However, this reasoning disregards the principle of collective responsibility. After all, collective responsibility implies that a division of tasks does not affect the joint liability of directors.

About the task allocation rule is noted: "The rule is of particular importance for legal entities with a monistic (one-tier) board system. In case of a legal entity with a monistic board system, there must be a clear division of tasks between the executive and non-executive directors (see also article 2:9a paragraph 1 DCC); this is to prevent the non-executive directors from being responsible for the management in the same way as the executive directors."[100] It seems that the legislator envisages the possibility for non-executive directors of a one-tier board to have recourse to a clear division of tasks in case they want to free themselves from liability.[101]

2.2.8 Corporate Governance as legal basis for internal liability

There are two grounds for internal liability of directors based on the Corporate Governance Code[102] (henceforth "Code"). First of all, in case a director of a listed

---

[93] Strik, 'Aansprakelijkheid van Niet-Uitvoerende Bestuursleden: You Cannot Have Your Cake and Eat It' (n 80) 7.
[94] JB Wezeman, 'Uitvoerende Bestuurders En Niet Uitvoerende Bestuurders van Naamloze En Besloten Vennootschappen' [2009] Ars Aequi 112.
[95] *Parliamentary Documents II* 2015/16, 34 491, nr. 2 (legislative proposal). On 8 June 2016 the Dutch Ministry of Justice filed a legislative proposal on the Management and Supervision of Legal Entities for discussion and adoption with Dutch Parliament. After a two-year pause, the Dutch Parliament submitted an amended bill on Management and Supervision of Legal Entities in November 2018. This bill has not been passed yet.
[96] See Appendix D.
[97] *Parliamentary Documents II* 2015/16, 34 491, nr. 3 (MvT), p. 11.
[98] *Parliamentary Documents* 31 763, nr. c, p. 5, 6.
[99] AF Verdam, 'Over de Bestuurstaak, Taakverdeling En Individuele Verantwoordelijkheid van de Bestuurder' (2017) 7135 Weekblad voor Privaatrecht, Notariaat en Registratie 97-100.
[100] *Parliamentary Documents II* 2015/16, 34 491, nr. 3 (MvT), p. 11.
[101] Maarten Mussche, 'De Informele Taakverdeling Als Disculpatieverweer' in Bastiaan Assink and others (eds), *De vele gezichten van Maarten Kroeze's 'bange bestuurders'* (Wolters Kluwer 2017).
[102] Monitoring Committee Corporate Governance Code (n 41).

company or a non-listed company, which declares to comply with the Code, violates the Code this can lead to internal liability of directors based on article 2:9 DCC.[103] Secondly, the reasonableness standard ("proper" performance of duties) for liability of directors is defined by reasonableness and fairness pursuant to article 2:8 DCC, which in turn can be interpreted by the Code. In that case there is mutual commitment to the Code of the interested party as referred to in article 2:8 DCC.[104] Because of this, the principles of the Code are legally enforceable.[105] This legal enforceability of the obligations of the Code was further confirmed by the Supreme Court in the *Versatel* judgment.[106] After this judgment it was said that the Code could be aligned with the law and articles of association with regard to legal force.[107] Hence, the Code can be a basis for internal liability of directors.

2.3 External liability of directors

2.3.1 The "personal" serious blame standard

Besides internal liability of directors, there is external liability of directors towards third parties. In my research the meaning of third parties is limited to individual shareholders of a company. The general basis for liability of directors towards third parties is the unlawful act based on article 6:162 DCC.[108] A director, as a representative of the company, is, in principle, not liable to third parties. The reason for this is that he does not act on his own behalf, but on behalf of the company. However, in some instances an unlawful act may be attributed to him personally.

The Supreme Court has established a clear connection between article 6:162 DCC and article 2:9 DCC. It did so by rendering the landmark *Ontvanger/Roelofson*[109] case in which it introduced the serious blame standard into the legal framework for the external liability of directors. The Supreme Court ruled that in general it is only then assumed that a director acted unlawfully towards the creditor of the company if, partly due to its obligation to proper performance of his duties referred to in article 2:9 DCC, a sufficiently serious blame may be attributed to him.[110] Because of this judgment, the rules for internal liability and external liability were now converged due to the usage of the same standard for both forms of liability. Besides this *Ontvanger/Roelofson* case, there has been other extensive case law that interpreted the application of article 6:162 DCC in conjunction with article 2:9 DCC. The *Ontvanger/Roelofsen* judgment will be discussed more in detail below as well as other case law. In two judgments, issued in September 2014[111], the Supreme Court has formulated a general liability standard for external liability and therewith again emphasized that there is a high threshold for

---

[103] RTL Vaessen, 'Bestuurdersaansprakelijkheid En Corporate Governance' (2017) 15 Maandblad voor Vermogensrecht 324 <http://www.bjutijdschriften.nl/doi/10.5553/MvV/157457672017015012003> accessed 21 December.
[104] ibid.
[105] ibid.
[106] Supreme Court 14 September 2007, ECLI:NL:HR:2007:BA4887, *NJ* 2007/612 with annotation by J.M.M. Maeijer (*Versatel*); see also Supreme Court 21 February 2003, ECLI:NL:PHR:2003:AF1486, *NJ* 2003/182 with annotation by J.M.M. Maeijer (*HBG*).
[107] ibid.
[108] See Appendix B.
[109] Supreme Court 8 December 2006, ECLI:NL:HR:2006:AZ0758, *NJ* 2006/659 with annotation by J.M.M Maeijer (*Ontvanger/Roelofsen*).
[110] ibid para 3.5.
[111] Supreme Court 5 September 2014, ECLI:NL:HR:2014:2628, *NJ* 2015/21 with annotation by P. van Schilfgaarde and *JOR* 2014/296 with annotation by M.J. Kroeze (*Hezemans Air*) and Supreme Court 5 September 2014, ECLI:NL:HR:2014:2627, *NJ* 2015/22 with annotation by P. van Schilfgaarde and *JOR* 2014/325 with annotation by S.C.J.J. Kortmann (*RCI/Kastrop*).

liability of directors. A director only commits an unlawful act towards a third party if a "personal" serious blame can be attributed to this director.[112] This standard differs from the standard of article 2:9 DCC in that a "personal" serious blame must be attributed to the director. This is not required in the event of a liability action pursuant to article 2:9 DCC. The reason for this is that directors, in principle, are jointly and severally liable towards the legal entity for the improper performance of their duties.

The "personal" serious blame standard was not entirely unexpected. It is rather the somewhat casuistic case law that resulted in the standard coming to the fore.[113] Below, I will outline the development of this serious blame standard towards shareholders. Subsequently I will discuss the "September judgments".

2.3.2 Development of liability of directors towards shareholders

In 2008, the Supreme Court rendered the *Willemsen Beheer/NOM*[114] case. This judgment concerned the liability of the director towards a shareholder. In this case, the Supreme Court also introduced the "serious blame" standard as the applicable standard for shareholders' claims.[115] It considered that in view of the deliberate involvement of a shareholder with the legal entity, the serious blame standard of article 2:9 DCC is justified as a high threshold for liability of directors. Hence, the Supreme Court ruled that the applied high threshold for internal liability (article 2:9 DCC) also applies in liability proceedings brought by individual shareholders.[116] It further considered that directors, in principle, are liable towards individual shareholders for actions that contravene provisions in the articles of association that aim to protect the individual shareholders. This is also aligned with the rules for internal liability.

In the fall of 2014 – in the "September judgments"[117] – the Supreme Court elaborated on the cases *Ontvanger/Roelofsen* and *Willemsen Beheer/NOM*. In these judgments, the Supreme Court seems to have firmly chosen for the wording "personal serious blame" as the standard for all cases of external liability. It can be inferred from this that the standard from *Otvanger/Roelofsen* (for creditors) and the standard from *Willemsen Beheer/NOM* (for shareholders) were tied together. In the September judgments, the Supreme Court ruled that external liability of directors requires serious blame to be *personally* attributed to a director.[118] This again shows there is a high threshold for liability. The Supreme Court considered that the rationale behind this high threshold is to prevent directors from being led by defensive motives.[119] In other words:

---

[112] In my view, in this context, "third parties" should be understood to mean anyone other than the legal entity itself (who can act on the basis of article 2:9 DCC). The term "third parties" therefore also includes shareholders.

[113] AJP Schild, 'Ontwikkelingen Bestuurdersaansprakelijkheid: Een Overzicht' (2015) 7087 Weekblad voor Privaatrecht, Notariaat en Registratie 1049.

[114] Supreme Court 20 June 2008, ECLI:NL:HR:2008:BC4959, *NJ* 2009/21 with annotation by J.M.M. Maeijer and H.J. Snijders (*Willemsen Beheer/NOM*).

[115] ibid; the connection with article 2:9 DCC was explicitly sought in para 5.3.

[116] In view of the self-chosen involvement of individual shareholders in the course of business within the company, the standards of reasonableness and fairness of article 2:8 paragraph 1 DCC entail that the high threshold of article 2:9 DCC is accordingly applicable in the event of liability proceedings brought by an individual shareholder against a director.

[117] Supreme Court 5 September 2014, ECLI:NL:HR:2014:2628, *NJ* 2015/21 with annotation by P. van Schilfgaarde and *JOR* 2014/296 with annotation by M.J. Kroeze (*Hezemans Air*); Supreme Court 5 September 2014, ECLI:NL:HR:2014:2627, *NJ* 2015/22 with annotation by P. van Schilfgaarde and *JOR* 2014/325 with annotation by S.C.J.J. Kortmann (*RCI/Kastrop*).

[118] ibid para 3.5.2; ibid para 4.2, 4.3.

[119] ibid.

do not dare to take risks. The question as to whether a director can be personally blamed has to be answered on the basis of all the circumstances of the case.

It is important to consider the fact that the "September judgments" do not recall that when a shareholder asserts a claim against a director, it is of importance to ascertain to what extent there may be "derivative damage". This will therefore be discussed in the next chapter.

Lastly, it is important to note that relatively recently the Supreme Court rendered a case concerning the principle of collective responsibility regarding external liability of directors.[120] In this case, the Supreme Court ruled that the principle of collective responsibility and the influence of the division of tasks in that context, as applied within the framework of internal liability of directors pursuant to article 2:9 DCC, do not apply to external liability of directors under article 6:162 DCC.[121] For a director to be liable towards third parties, *personal* serious blame has to be attributed to the director. In addition, the Supreme Court considered that it is in itself correct that also the insufficient supervision of the performance of duties by a co-director may, under certain circumstances, entail the personal liability of a director.[122]

2.4 Sub-conclusion

Article 2:9 DCC stipulates that a director is obliged to a proper performance of his duties. It can be deduced from this that a director has the general duty to properly perform his duties. In 1997, the Supreme Court introduced the serious blame standard for internal liability. It ruled that liability of the director towards the legal entity could only arise if the so-called "serious blame" can be attributed to the director. It formulated this standard in the *Staleman/Van de Ven* case, which is now considered a landmark judgment of the Supreme Court for internal liability of directors. With respect to the principle of collective responsibility, the system of article 2:9 DCC entails that if one director improperly performs his duties, in principle all directors are liable unless one can exculpate himself. However, directors cannot exculpate themselves from core tasks, which include (cyber-security) risk management. It is important to reiterate that article 2:9 DCC applies to both one-tier board structures and two-tier board structures. This implies that executive and non-executive directors are treated equally with regard to exculpation possibilities. Therefore, there is no need to choose for a one-tier board structure respectively two-board structure regarding the liability regime of directors. In addition, besides liability of directors based on article 2:9 DCC, acting in violation of the Code can also be a basis for internal liability of directors. However, this is only the case when listed companies are in charge or when the board of a non-listed company has declared to comply with the Code.

In 2006, the Supreme Court rendered its judgment in the case *Ontvanger/Roelofson* in which it introduced the serious blame standard for external liability of directors (article 6:162 DCC). In the "September judgments", the Supreme Court reaffirmed the serious blame standard for external liability of directors and further substantiated this standard to *personal* serious blame. In addition, in these judgments, the Supreme Court again stressed that there is a high threshold for liability of directors.

---

[120] Supreme Court 30 March 2018, ECLI:NL:HR:2018:470, *NJ* 2018/330 with annotation by P. van Schilfgaarde (*Eisers/TMF c.s.*).
[121] ibid para 3.3.1-3.3.4.
[122] ibid para 3.5.2.

3. Possibilities for a shareholder to claim derivative damage

3.1 Introduction

A great many recent cyber-incidents show that shareholders are suffering enormous damage because of sharp declines in share prices due to these incidents.[123] Derivative damage is the damage that a shareholder suffers due to a depreciation of his shares as a result of damage caused to the company.[124] The question arises as to whether under Dutch law a shareholder can recover this derivative damage from negligent directors. There are two ways in which a shareholder can claim compensation for derivative damage. First of all, a shareholder can indirectly claim compensation for derivative damage through the company itself pursuant to article 2:9 DCC. Secondly, by stating a specific due diligence standard has been violated, a shareholder could directly claim compensation for derivative damage against a director pursuant to article 6:162 DCC. I will discuss both possibilities in this chapter. Lastly, I will set out what kinds of damage a shareholder can possibly claim as derivative damage.

3.2 Starting point: no direct compensation for derivative damage

Shareholders have a financial interest in the company's assets. If the company suffers damage due to improper performance of duties by its directors (article 2:9 DCC), the value of the shares will most likely decline. This reduces the shareholders' equity. This depreciation of shares is also referred to as derivative damage.[125] Hence, a shareholder that suffered a depreciation of his shares, as the result of misconduct of a director, can assert a claim against that director for compensation. As *Staleman/Van de Ven* was a landmark judgment for internal liability of directors, a groundbreaking judgment with regard to derivative damage was the *Poot/ABP* case.[126]

The Supreme Court in *Poot/ABP* ruled that shareholders cannot recover derivative damage directly from directors.[127] The reason for this is that a shareholder cannot claim any damage that could also be claimed from the director by the company (legal entity) itself. The company itself will claim the damage that it suffers as a result of the actions of the director(s). This protects the interests of *all* shareholders and not just those of the litigating shareholder(s). An exception is possible in only a few cases, namely derivative damage is only eligible for compensation if a shareholder can demonstrate a violation of a specific due diligence standard by a director.[128] This is the case, for

---

[123] Bischoff (n 7).

[124] Kroeze (n 31) 17; Kroeze uses a factual approach to the concept of derivative damage. In other words, whether there is derivative damage only depends on the way in which the damage was suffered (through the company). Most authors agree with Kroeze's definition or endorse a similar definition. See also L Timmerman, 'Kan Een Aandeelhouder of Vennootschapsschuldeiser Afgeleide Schade Vorderen?' (1998) 50 Maandblad voor Ondernemingsrecht en rechtspersonen 97; Frank Veenstra, 'De Aandeelhouder En Zijn Afgeleide Schade' (2008) 4 Ondernemingsrecht 140; L Timmerman, 'Pragmatisch Denken over Afgeleide Schade' (2013) 6962 Weekblad voor Privaatrecht, Notariaat en Registratie 115; AE Goossens, 'De Mogelijkheden Voor Vergoeding van Afgeleide Schade Verruimd' (2016) 14 Maandblad voor Vermogensrecht 278 <http://www.bjutijdschriften.nl/doi/10.5553/MvV/157457672016014010004> accessed 23 December 2019; WJ Oostwouder, 'Actualiteiten "Afgeleide Schade"' (2018) 26 Onderneming en Financiering 5 <http://www.bjutijdschriften.nl/doi/10.5553/OenF/157012472018026004002> accessed 23 December 2019.

[125] ibid.

[126] Supreme Court 2 December 1994, ECLI:NL:HR:1994:ZC1564, *NJ* 1995/288 with annotation by J.M.M. Maeijer (*Poot/ABP*).

[127] ibid.

[128] ibid para 3.4.3.

example, if there has been a violation of a provision in the articles of association that is intended to protect the interest of the shareholder.[129] Such default establishes, in principle, the liability of a director towards that individual shareholder.[130] Hence, since the *Poot/ABP* judgment of 1994, the Supreme Court has confirmed the prevailing doctrine in literature and case law on derivative damage.[131] In conclusion, the following three important principles can be derived from the judgment of the Supreme Court in *Poot/ABP*:

1) The starting point is that only the company has the right to claim compensation for the damage caused to it by a director[132];
2) The shareholder does not, in principle, have any right to claim derivative damage[133];
3) The shareholder only accrues his own claim if the director has breached a specific due diligence standard towards the shareholder.[134]

As mentioned in the previous chapter, both internal and external liability require that serious blame be attributable to a director. The starting point of this chapter is that a shareholder is of the opinion that the negligent director(s) can be seriously blamed. Firstly, I will elaborate on the way a shareholder can bypass the first principle, which is considered the main principle from the *Poot/ABP* judgment. Thereafter, the way in which a shareholder himself can bring proceedings against a director will be set out.

3.3 Shareholder forcing company based on article 2:9 DCC

In this paragraph I will go into principle 1, which states that only the company has the right to claim compensation for the damage caused to it by a director. If a director of a company falls short in the proper performance of his duties (article 2:9 DCC), only the company (and not also the shareholder) has the right to address the director pursuant to article 2:9 DCC. The reason for this is that in the case of derivative damage, it is for the company itself, in order to protect the interests of all those who have an interest in maintaining its assets, to claim compensation for the damage caused.[135]A shareholder has every interest in the company making the decision to take action against the director. The reason for this is to be compensated for derivative damage. However, the director, with whom the dispute exists, will not be inclined to hold himself liable. It is important to note that decision-making of the company is done by the board, which consists of directors. This being said, there are two ways in which a shareholder, by means of the annual general meeting (henceforth "AGM"), can force a company to bring proceedings against a director based on article 2:9 DCC.

First of all, the conflict-of-interest-rule offers the possibility to the AGM to pass a resolution about bringing a claim against a director. A director does not participate in

[129] Supreme Court 20 June 2008, ECLI:NL:HR:2008:BC4959, *NJ* 2009/21 with annotation by J.M.M. Maeijer and H.J. Snijders (*Willemsen Beheer/NOM*) para 5.4.
[130] Supreme Court 29 November 2002, ECLI:NL:HR:2002:AE7011**,** *NJ* 2003/55, with annotation by J.M.M. Maeijer (*Schwandt/Berghuizer Papierfabriek*) para 3.4.5.
[131] Kroeze (n 31) 4.
[132] Supreme Court 16 February 2007, ECLI:NL:HR:2007:AZ0419, *NJ* 2007/256 with annotation by J.M.M. Maeijer (*Tuin Beheer*).
[133] Supreme Court 2 December 1994, ECLI:NL:HR:1994:ZC1564, *NJ* 1995/288 with annotation by J.M.M. Maeijer (*Poot/ABP*) para 3.4.1.
[134] ibid para 3.4.3.
[135] ibid para 3.4.1-3.4.3.

the deliberations and decision-making if he has a direct or indirect personal interest that conflicts with the corporate interest.[136] In 2013, this conflict-of-interest-rule has been introduced by the Act on Supervision and Management.[137] When a director does not participate in the deliberations and decision-making because he has a conflict of interest, no board decision can be taken. In this event, the decision is made by the Supervisory Board. In the absence of a Supervisory Board (which is not a mandatory body, except for a two-tier board company) the resolution is passed by the AGM, unless the articles of association provide otherwise. Hence, this can be the case for a one-tier board structure.

In literature, various authors state that the AGM *as such* may decide to hold directors liable under article 2:9 DCC.[138] This is considered the second possibility for a shareholder to force a company to bring proceedings against a director based on article 2:9 DCC. This possibility is supported in various ways. The law does not explicitly state who is authorized to hold directors liable towards the company. Huizink believes that the body, who is authorized to grant discharge to directors, is also authorized to decide on whether the company has to take action against one or more directors pursuant to article 2:9 DCC.[139] Huizink is of the opinion that this authority does not fall under the concept of "management" within the meaning of article 2:129/239 paragraph 1 DCC.[140] Timmerman's argument is based on the ratio of the old conflict-of-interest-rule of article 2:146/256 DCC.[141] Kroeze rejects Timmerman's arguments by arguing that the old conflicts-of-interest-rule related to representation and not to decision-making.[142] The authority of the AGM regarding the determination to hold a director liable results from the same ratio as expressed in article 2:146/256 DCC (old). This is in fact, according to Kroeze, that conflicting interests must be prevented to the greatest extent possible.[143] In support of the power of the AGM to decide to hold a director liable, Kroeze relies on article 2:8 paragraph 2 DCC.[144] This article offers the possibility to deviate from the legal division of powers within the company in virtue of reasonableness and fairness.[145] I agree with Kroeze's reasoning. By the standards of reasonableness and fairness it is, after all, unacceptable for the board to have *exclusive* competence over its own or that of one of its board members' liability determination.[146]

It is important to note that, for *both* above-mentioned ways to force a company to bring proceedings against a director based on article 2:9 DCC, only shareholders who reach a quorum in the AGM can force a resolution thereon. The reason for this is that a quorum is needed in the AGM to do so.[147] Resolutions in the AGM are adopted by

[136] Article 2:129 paragraph 5 and 6 DCC for public limited liability companies; article 2:239 paragraph 5 and 6 DCC for private limited liability companies.
[137] Act of 6 June 2011, *Stb*. 2011, 275 (n 40).
[138] Jan Bernd Huizink, 'Bestuurders van Rechtspersonen' (thesis, University of Groningen 1989); L Timmerman, 'Van Afgeleide Schade Naar Afgeleide Actie' in AFJA Leijten (ed), *Conflicten rondom de rechtspersoon* (Kluwer 2000); Kroeze (n 24).
[139] Kroeze (n 31) 103; Huizink (n 138) 106, 107.
[140] Kroeze (n 31) 104; Huizink (n 138) 106, 107.
[141] Timmerman, 'Van Afgeleide Schade Naar Afgeleide Actie' (n 140) 22.
[142] Kroeze (n 31) 105.
[143] ibid.
[144] See Appendix E.
[145] Kroeze (n 31) 106.
[146] ibid.
[147] Article 2:120 DCC for public limited liability companies; article 2:230 DCC for private limited liability companies.

an absolute majority of votes, unless a larger majority is prescribed by law or by the articles of association.[148] In practice, for non-listed companies the majority shareholder will be the one to force such a resolution. Hence, in general, a shareholder can use his vote to reach the quorum in the AGM.

To conclude, it is often extremely difficult for a shareholder to urge the company to claim compensation for derivative damage from its director.[149] The reason for this is that the director, with whom the dispute exists, will not be inclined to hold himself liable. In summary, derivative damage is not eligible for indirect compensation, *unless* a shareholder can force a company to bring proceedings against its director through the AGM. For the sake of my research I will assume that a shareholder, by means of a shareholders' resolution in the AGM, can force the company to start proceedings against the directors pursuant to article 2:9 DCC.[150]

In short, internal liability of a director on the grounds of improper performance of duties concerns liability towards the company and not also liability towards the individual shareholder. However, this does not change the fact that a shareholder could directly claim compensation for derivative damage. This possibility is introduced in principle 3, which states that the shareholder only accrues his own right to claim if the director has breached a specific due diligence standard towards the shareholder. I will go into this possibility in the next paragraphs. Derivative damage is eligible for direct compensation if a shareholder can demonstrate a violation of a specific due diligence standard by a director. Below, I will go into this violation.

3.4 Shareholder claiming derivative damage based on article 6:162 DCC

A shareholder can directly bring proceedings against a director pursuant to article 6:162 DCC. As explained above, to do so, a shareholder has to demonstrate a violation of a specific due diligence standard by this director. In this research I will not discuss the other requirements of article 6:162 DCC[151], since these requirements only come into play when a violation of a specific due diligence standard has been established.[152] In addition, literature and case law mainly concentrate on this violation. It is important to note that when a shareholder invokes article 6:162 DCC, this only concerns a claim against one particular director. This is in line with the judgment I mentioned in the last part of the previous chapter. In this judgement the Supreme Court ruled that the principle of collective responsibility does not apply to external liability of directors according to article 6:162 DCC.[153] Below I will elaborate on the violation of a specific due diligence standard.

Kroeze, Timmerman, A-G Hartkamp and A-G Hartlief have extensively discussed the question of *when* derivative damage should be eligible for direct compensation to the

---

[148] ibid.
[149] District Court of The Hague 14 February 2001, *JOR* 2001/90A with annotation by M.J. Kroeze. In this case a shareholder, who held 50% of the company's shares, could start proceedings against the director of the company based on article 2:9 DCC. This is contrary to the judgement in *Poot/ABP*.
[150] Article 2:120 DCC for public limited liability companies; article 2:230 DCC for private limited liability companies.
[151] The requirements that can be deduced from the legal text of article 6:162 DCC are: (i) unlawful act; (ii) accountability; (iii) damage; (iv) causation; (v) relativity; see Appendix B.
[152] Assessing whether the other requirements of the previous footnote are met, is beyond the scope of my research.
[153] Supreme Court 30 March 2018, ECLI:NL:HR:2018:470, *NJ* 2018/330 with annotation by P. van Schilfgaarde (*Eisers/TMF c.s.*) para 3.3.1-3.3.4.

shareholder.[154] It follows from the *Tuin Beheer* judgment that the mere fact that the disadvantage of the shareholder (in this case Tuin Beheer) was foreseeable by the (intentional) conduct of the damage provider to the company does not mean that a specific due diligence standard has been violated towards the shareholder.[155] The Supreme Court added that:

"*If no additional circumstances have been set, such as the intention to disadvantage that shareholder, it cannot be said that the director has thereby also violated a specific due diligence standard towards that shareholder."*[156]

This consideration raises various questions. For example, Veenstra wonders whether this means that a specific due diligence standard can only be breached if the director *intended* to disadvantage the shareholder, or if a less serious form of guilt is sufficient.[157] The Supreme Court mentions intent only as an example of an additional circumstance that may result in a violation of a specific due diligence standard and does not mention this as a separate requirement. In my opinion, a less serious form of guilt is in itself not sufficient. After all, the Supreme Court ruled that the *foreseeability of the disadvantage* of the shareholder did not mean that a specific due diligence standard was violated towards the shareholder.[158]

Thus far, the literature is in line with what has been made clear by the Supreme Court in the case *Poot/APB*: there must in any case be a violation of a specific due diligence standard. It is important to note that, according to Kroeze, when determining whether derivative damage is eligible for direct compensation a judge must take into account the definitive nature of the damage.[159] However, it is not apparent from the case law of the Supreme Court that the shareholder's damage should be definitive and is therewith not considered a necessary condition for assuming a right to compensation for derivative damage.[160] In the *Kessock* judgment, the Supreme Court considered that the right to compensation for derivative damage may, but does not always have to, exist if the derivative damage of the shareholders has become definitive.[161] A case in which the definitive nature of the damage played an important role was in the *Kip/Rabobank* judgment.[162] Briefly summarized, this case concerned the following. Kip (shareholder of Elka Beheer B.V., the parent company of the Elka group) is claiming compensation from Rabobank for the damage it has suffered. It was established that the conduct of Rabobank, consisting of a negligent financing methods and the negligent reduction and

---

[154] Kroeze (n 31); Timmerman, 'Pragmatisch Denken over Afgeleide Schade' (n 124); Supreme Court 15 June 2001, ECLI:NL:PHR:2001:AB2443, *NJ* 2001/573 with annotation by J.M.M. Maeijer (*Chipshol*); Conclusion of A-G Hartlief of Supreme Court 12 October 2018, ECLI:NL:HR:2018:1899, *NJB* 2018/1955 (*Potplantenkwekerij*); Conclusion of A-G Hartlief of Supreme Court 29 September 2017, ECLI:NL:HR:2017:2521 (*Cross Options/ING*).
[155] Supreme Court 16 February 2007, ECLI:NL:HR:2007:AZ0419, *NJ* 2007/256 with annotation by J.M.M. Maeijer (*Tuin Beheer*), para 3.5.
[156] ibid.
[157] Veenstra (n 124) 140-46.
[158] In my opinion, the predictability of the shareholder's disadvantage can be seen as a less serious form of guilt.
[159] Kroeze (n 31) 65, 66.
[160] Conclusion of A-G Hartlief of Supreme Court 29 September 2017, ECLI:NL:HR:2017:2521, (*Cross Options/ING*), para 3.7.
[161] Supreme Court 2 November 2007, ECLI:NL:HR:2007:BB3671, *NJ* 2008/5 with annotation by J.M.M. Maeijer (*Kessock*), para 3.4.
[162] Supreme Court 2 May 1997, ECLI:NL:HR:1997:ZC2365, *NJ* 1997/662 with annotation by J.M.M. Maeijer (*Kip/Rabobank*).

subsequent cancellation of the credit, was unlawful towards the Elka group.[163] The claim of Kip is therefore based on the fact that Rabobank's conduct was not only highly negligent towards the Elka group, but also towards itself and led to it being forced to sell its shares in Elka Beheer B.V. at very low prices.[164]

The Supreme Court ruled that the derivative damage should be compensated to Kip. The Supreme Court considered it of importance that the "*damage caused by the depreciation was definitively charged to their assets and could no longer be eliminated by any compensation from the Bank to the companies of the group*."[165] The derivative damage became definitive after Rabobank pressured Kip to transfer the shares to a third party. The company was dissolved, which means that the board can no longer appeal to Rabobank.[166]

No real benchmark can be derived from the case law of the Supreme Court for directly granting derivative damage. The circumstances of the case play an important role in the assessment. That the possibility exists is in any case clear, although various judgments show that the Supreme Court does not quickly deviate from the main *Poot/ABP*-principle.[167] This principle implies that in the case of derivative damage it is for the company itself to claim compensation for the damage caused to it in order to protect the interests of all those who have an interest in maintaining its assets. Hence, there is, in principle, no compensation in the form of derivative damage for a shareholder in case the company itself has a right to claim. The Supreme Court in *Potplantenkwekerij* judgment considered, however, that the derivative damage suffered by the shareholder (in this case a holding company) was directly eligible for compensation to the shareholder.[168] This judgement is surprising but does not violate the *Poot/ABP*-principle. Unlike in the case underlying the *Poot/ABP* judgment, the *Potplantenkwekerij* judgment stated that the company itself had *no* right to claim, because no unlawful act had been committed towards the company, but towards the shareholder.[169] This in any case shows that there is a brighter outlook for claiming compensation for derivative damage. A recent judgment of the District Court of Central-Netherlands has confirmed this positive development regarding a successful appeal to a violation of a specific due diligence standard.[170]

However, in another recent case the District Court of Central-Netherlands ruled that there had been a violation of a specific due diligence standard, but the establishment of liability of the concerned director collapsed because the serious blame standard was considered not to be fulfilled. In this case, the Court stated that the director can be held liable for damage suffered by the shareholder if (1) the director has violated a specific due diligence standard towards the shareholder and (2) if the director can be seriously blamed for this violation. If this is the case, the director is jointly and severally

[163] ibid para 3.1-3.4.
[164] ibid para 3.2.
[165] ibid para 3.6.
[166] Timmerman, 'Kan Een Aandeelhouder of Vennootschapsschuldeiser Afgeleide Schade Vorderen?' (n 124) 97-101.
[167] G Van Solinge and MP Nieuwe Weme, *Mr. C. Assers Handleiding Tot de Beoefening van Het Nederlands Burgerlijk Recht. 2. Rechtspersonenrecht. Deel II. De Naamloze En Besloten Vennootschap* (Kluwer 2013) 214.
[168] Supreme Court 12 October 2018, ECLI:NL:HR:2018:1899, *JIN* 2018/209 with annotation by E.S. Ebels, R.A.G. de Vaan (*Potplantenkwekerij)* para 3.5.2.
[169] ibid.
[170] District Court Central-Netherlands 22 May 2019, ECLI:NL:RBMNE:2019:2203, *RO* 2019/57.

liable for the damage.[171] Article 2.3. of the management agreement stated that the director performs his duties carefully, diligently and faithfully and to the best of his ability in a manner that is beneficial to the interests of the company and its shareholders. The shareholder is not a party to the management agreement, but the clause has third-party effect. The Court considered this article as a specific due diligence standard.[172] It then ruled that the director had not always acted in a way that was beneficial to the interests of the shareholder and thereby violated the due diligence standard.[173] However, in view of the circumstances of the case, and in particular the role of the shareholder himself, this violation could not be seriously blamed on the director.[174]

3.5 Substantiating derivative damage

Kroeze is of the opinion that derivative damage should, in principle, be estimated on the basis of the amount of damage that the company has suffered. The amount of damage per share therefore depends on the number of issued shares.[175]

In the *Poot/ABP* judgment[176], which I cited earlier, it seems that the Supreme Court supports Kroeze's opinion. According to the Supreme Court in this case, the disadvantage for the shareholder will disappear when the company has successfully established its claim.[177] This implies that if the company suffers damage and this damage is compensated, also the derivative damage to the shareholder is thereby reversed. In the *Chipsol* judgment the Supreme Court points out that a claim for missed price gains from a shareholder is not necessarily refuted. In this judgment, the Supreme Court considered:

"The assessment of the plea must be based on the assumption that if a third party inflicts financial loss on a public or private limited liability company by a (attributable) failure to comply with a contractual obligation towards the company or by conduct that is unlawful towards the company, only the company has a claim for compensation for this damage caused to it. In principle, one or more shareholders of the company do not have a claim for compensation for damage consisting of a reduction in the value of their shares or missed price gain that is the result of the aforementioned shortcoming or unlawful conduct of a third party towards the company. An exception to this rule may be accepted if there is behavior that is specifically careless towards the shareholder."[178]

It can be deduced from this consideration that the Supreme Court considers it possible for a shareholder to also claim missed price gains. However, the Supreme Court does not discuss how these missed price gains should be calculated. In addition, this consideration appears to have been overtaken by later case law. After all the Supreme Court ruled in the *Tuin Beheer* and *Kessock* judgments that derivative damage is the

[171] District Court Central-Netherlands 4 February 2019, ECLI:NL:RBMNE:2019:368, *RO* 2019/48, para 4.4.
[172] ibid para 4.8.
[173] ibid para 4.13.
[174] ibid para 4.14.
[175] Kroeze (n 31) 20-22.
[176] Supreme Court 2 December 1994, ECLI:NL:HR:1994:ZC1564, *NJ* 1995/288 with annotation by J.M.M. Maeijer (*Poot/ABP*).
[177] Supreme Court 2 December 1994, ECLI:NL:HR:1994:ZC1564, *NJ* 1995/288 with annotation by J.M.M. Maeijer (*Poot/ABP*) para 3.4.1.
[178] Supreme Court 15 June 2001, ECLI:NL:PHR:2001:AB2443, *NJ* 2001/573 with annotation by J.M.M. Maeijer (*Chipsol*), para 3.4.2.

damage that a shareholder suffers due to a depreciation of his shares as a result of damage caused to the company.[179] This indicates that it is therefore only necessary to look at the relationship between the damage caused to the company and, as a result of this, the depreciation of shares. In this regard, the law states that the court estimates the extent of the damage in the way which is most consistent with the nature of the damage caused. Where the extent of the damage cannot be assessed exactly, it shall be estimated.[180] Hence, in principle, the damage should be estimated on the basis of the disadvantage suffered by the company. Therefore, in my opinion, when appealing to article 2:9 DCC, a shareholder can only claim compensation for depreciation of his shares.

Lastly, it is important to note that duplication of the compensation in the form of derivative damage must be avoided at all times.[181] This duplication of compensation would arise if both the company and a shareholder claim derivative damage as a result of a depreciation of shares. The danger of duplication of compensation is also one of the reasons why a shareholder has no direct compensation for derivative damage.[182]

3.6 Sub-conclusion

It follows from this chapter that the damage suffered by a shareholder as a consequence of a depreciation of its shares as a result of the damage inflicted on the company, does in principle not accrue a right to direct compensation to the shareholder based on article 2:9 DCC. Hence, the starting point is that only the company is entitled to claim direct compensation for derivative damage. However, a shareholder can force the company, by means of a shareholders' resolution in the AGM, to take action against a director. In addition, a shareholder can seek *direct* compensation for derivative damage based on liability pursuant to article 6:162 DCC. This opportunity to directly claim compensation for derivative damage, however, can only be successful if a shareholder can demonstrate a violation of a specific due diligence standard by one director in particular.

[179] Supreme Court 16 February 2007, ECLI:NL:HR:2007:AZ0419, *NJ* 2007/256 with annotation by J.M.M. Maeijer (*Tuin Beheer*), para 3.3, 3.5; Supreme Court 2 November 2007, ECLI:NL:HR:2007:BB3671, *NJ* 2008/5 with annotation by J.M.M. Maeijer (*Kessock*), para 3.4
[180] Article 6:97 DCC.
[181] Kroeze (n 31) 37-39.
[182] ibid.

4. Duties of a director regarding cyber-risks

4.1 Introduction

In chapter 2, I laid down the general duty of directors with respect to managing the company. This general duty implies that directors should properly perform their duties pursuant to article 2:9 DCC. In this chapter, I will discuss the duties of directors regarding cyber-risks. It is important to note that these more specific duties of directors, which will be set out in this chapter, should be considered in light of the general duty to properly perform their duties. More specifically, the general duty ("proper performance of duties") of article 2:9 DCC is completed by the specific duties of directors with respect to cyber-risks. In chapter 2, I discussed the Code as a legal basis for internal liability of directors. Since the Code prescribes various duties for directors regarding risk management, which covers cyber-security management, these specific duties will be outlined. As mentioned in chapter 2, the Supreme Court in *Staleman/Van de Ven* ruled that any guidelines applicable to the management should be taken into account in the serious blame assessment. In case a cyber-risk has occurred in the Netherlands, two guides with regard to warranting cyber-security are relevant for both giving shape to the general duty of a director to "properly perform his duties" and this serious blame assessment. These two guides have been presented by the CSR in 2017 and 2018, respectively: the Cyber Security Guide for Businesses[183] and the Cyber Security Guide for Board Members[184]. These guides will be set out in this chapter. The relevance of outlining the duties regarding cyber-risks deriving from the Code and these guides is to support the serious blame assessment and therewith possibly establish liability of directors. The reason why I have chosen for the Code and the above-mentioned guides is that they cover relevant duties regarding cyber-security management.

4.2 The role of the board in the Code

In short, the Code applies to Dutch listed companies and is based on the principle of *comply or explain.* In addition, all principles in Chapter 1 through 4 of the Code refer to a two-tier board.[185] Chapter 5, however, only concerns one-tier boards. The board indicates in the management report whether the company complies with the Code. This obligation is laid down in article 2:391 paragraph 5 DCC.[186] If the company (in certain respects) deviates from the Code or the company intends to do so, this must be substantiated. In legal literature it is generally assumed that a certain "reflexive effect" may arise from the Code.[187] This implies that, although the scope of the Code is explicitly limited to listed companies, provisions from the Code may very well be of great relevance for non-listed companies.[188] This is due to the fact that there are

[183] Pieter Wolters and Corjo Jansen, 'Cyber Security Guide for Businesses' (2017) <https://www.cybersecurityraad.nl/binaries/Handreiking_Zorgplichten_ENG_DEF_tcm107-314471.pdf> accessed 2 December 2019.
[184] 'Cybersecurity Guide For Board Members' (2019) <https://www.cybersecurityraad.nl/binaries/Handreiking_Bestuurders_ENG_DEF_2019_tcm107-323477.pdf> acccessed 2 December 2019.
[185] Explanatory note to principle 5.1 Code.
[186] See Appendix F.
[187] Asser/Van Sollinge & Nieuwe Weme 2-IIa 2013/46; Frank Veenstra, 'Aantekeningen Bij Art. 2:346 BW' in Jan Bernd Huizink (ed), *Groene Serie Rechtspersonen* (Wolters Kluwer 2016); SWAM Visée, 'Het Rechtskarakter van de Code Tabaksblat' in FB Falkena and others (eds), *Markten onder toezicht* (Kluwer 2004) 279-87.
[188] Vaessen (n 103) 323; HJ De Kraker, 'Het Praktisch Nut van de Herziene Corporate Governance Code Voor Het MKB' (2017) 44 Bedrijfsjuridische Berichten 152.

numerous non-listed companies that voluntarily adhere to the Code. However, account must be taken of the fact that the Code was written for a relatively homogeneous group of companies and that non-listed companies are more diverse. That is why there has been a reluctance to adopt a "one size fits all"-approach: reflexive effect does not mean that the Code applies to *all* non-listed companies.[189] This is also reflected in case law.[190] While in 2006 the Court of Appeal of Amsterdam ruled that the reflexive effect of the Code applied to non-listed companies[191], in 2016 it decided otherwise.[192]

The most important principle in chapter 1 of the Code, with regard to my research, prescribes that the board must make a risk assessment, on the basis of which it implements and maintains the internal risk management and control systems.[193] To do so, the board is responsible for identifying and managing the risks associated with the strategy and activities of the company.[194] According to Strik, the requirements that may be imposed per company on internal risk management and control systems will depend on the nature of the company and the nature of the risks incurred.[195] In addition, the board should monitor the operation of the internal risk management and control systems and should carry out a systematic assessment of their design and effectiveness at least once a year.[196] It is also important to note that the board must render account to the Supervisory Board about the risk management and control systems.[197] This applies equally to the one-tier board.[198]

4.3 The role of the internal auditor and Audit Committee in the Code

An important role has been assigned to the internal auditor in the Code. The provisions regarding the internal auditor are laid down in principle 1.3 of the Code. The internal auditor falls under the responsibility of the board and has the task of objectively assessing the design and operation of the internal risk management and control systems. The Supervisory Board supervises the internal auditor and maintains regular contact with the person who holds this position. This role will fall upon the Audit Committee. Hence, at least one member of the Supervisory Board joins the Audit Committee. The Audit Committee has an important role to play with regard to risk management in the Code. In accordance with principle 1.5 of the Code, the Supervisory Board supervises the policy of the management board and the general course of affairs of the company and the associated activities. It is explicitly stated that the Supervisory Board focuses on monitoring the effectiveness of the internal risk management and control systems. The Audit Committee prepares the decision-making of the Supervisory Board on the supervision of the integrity and quality of the financial reporting of the company and on the effectiveness of the internal risk management and control systems. The Audit

[189] Josephus MW Jitta, '(G)Een Code Voor Niet-Beursgenoteerde Ondernemingen?' (2007) 135 Ondernemingsrecht 465; De Kraker (n 188) 152, 153.
[190] Enterprise Division of the Court of Appeal of Amsterdam 9 October 2006, *JOR* 2007/9 with annotation by De Groot, Enterprise Division of the Court of Appeal of Amsterdam 9 December 2016, *JOR* 2017/93 with annotation by Fleming.
[191] Enterprise Division of the Court of Appeal of Amsterdam 9 October 2006, *JOR* 2007/9 with annotation by De Groot.
[192] Enterprise Division of the Court of Appeal of Amsterdam 9 December 2016, *JOR* 2017/93 with annotation by Fleming.
[193] Principle 1.2, Best practice provision (henceforth "Bpp") 1.2.1, 1.2.2 Code.
[194] ibid.
[195] Strik, 'Grondslagen Bestuurdersaansprakelijk, Een Maatpak Voor de Boardroom' (n 63) 283, 284.
[196] Bpp 1.2.3 Code.
[197] Bpp 1.4.1 Code.
[198] Bpp 5.1.5 Code.

Committee must supervise the board with regard to the application of information and communication technology by the company.

It is striking that the following phrase was explicitly added to the Code: "including risks relating to cyber security".[199] In particular, it is remarkable that the CSR advised the Monitoring Committee of the Code to add this phrase under duties and responsibilities of the Audit Committee.[200] By dedicating this task to the Audit Committee, it seems that the CSR considers cyber-security to be of such importance that a supervisory body must be entrusted with it. The Monitoring Committee of the Code incorporated this phrase into the Code without any addition, change or modification. In my opinion, it is a very sparse addition. I agree with the content of the advice of the CSR but would have expected that the CSR would have advised to give a more prominent meaning to cyber-security in the Code. It is also worth noting that this cyber-security theme has not been reflected in Chapter 5, which concerns one-tier board structures. To me, it therefore appears that non-executive directors are not charged with such a cyber-security responsibility.

4.4 Accountability for risk management in the Code

In principle 1.4 of the Code, the rules are laid down with regard to accountability for risk management. In accordance with the Best practice provision (henceforth "Bpp") 1.1.4, the board discusses the effectiveness of the design and operation of the internal risk management and control systems with the Audit Committee and reports on this to the Supervisory Board. Finally, the board issues the so-called "in control" statement.[201] The question arises as to whether the board should render account of cyber-risks in the management report.[202] In addition, the same question applies to the Audit Committee in its report.[203] In view of the fact that the Monitoring Committee has underlined the seriousness of cyber-risks by explicitly including this in Bpp 1.5.1, I see no reason to assume that cyber-risks are not covered.

While in the Code a general provision to implement adequate risk management and control systems is laid down for the board, two cyber-security guides have been introduced by the CSR to specifically warrant cyber-security within a company. The first guide concerns the Cyber Security Guide for Businesses.[204] The second guide concerns the Cyber Security Guide for Board Members.[205] Compared to the Code, these guides are neither binding nor enforceable. However, the Supreme Court in the earlier cited judgment *Staleman/Van de Ven* has considered that "any guidelines applicable to the management" is one of the relevant circumstances to be taken into account when assessing whether the serious blame standard is met. In addition, the specific duties for directors deriving from these two guides also determine the general duty ("proper performance of duties") of article 2:9 DCC. Because of this, these Cyber Security Guides are relevant to discuss.

---

[199] Bpp 1.5.1 Code.
[200] Dick Schoof and Eelco Blok, 'Advies Herziening Corporate Governance Code' (Cyber Security Council 2016) <https://www.cybersecurityraad.nl/binaries/Brief%20voorstel%20herziening%20corporate%20governance%20code_tcm107-263139.pdf> accessed 30 November 2019.
[201] Bpp 1.4.2, 1.4.3 Code.
[202] Bpp 1.4.2(i), 1.4.3(iv) Code.
[203] Bpp 1.5.3(iv) Code.
[204] 'Cybersecurity Guide For Businesses' (n 183).
[205] 'Cybersecurity Guide For Board Members' (n 184).

4.5 Cyber Security Guides

I will lay down the most important duties of the Cyber Security Guide for Businesses. First and foremost, companies must take appropriate technical and organizational security measures and regularly check that these measures taken are (still) adequate.[206] Secondly, companies must report breaches involving personal data to the Data Protection Authority within 72 hours (henceforth "data breach notification obligation").[207] Thirdly, following a security incident, companies must take measures to limit the impact of the incident and prevent similar incidents from occurring in the future.[208]

With regard to the Cyber Security Guide for Board Members, it is of great significance that directors put cyber-security in place in their company. This guide presents several ways in which directors can strengthen their management regarding cyber-security. It determines that directors must appoint a portfolio holder on the board.[209] The portfolio holder and the person who is charged with risk management define the objectives and frameworks, facilitate implementation and monitor the progress and enforcement of the cyber-security policy.[210] That does not absolve the other directors of their responsibilities. In addition, the guide states that all directors should have the desired basic knowledge of cyber-security.[211] The position that can have cyber-security in its range of tasks is the Chief Risk Officer (henceforth "CRO").

In an illustrative recent case, the Dutch Central Bank urged the Triodos Bank in the Netherlands to appoint a CRO as member of the board.[212] This shows that the supervisory authority in the financial sector, the Dutch Central Bank, examines whether risk management and therewith cyber-security management is well implemented within companies in this sector. If this answer is in the negative, it advises to do so. It is important to note that by appointing a CRO, who is responsible for risk management and therewith for cyber-security management, the Triodos Bank puts cyber-security in place in its organization.

Regarding these two guides, I would like to make passing reference to US legislation and a very recent US data breach of Facebook. The reason for briefly discussing US legislation is that the US recently drafted a bill that aims for more transparency in the oversight of cyber-risks, which corresponds to the purpose of both guides. In February 2019, the Cybersecurity Disclosure Act was introduced.[213] The main provisions prescribe that listed companies should disclose in its mandatory annual report or annual proxy statement whether any member of its governing body has expertise or experience in cyber-security.

---

[206] 'Cybersecurity Guide For Businesses' (n 183) 10.
[207] ibid.
[208] ibid 17.
[209] 'Cybersecurity Guide For Board Members' (n 184) 7.
[210] ibid.
[211] ibid.
[212] Jan Bonjer, 'Triodos Nomineert Risicodirecteur Na Aandringen DNB' *Financieel Dagblad* (Amsterdam, 13 April 2019) <https://fd.nl/ondernemen/1297194/triodos-nomineert-risicodirecteur-na-aandringen-dnb#%3E> accessed 1 December; 'Carla Van Der Weerdt Nominated As Chief Risk Officer Triodos Bank' (*Triodos Bank*, 13 April 2019) <https://www.triodos.com/press-releases/2019/carla-van-der-weerdt-nominated-as-chief-risk-officer-triodos-bank> accessed 1 December 2019.
[213] 116th Congress, S. 592: Cybersecurity Disclosure Act of 2019 2019 <https://www.congress.gov/bill/116th-congress/senate-bill/592/text> accessed 7 December 2019.

With respect to the recent Facebook data breach, it was announced on 19 December 2019 that more than 267 million Facebook users' IDs, phone numbers, and names were exposed to an online database that could potentially be used for spam and phishing campaigns.[214] This, however, is not the first time Facebook had to deal with its users' data being compromised. I will go into important measures Facebook had to implement in the wake of one of its earlier data breaches, i.e. the Cambridge Analytica scandal. In short, Cambridge Analytica, a British consulting firm to the Trump campaign, unintentionally got hold of the personal data of millions of Facebook users.[215] Cambridge Analytica used the data to build profiles of American voters without the consent of Facebook users.[216] These measures Facebook had to implement because of this scandal implied embedding privacy in the board of directors. The Federal Trade Commission (henceforth "F.T.C.") mandated Facebook to create an independently appointed privacy committee on its board that would review decisions affecting user privacy.[217] The F.T.C. also ordered the company to designate compliance officers to oversee a privacy program, undergo regular privacy audits that Facebook's chief operating officer and others must submit to, and appoint an outside assessor to monitor the handling of data. [218] In view of the recent Facebook data breach, it may be of great relevance whether Facebook has implemented these measures. The reason for this is that following up respectively ignoring these measures might play a role in determining the personal liability of certain directors of Facebook according to the Dutch legal liability framework. I will return to this case in my final chapter.

To conclude this chapter, I will discuss the Dutch DigiNotar case.[219] The reason why I will go into this case is that this is the only Dutch judgment that addresses liability of directors regarding poor cyber-security management and therewith regarding an occurred cyber-risk. However, it is important to note that the judge in this case assessed a breach of a security warranty.

DigiNotar was a company that provided digital certificates to secure electronic data traffic and guarantee the origin of websites.[220] However, it had done too little to secure its systems and had kept that hidden from customers. In particular, DigiNotar did not sufficiently upgrade DotNetNuke, which is the software DigiNotar used, on several servers. It only upgraded the critical parts and not the medium and low ones.[221] In addition, DigiNotar ignored various warnings regarding saving unencrypted

---

[214] Allison Matyus, 'Facebook Faces Another Huge Data Leak Affecting 267 Million Users' (*Digital Trends*, 19 December 2019) <https://www.digitaltrends.com/news/facebook-data-leak-267-million-users-affected/> accessed 21 December 2019.

[215] Kevin Granville, 'Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens' *The New York Times* (New York, 19 March 2018) <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html> accessed 21 December 2019.

[216] ibid.

[217] Mike Isaac and Natasha Singer, 'Facebook Agrees to Extensive New Oversight as Part of $5 Billion Settlement' *The New York Times* (New York, 24 July 2019) <https://www.nytimes.com/2019/07/24/technology/ftc-facebook-privacy-data.html> accessed 30 December 2019.

[218] Victor Pak, 'Facebook Wordt Verplicht Privacy Te Verankeren In Bestuur' *Financieel Dagblad* (Amsterdam, 2 May 2019) <https://fd.nl/ondernemen/1299386/facebook-wordt-verplicht-privacy-te-verankeren-in-bestuur#> accessed 2 December 2019.

[219] District Court Amsterdam 30 July 2014, ECLI:NL:RBAMS:2014:4888.

[220] ibid para 2.9

[221] ibid para 4.3, 4.13.

passwords and credentials.[222] As a result of this poor cyber-security management, DigiNotar was hacked and then went bankrupt. The internet, especially in the public sector, was down for a week due to this hack. The reason why the public sector was particularly hit, was because the government encrypted its traffic by using above-mentioned certificates. Since these certificates were no longer trusted, the encrypted communication was also no longer reliable. This led to all the traffic of vital institutions of the government, such as the tax authority and courts, coming to a standstill. Shortly before the hack, DigiNotar was taken over. At the Court in Amsterdam, the new owner successfully held the former directors of DigiNotar liable for several million euros through their personal private limited liability companies.

This judgment mainly revolved around a security-warranty that implied that "The Company has for its current business in place fully tested, current and otherwise appropriate disaster recovery plans and procedures for its IT Systems and Software in order to prevent the loss and facilitate the recovery of data lost through system failure, physical destruction or otherwise and has taken reasonable steps and implemented all reasonable procedures to safeguard its IT Systems and Software and prevent unauthorized access thereto."[223] The Court assessed this warranty and came to the conclusion that DigiNotar, although it was warned several times for vulnerabilities in its security system, had not followed all reasonable procedures to guarantee this obligation.[224] Since the Court ruled that DigiNotar had breached the concerned security-warranty, one can deduce from this that there is a general obligation for directors to take all reasonable steps and implement all reasonable procedures to safeguard its IT systems and software and prevent unauthorized access thereto. Hence, although this case concerned a breach of a security-warranty, this warranty was formulated in such a general way in the acquisition agreement that it is, in fact, an obligation that should apply to all companies where data is being processed.

4.6 Sub-conclusion

Regarding the sub-question about the duties of directors regarding a cyber-risk, the answer can be found in the Code and the Cyber Security Guides. According to the Code, a director must put adequate internal risk management and control systems in place in its company. In addition, a director should ensure that the duties of the Audit Committee with regard to monitoring risk management (which covers cyber-security management) are fulfilled. According to the Cyber Security Guide for Board Members, a director must ensure that internal or external knowledge and/or expertise about cyber-security is embedded in the board. The two main obligations that can be derived from the Cyber Security Guide for Businesses are: (i) taking appropriate technical and organizational security measures and (ii) the data breach notification. The relevance of this chapter is to both determine the general duty of a director to "properly perform his duties" and to support the serious blame assessment by means of outlining these specific duties of directors regarding cyber-risks. In the next chapter, these described duties will be used to assess whether the (personal) serious blame standard, which is a requirement for both internal and external liability of directors, is met in case a cyber-risk has occurred.

[222] ibid para 4.3, 4.14.
[223] ibid para 2.7.
[224] ibid para 4.13, 4.14.

5. Cyber liability of a director in case of derivative damage

5.1 Introduction

As previously stated in chapter 3, it is difficult for a shareholder to claim – whether directly or indirectly – derivative damage. There are two ways to do so. A shareholder can indirectly claim compensation for derivative damage through the company itself pursuant to article 2:9 DCC. In addition, by stating a specific due diligence standard has been violated, a shareholder could directly claim compensation for derivative damage against a director pursuant to article 6:162 DCC.

With regard to indirectly claiming compensation in the form of derivative damage for a shareholder, I will set out two American cases that dealt with shareholder derivative actions in light of a cyber-attack. First, the Yahoo data breaches will be discussed as some of the biggest data breaches of all time. Second, the retail data breach at Home Depot will be analyzed. While these breaches took place at companies established in the US and therefore US law applied, they illustrate that a data breach can have great impact on the company itself and its shareholders. I will examine whether the directors of these American companies can be personally held liable by hypothetically applying the facts of these cases to the Dutch legal context. Lastly, I will go into the Dutch ASML case, which concerned intellectual property theft. However, the shareholders of ASML never brought proceedings against the directors. After summarizing the most relevant facts of these three cases, I will analyze whether the serious blame standard is met and therewith leads to internal liability of directors pursuant to article 2:9 DCC. I will do so by examining whether the directors in these three cases complied with the duties regarding cyber-risks, which have been outlined in the previous chapter. For this, the relevant facts and circumstances of these cases will be used. If internal liability of directors is likely to be established, the question as to whether a shareholder can recover the derivative damage will be answered.

With respect to directly claiming compensation in the form of derivative damage as a result of a cyber-incident for a shareholder, I will set out two devised cases and examine whether a shareholder can hold a director liable for derivative damage.

5.2 Cyber liability of a director based on article 2:9 DCC

5.2.1 Case Study: Yahoo facts

In September 2016, Yahoo announced that a series of data breaches, which affected over one billion user accounts, had taken place over a period of years.[225] It learned that these massive breaches of its user database resulted in the theft, unauthorized access, and acquisition of hundreds of millions of its users' data, including usernames, birthdates, and telephone numbers.[226] These series of data breaches occurred between 2013 and 2016 and in 2014. They are together called "Security Incidents".[227] Despite its knowledge of these Security Incidents, Yahoo did not disclose these in its public filings for nearly two years.[228] It did so in September 2016. Attempting to explain the delay between discovery and disclosure, Yahoo's Annual Report claimed that "certain senior executives did not properly comprehend or investigate, and therefore failed to act sufficiently upon, the full extent of knowledge known internally" about the

[225] Lawrence J Trautman, 'Corporate Directorss and Officerss Cybersecurity Standard of Care: The Yahoo Data Breach' [2016] SSRN Electronic Journal 1231, 1262 <http://www.ssrn.com/abstract=2883607> accessed 7 December 2019.
[226] ibid.
[227] ibid 1270.
[228] ibid 1271, 1272, 1278, 1283.

breach.[229] From this Annual Report can also be deduced that the security team knew about the data breach. It is, however, unclear whether and to what extent that knowledge was communicated to Yahoo's board and senior management. I will mention three relevant shortcomings of Yahoo's security. First of all, Yahoo failed to empower, and denied requested resources to its new CISO Alex Stamos, who was hired in 2014.[230] Stamos frequently clashed with Mayer, former CEO of Yahoo, and Yahoo's senior vice president, Jeff Bonforte, who oversaw Yahoo's email and messaging services.[231] Secondly, Mayer repeatedly refused to invest meaningful resources to secure Yahoo's security infrastructure.[232] Thirdly, Mayer rejected the suggested implementation of one of the most basic security measures: automatically resetting all users' passwords.[233] According to security experts, this is considered a standard step after a data breach.[234]

The day after Yahoo publicly disclosed the Security Incidents, Yahoo's market capitalization fell nearly $1.3 billion by virtue of a 3% decrease in its share price.[235] In the wake of these Security Incidents, former directors and officers of Yahoo agreed to pay $29 million to settle a breach of fiduciary duty by means of derivative lawsuits.[236] As a reminder, derivative suits are breach of fiduciary duty suits against directors and officers brought by shareholders on behalf of a company.[237] It is also important to note that the Securities and Exchange Commission tagged Altaba, which was previously Yahoo, with a $35 million penalty for failing to make a timely disclosure of the data breach, the commission's first action for a cyber-security disclosure violation.

5.2.2 Case Study: Yahoo analysis

In this paragraph, I will apply the above-mentioned facts of the Yahoo case to the Dutch legal framework, which has been articulated in the previous chapters. For a director to be liable under article 2:9 DCC, a director should have improperly performed his duties, for which "serious blame" can be attributed to him. This follows from the judgment of the Supreme Court in *Staleman/Van de Ven*. I will highlight five elements of this Yahoo case and examine whether this serious blame standard is met based on these elements. These elements are reviewed in light of the hypothetical example that Yahoo would be a Dutch listed company.

Firstly, there was a long delay – nearly two years – between the internal discovery and public disclosure of the Security Incidents. This considerably long delay

---

[229] 'Yahoo! Inc. Annual Report 47 (Form 10-K)' (2017) <https://www.sec.gov/Archives/edgar/data/1011006/000119312517065791/d293630d10k.htm> accessed 6 December 2019.
[230] Trautman (n 225) 1267.
[231] ibid 1266.
[232] ibid 1267.
[233] ibid.
[234] Nicole Perlroth and Vindu Goel, 'Defending Against Hackers Took a Back Seat at Yahoo, Insiders Say' *The New York Times* (New York, 28 September 2016) <https://www.nytimes.com/2016/09/29/technology/yahoo-data-breach-hacking.html> accessed 30 December 2019.
[235] Edwards (n 32) 675, 676.
[236] Craig A Newman, 'Lessons for Corporate Boardrooms from Yahoo's Cybersecurity Settlement' *The New York Times* (New York, 23 January 2019) <https://www.nytimes.com/2019/01/23/business/dealbook/yahoo-cyber-security-settlement.html?auth=login-facebook&login=facebook> accessed 7 December 2019.
[237] It is important to note that the legal ground for compensation for derivative damage in the United States is different than the one in the Netherlands. However, this is beyond the scope of my research, since I will neither compare the US liability framework of directors with the Dutch liability framework of directors, nor the distinction in possibilities for a shareholder to do so.

between discovery and revelation is contrary to the Cyber Security Guide for Businesses, which states that a data breach must be reported within 72 hours to the supervisory authority.[238]

Secondly, the suggested implementation of the most basic security measures: automatically resetting all users' passwords can be seen as a technical measure that ensures appropriate security of personal data.[239] By rejecting the suggested implementation of automatically resetting all users' passwords, Yahoo does, therefore, again not comply with the Cyber Security Guide for Businesses.[240]

Thirdly, there are four tools that can provide some guidance on how to undermine the argument in Yahoo's annual report about the lack of knowledge and expertise by Yahoo's board and senior management with respect to the Security Incidents:

(i) The Cyber Security Guide for Board Members states all directors should have the desired sufficient basic knowledge of cyber-security.[241] The facts clearly indicate that the CISO Stamos was not able to properly fulfill his tasks regarding the enforcement of Yahoo's cyber-security policy;

(ii) The main provisions of the Cybersecurity Disclosure Act of 2019, if passed, prescribe that listed companies should either acquire cyber-security expertise on the board or prove to the SEC that having the expertise is not necessary because of other compensating controls[242];

(iii) Since Yahoo is a listed company[243], the Code is binding. The Code stipulates that each director should have the specific expertise required for the fulfillment of his duties.[244] This implies that it is important that sufficient expertise is available within the board to identify risks that may be associated with innovations in business models and technologies in a timely manner.[245] Here one may think of acquiring expertise regarding the identification of cyber-risks to personal data.

(iv) Circumstance (v) of the *Staleman/Van de Ven* judgment, which states that the information that was available to the director or should have been available at the time of his actions, must be taken into account in the assessment of the serious blame standard.[246] It is doubtful whether Yahoo's board and senior management really did not know about the Security Incidents until mid 2016. It may be expected that, in particular, the board was well-informed about such severe security incidents and that internal processes were in place to ensure that this vital information reached the board.

These four specific tools aim to raise the level of awareness for cyber-security oversight, and in particular contribute to drawing attention to companies' risk focus for cyber-security. These tools could, therefore, also be taken into account when interpreting the serious blame standard.

---

[238] 'Cybersecurity Guide For Businesses' (n 183) 10.
[239] ibid.
[240] ibid.
[241] 'Cybersecurity Guide For Board Members' (n 184) 7.
[242] 116th Congress S. 592: Cybersecurity Disclosure Act of 2019 (n 210).
[243] Stock Price Altaba (Former Yahoo), (*Markets Insider*)
<https://markets.businessinsider.com/stocks/aaba-stock> accessed 1 January 2020.
[244] Bpp 2.1.4 Code.
[245] Explanatory note to Bpp 2.1.4 Code.
[246] Supreme Court 10 January 1997, *NJ* 1997/360 with annotation by J.M.M. Maeijer and *JOR* 1997/29 (*Staleman/Van de Ven*) para 3.3.1

Fourthly, it seems that the investments in cyber-security management of Yahoo were too low to prevent hackers from gaining access to its users' databases. Despite the insistence of the CISO on additional resources, this has not been followed up. As a result, Yahoo's directors[247], including the CEO, have consciously taken the risk that cyber-incidents, such as the ones that have occurred, would occur. Also, the fact that millions of users' accounts had been compromised and no adequate resource investments were made in Yahoo's security infrastructure might be of relevance to interpret the serious blame standard. Regarding this falling short in investing in Yahoo's cyber-security infrastructure, the Laurus-standard of chapter 2 comes into play.[248] The performance of duties of a director is assessed by comparing his actions to how an average reasonable and capable director would have acted under the same circumstances as the circumstances that occurred during the performance.[249] In the Yahoo case, it may be expected from an average reasonable and capable director, especially since Yahoo is one of the biggest data companies in the world, to invest in appropriate technical and organizational measures regarding cyber-security management. The *Laurus*-standard was also taken into account in the *Ceteco* case, which has been set out in chapter 2.

Fifthly and lastly, the fact that the SEC has fined Altaba, formerly Yahoo, with a $35 million-dollar fine for failing to make a timely disclosure of the data breach could also be taken into account in the assessment of the serious blame standard.

In my opinion, falling short of both the data breach notification obligation and taking technical and organizational security measures pursuant to the Cyber Security Guide for Businesses would be decisive factors in meeting the serious blame standard with respect to my hypothetical example. Based on this analysis, it seems likely that the serious blame standard can be attributed to Yahoo's directors. In case this has been established, the question as to whether internal liability arises depends on the exculpation possibilities of these directors. As mentioned in chapter 2, risk management, which covers cyber-security management, is considered a core task of the board. This implies that directors of a two-tier board cannot exculpate themselves from liability. However, Yahoo has a one-tier board. As already stated in chapter 2, the executive directors and non-executive directors, who are assigned to executive tasks, will be treated equally to directors within a two-tier board structure regarding exculpation. However, non-executive directors, who are assigned to supervisory tasks, fall under the Supervisory Board regime. From the fact that the senior management did not have knowledge about the Security Incidents, can be deduced that these non-executives neither had knowledge and therewith will try to exculpate themselves from liability be relying upon the division of tasks. However, the facts of this case do not mention anything regarding a division of tasks.

To conclude, since Yahoo's shareholders suffered derivative damage, as a result of a depreciation of their shares, it is important to examine whether they can claim indirect compensation through the company itself based on article 2:9 DCC. It seems that Yahoo has a justified claim against one or more of its directors based on article 2:9

[247] The board of directors at the time of the Security Incidents was composed of: Marissa Mayer as President and Chief Executive Officer; Eric Brandt as Chairman of the Board; Maynard Webb as Chairman Emeritus; Tor Braham; David Filo; Catherine Friedman; Eddy Hartenstein; Richard Hill; Thomas McInerney; Jane Shaw Ph.D.; and Jeffrey Smith.
[248] Supreme Court 8 April 2005, ECLI:NL:HR:2005:AS5010, *NJ* 2006/443 with annotation by G. van Solinge; *JOR* 2005/119 with annotation by M. Brink (*Laurus*).
[249] De objectieve "maatman-bestuurder".

DCC, since the serious blame standard is likely to be met. However, Yahoo will not be inclined to bring proceedings against itself. A shareholder would, therefore, need to force Yahoo to do so by means of a shareholders' resolution in the AGM. This resolution can be made by using the conflict-of-interest-rule. To do so, a quorum has to be reached in the AGM.[250]

5.2.3 Case Study: Home Depot facts

Home Depot – a retail company – has been one of the many victims of a retail data breach in recent years. It was the result of hackers obtaining access to 56 million customer credit card records and millions of email addresses and therewith has been the largest retail breach in U.S. history.[251] To get some understanding of the security systems of Home Depot, I will give a short overview. With regard to Home Depot's prevention and detection of a cyber-attack, there were a few controls that were lacking to ensure its cyber-security.

First of all, neither the software nor the hardware was securely configured on the Point of Sale (henceforth "POS") terminals. In particular, a secure configuration that was lacking was the use of Point-to-Point (P2P) encryption.[252] This enables payment card data to be encrypted at the point of swipe and allows the data to be encrypted in memory. To be able to use this technology, it exacts hardware that is capable of using the technology. In addition, an upgrade to the operating system of the POS devices was also required. The operating system running on POS devices was Windows XP Embedded SP3.[253] It is important to note that Windows XP machines are highly vulnerable to attacks.

Secondly, there was no proof of frequently planned vulnerability scanning of the POS environment.[254] This frequent scanning has to be performed to ensure that the POS environment is compatible with P2P encryption, antivirus, and many other applications that are crucial to secure the POS devices.

Thirdly, Home Depot did not have solid network segregation between its corporate network and the POS network.[255]

Fourthly and lastly, proper monitoring capabilities and the management of third-party vendor identities and access were absent at Home Depot.[256] With respect to monitoring the company's IT and digital security, Home Depot had earlier set up the Infrastructure Committee. However, Home Depot dissolved this committee in May 2012. It stated in its Proxy Statement of 2012 that the responsibility for IT and data security, which had previously been the field of the Infrastructure Committee, was now

---

[250] Article 2:120 DCC for public limited liability companies; article 2:230 DCC for private limited liability companies.

[251] Kate Vinton, 'With 56 Million Cards Compromised, Home Depot's Breach Is Bigger Than Target's' (*Forbes*, 18 September 2019) <https://www.forbes.com/sites/katevinton/2014/09/18/with-56-million-cards-compromised-home-depots-breach-is-bigger-than-targets/#23d337a33e74> accessed 14 December 2019.

[252] Brett Hawkins, 'Case Study: The Home Depot Data Breach', *SANS Institute Information Security Reading Room* (January 2015) 7,8 <https://www.sans.org/reading-room/whitepapers/casestudies/case-study-home-depot-data-breach-36367> accessed 13 December 2019

[253] ibid 8.

[254] ibid 7.

[255] ibid 7, 8.

[256] ibid.

being borne by the Audit Committee.[257] The Audit Committee's charter, however, was never amended to reflect this change.[258]

The data breach lasted from April to September 2014. On 8 September that year, Home Depot released a statement indicating that its payment card systems were breached. They stated that the investigation began on 2 September and they were still trying to figure out the actual scope and impact of the breach. They also indicated that their Incident Response Team was following its Incident Response Plan to contain and eradicate the damage and was working with security firms for the investigation.[259]

Shareholder derivative suits soon followed. They alleged that Home Depot failed to institute internal controls sufficient to oversee the risks that Home Depot faced in the event of a breach and because it disbanded a board of directors committee that was supposed to have oversight of those risks.[260] In addition, shareholders stated that Home Depot's 2014 and 2015 Proxy Statements, which were issued after the data breach had begun, did not include any indication that the Audit Committee's charter had been changed to reflect its new duties. Finally, the shareholders claimed that Home Depot had ignored various notifications, ranging from payment processing forensic experts, to letters of notice from Visa, to reports issued by security consultants.[261] Despite this, Home Depot did not admit wrongdoing or liability in agreeing to settle in the derivative lawsuits.[262] It agreed to pay at least $19.5 million to compensate US consumers harmed by this data breach.[263] In addition, Home Depot agreed to improve data security over a two-year period and hire a chief information security officer to oversee its progress.[264]

5.2.4 Case Study: Home Depot analysis

As I did in the Yahoo case, I will apply the above-mentioned facts of the Home Depot case to the Dutch legal framework, which has been articulated in the previous chapters. Therefore, I will analyze the Home Depot facts and examine whether the serious blame standard of article 2:9 DCC is met. It is important to note that, like Yahoo, Home Depot is a listed company.[265] In my hypothetical example, it therefore has to comply with the Code.

First of all, the fact that Home Depot's POS registers were still running Windows XP Embedded SP3 made the company considerably vulnerable to cyber-attacks. Because an operating system is the most important software on a device, it should have been upgraded to a more current Windows operating system for its POS devices. Due to this lack of upgrading, it can be inferred that Home Depot did not have appropriate technical and organizational security measures in place to prevent this data breach from happening. The reason for this can also be found in Home Depot not taking all the

---

[257] Jeff Kosseff, *Cybersecurity Law* (2nd edn, Wiley 2020).
[258] ibid.
[259] Brett Hawkins, 'Case Study: The Home Depot Data Breach' (2015) 2.
[260] Edwards (n 32) 673.
[261] Dynkin and Dynkin (n 32) 41.
[262] Jonathan Stempel, 'Home Depot Settles Consumer Lawsuit over Big 2014 Data Breach' (*Reuters*, 8 March 2016) <https://www.reuters.com/article/us-home-depot-breach-settlement/home-depot-settles-consumer-lawsuit-over-big-2014-data-breach-idUSKCN0WA24Z> accessed 13 December 2019.
[263] ibid.
[264] ibid.
[265] Stock Price Home Depot (*Markets Insider*) <https://markets.businessinsider.com/stocks/hd-stock> accessed 1 January 2020.

necessary steps to prevent and detect a cyber-incident from taking place. This would be contrary to the Cyber Security Guide for Businesses.[266]

Secondly, an obligation pursuant to this guide is the data breach notification obligation. In this regard, the data breach should be notified to the Data Protection Authority within 72 hours after having become aware of it.[267] Given the fact that Home Depot began its investigation into the breach on 2 September and released a statement on 8 September, shows that it would not have complied with the data breach notification obligation. The reason for this is that this release statement of the data breach is not considered sufficient to meet this notification obligation and, if considered sufficient, would have been notified too late.

Thirdly, shareholders of Home Depot alleged that it failed to institute adequate internal controls sufficient to monitor the risks that Home Depot faced in case of a breach. This would imply that Home Depot violated principle 1.2 of the Code, since it failed to have adequate internal control systems in place. The same happened in the *Vie d'Or* case, in which the Enterprise Division ruled that the administrative organization and internal control did not comply with the required standards.[268] In addition, the Infrastructure Committee, which oversaw Home Depot's IT and digital security, was dissolved. This task was handed over to the Audit Committee. However, it is not clear whether the Audit Committee monitored the board with regard to risk management, which includes cyber-security management. This monitoring obligation of the Audit Committee follows from the Code.[269] If the Audit Committee did not do so, this would also result in a violation of the Code.

Fourthly, disregarding several notifications by Home Depot corresponds to the facts of the DigiNotar case. This case has been discussed in the previous chapter. The fact that DigiNotar ignored several warnings was considered a major factor which the Court took into account in its deliberations regarding the board's knowledge of vulnerability of the systems. This, therefore, led to accountability of the board of DigiNotar.

Fifthly and lastly, Home Depot set up an Incident Response Plan that would limit and eliminate the damage resulting from the data breach. This is in accordance with the Cyber Security Guide for Businesses, which states that – following an incident – a company should: i) investigate the incident and the severity of its consequences, and ii) take steps without delay to resolve the incident and prevent or limit (further) negative consequences.[270]

Based on this hypothetical analysis, the non-compliance with the Cyber Security Guide for Businesses and the Code, in particular failing to meet the data breach notification obligation and not putting in place technical and organizational measures to secure data of its customers would weigh heavily in the assessment of whether the serious blame standard is met. Due to not implementing adequate internal control systems, which is required according to the Code, technical and organizational measures were also insufficient. In addition, the fact that Home Depot disregarded several warnings may also be considered as a circumstance to arrive at meeting the serious blame standard. The reason for this is that this was also of great importance in the DigiNotar case for the accountability of the board. I believe that, by relying on these findings, it seems

[266] 'Cybersecurity Guide For Businesses' (n 183) 10, 11.
[267] ibid 10.
[268] Enterprise Division of the Court of Appeal of Amsterdam 9 July 1998, *JOR* 1998, 122 (*Vie d'Or*).
[269] Bpp 1.5.1(iii) Code.
[270] 'Cybersecurity Guide For Businesses' (n 183) 17.

likely that the serious blame standard would be met in this case. However, the directors of Home Depot will try to exculpate themselves from liability. In this regard, the Incident Response Plan might be a factor to be taken into account when assessing the exculpation possibilities. However, as mentioned in chapter 2, risk management, which covers cyber-security management, is considered a core task of the board. This implies that directors of a two-tier board cannot exculpate themselves from liability. Home Depot has, like Yahoo, a one-tier board. Executive directors and non-executive directors, who are assigned to executive tasks, will be treated equally to directors within a two-tier board structure regarding exculpation. Since there is nothing stated about a division of tasks in this case, the main principle of collective responsibility will apply. In my opinion, there is no sufficient ground for a successful exculpation appeal for directors. In case shareholders want to be compensated for derivative damage, they have to follow the same procedure as described in the Yahoo case above.

5.2.5 Case Study: ASML facts

A recent case concerned corporate espionage on Dutch soil. The chip manufacturer for advanced machinery, ASML, had suffered a data breach in March 2015. However, it said at the time that no "valuable" files had been accessed.[271] This highly discussed ASML case, in which large-scale theft of trade secrets by high-ranking Chinese R&D-employees has occurred, is an example of a major cyber-security breach. What happened was that six former ASML employees, all with Chinese names, breached their employment contract by sharing information on ASML software processes with a company called XTAL Inc.[272] ASML said XTAL's funding came from South Korea and China.[273] It said the aim of the theft was to create a competing product and sell it to an existing ASML customer in South Korea.[274] Because of this breach, i.e. intellectual property theft, there is a high probability that sensitive information has fallen into the hands of Chinese and South Korean competitors.

ASML only discovered the theft of intellectual property after ASML technology was "out of the blue" being used by a competitor in 2015.[275] After discovering this theft, ASML brought proceedings against XTAL.[276] In November 2018, the American court awarded ASML $223 million in damages.[277] Since ASML considered this amount of damage not of material importance to ASML's business and not material to investors, it decided (in 2015) not to communicate this issue externally till 11 April 2019, for

---

[271] Toby Sterling and Anthony Deutsch, 'ASML Says It Suffered Intellectual Property Theft, Rejects "Chinese" Label' (*Reuters,* 11 April 2019) 3 <https://www.reuters.com/article/us-asml-china-spying/asml-says-it-suffered-intellectual-property-theft-rejects-chinese-label-idUSKCN1RN0DK> accessed 26 December 2019.

[272] Bert Van Dijk and Johan Leupen, 'ASML Heeft Zijn Aandeelhouders Heel Wat Uit Te Leggen over de Chinese Technologieroof' *Financieel Dagblad* (Amsterdam, 12 April 2019) <https://fd.nl/ondernemen/1297022/asml-heeft-zijn-aandeelhouders-heel-wat-uit-te-leggen-over-de-chinese-technologieroof> accessed 26 December 2019.

[273] ibid.

[274] ibid.

[275] Johan Leupen and Jeroen Piersma, 'Bestuur ASML Steekt Hand in Eigen Boezem Na Chinese Spionagezaak' *Financieel Dagblad* (Amsterdam, 25 April 2019) <https://fd.nl/ondernemen/1298537/asml-steekt-hand-in-eigen-boezem-rond-spionagezaak> accessed 27 December 2019.

[276] 'Report of the Annual General Meeting of Shareholders of ASML Holding N.V.' (2019) 3 <https://www.asml.com/en/investors/shares/shareholder-meetings/agm-2019> accessed 27 December 2019.

[277] ibid 6.

example in the financial statements or the management report.[278] In addition, at the end of 2018, the Supervisory Board of ASML had not yet been informed of the intellectual property theft.[279] However, Paul Koster of the Dutch Association of Stockholders is of the opinion that ASML should have provided full insight into this cyber-incident through a press release in November 2018.[280] It is important to note that XTAL has never been able to commercially use the stolen information and went bankrupt quite soon after this conviction.[281]

ASML shares dropped 1.5 percent after this cyber-incident became known to the public.[282] Shareholders of chip-machine manufacturer ASML have demanded clarity about this security breach as quickly as possible.[283] The question arises as to whether ASML's shareholders can hold the directors liable for derivative damage due to poor cyber-security management.

5.2.6 Case Study: ASML analysis

As I did in the previous two American cases, I will hypothetically analyze the above-mentioned facts and check whether the serious blame standard of article 2:9 DCC is met. First and foremost, it is important to note that ASML is established in the Netherlands. In addition, as a listed company with a two-tier board[284], it has to comply with the Code.[285] I will go into four main considerations of this case.

Firstly, the CEO admitted that ASML, when the cyber-incident took place, was less on top of the risk of intellectual property theft than it is today.[286] Employees of ASML could download source codes on their ASML-computer. And from there they could download it on any device they wanted.[287] Moreover, someone could take his laptop home, swap the hard drive and have access everywhere. In addition, there was no periodic monitoring of computers to see if they had downloaded files.[288] Besides this case concerning the theft of trade secrets, another cyber-incident at ASML in 2014 has put cyber-security on the map at ASML.[289] The company now invests five times as much in cyber-security as it did back then.[290] Based on these findings, it seems that ASML did not conduct a risk assessment and therewith did not implement adequate internal risk management and control systems.[291] This obligation of the Code is in line with the Cyber Security Guide for Businesses. This guide states that a company must regularly check whether the security measures taken are still adequate.[292] From a company like ASML, which is a well-known high-tech company, one may expect that

---

[278] ibid 3.
[279] ibid 7.
[280] Sterling and Deutsch (n 271).
[281] 'Report of the Annual General Meeting of Shareholders of ASML Holding N.V.' (n 276) 3.
[282] Bert Van Dijk and Johan Leupen, 'Wat Gaat ASML Vertellen over de Spionagezaak?' *Financieel Dagblad* (Amsterdam, 24 April 2019) <https://fd.nl/ondernemen/1298270/wat-gaat-asml-zijn-aandeelhouders-vertellen-over-de-spionagezaak> accessed 29 December 2019.
[283] Van Dijk and Leupen (n 272).
[284] 'ASML Integrated Report on Corporate Governance' (2018) 79 <https://www.asml.com/en/company/governance> accessed 1 January 2020.
[285] Code 7.
[286] Leupen and Piersma (n 275).
[287] ibid.
[288] Van Dijk and Leupen (n 282).
[289] 'Report of the Annual General Meeting of Shareholders of ASML Holding N.V.' (n 276) 3, 4.
[290] ibid 3; Leupen and Piersma (n 275).
[291] Principle 1.2, Bpp 1.2.1, 1.2.2 Code.
[292] 'Cybersecurity Guide For Businesses' (n 183) 10.

it meets the state-of-the-art test regarding its cyber-security systems. Moreover, the fact that ASML already had to deal with a cyber-incident in 2014, should have urged the board to improve its internal risk management and control systems.[293] Again, this corresponds to the Cyber Security Guide for Businesses, which states that companies, following a cyber-incident, must prevent similar incidents from occurring in the future.[294] If they had complied with both the Code and this Guide and lessons were learned in the aftermath of the hack of 2014, maybe the intellectual property theft in 2015 would not have taken place.

Secondly, since the board did not mention this 2015 data breach in the management report[295], the Supervisory Board of ASML did not have any knowledge of the intellectual property theft. This is because the theft was not brought to the attention of the Audit Committee[296], and therefore it was not reported to the Supervisory Board as a material risk.[297] The reason for this was that the size of the activity for which the stolen information was relevant, was approximately 0.5% of ASML's turnover and ASML had not suffered any actual damage as a result of the theft.[298] Therefore it did not consider the data breach as material.

Thirdly, the board has violated its company's code of conduct and business principles. This document states that "ASML expects anyone entrusted with ASML assets to keep them safe from loss, damage, misuse, or theft. Under "assets" we do not only mean physical assets, such as products, tooling, funds, computers for conducting ASML business but also information (Intellectual Property, product-, business- and personal data). ASML assets shall never be used for purposes that violate the law or company policies."[299] Complying with its own code of conduct, which is considered a guideline applicable to the management, is one of the relevant circumstances that has to be taken into account in the assessment of the serious blame standard.[300]

Fourthly, the Supervisory Board and the Audit Committee had not been involved in the XTAL case over the years. This was because the board considered the intellectual property theft not of material importance to ASML's business and not material to investors and was therefore considered a small issue.[301] The fact that the board considered this issue non-material resulted in not dealing with this data breach in the Audit Committee.[302] Consequently, it was also not mentioned in the Audit Committee report.[303]

The fact that ASML considered the impact of the data breach not of material importance to ASML's business and not material to investors is – in my opinion – a major factor to determine whether the serious blame standard is met. However, this decision is difficult to judge, since this was an internal matter of the board.[304] The fact that XTAL has never

---

[293] Bpp 1.2.2 Code.
[294] 'Cybersecurity Guide For Businesses' (n 183) 17.
[295] 'Report of the Annual General Meeting of Shareholders of ASML Holding N.V.' (n 276) 3.
[296] Bpp 1.5.1(iii) Code.
[297] Bpp 1.5.3(iv) Code.
[298] 'Report of the Annual General Meeting of Shareholders of ASML Holding N.V.' (n 276) 3.
[299] ASML, 'The ASML Code of Conduct & Business Principles' (2016) 9, 23 <https://www.asml.com/en/company/governance/business-principles> accessed 31 December 2019.
[300] Supreme Court 10 January 1997, *NJ* 1997/360 with annotation by J.M.M. Maeijer and *JOR* 1997/29 (*Staleman/Van de Ven*) para. 3.3.1.
[301] 'Report of the Annual General Meeting of Shareholders of ASML Holding N.V.' (n 276) 7.
[302] Bpp 1.5.1(iii), 1.3.5(ii) Code.
[303] Bpp 1.5.3(iv) Code.
[304] 'Report of the Annual General Meeting of Shareholders of ASML Holding N.V.' (n 276).

been able to use the stolen information in the commercial area and went bankrupt quite soon after the conviction may also be taken into account in the assessment of meeting the serious blame standard. A judge will most likely consider this as a circumstance that would not result in meeting this standard.

Envision that the theft of intellectual property in 2015 resulted in a material impact for ASML and the board discovered this materiality in 2019. Hence, in this hypothetical case, the discovery of meeting the notion of materiality would be four years after the theft. This would imply that the thieves were able to commercially use the stole information all these years. Because of this, the damage to ASML would be considerably higher than the damage mentioned above. Assuming this materiality was disclosed to the public, its shareholders will start selling their shares, which in turn leads to a massive drop (e.g. 10%) in share price. Therefore, there is substantial derivative damage for shareholders. The question that arises is whether meeting the materiality threshold would change the outcome of meeting the serious blame standard. In my opinion it would, since the board completely misjudged the impact for ASML by considering it non-material. As a result of this misjudgment, the management report and the Audit Committee report as of 2015 till 2018 are not accurate regarding material risks.[305] This would imply that the board of ASML has severely violated the Code.

To conclude, it seems that in the "real" ASML case shareholders will have difficulty to attribute serious blame to the directors. However, in the "hypothetical" ASML case it seems that shareholders have a justified claim against one or more of ASML's directors based on article 2:9 DCC, since the serious blame standard is likely to be met. When this standard has been established, the question as to whether internal liability arises depends on the exculpation possibilities of these directors. However, as mentioned in chapter 2, risk management, which covers cyber-security management, is considered a core task of the board. This implies that directors of a two-tier board cannot exculpate themselves from liability. Consequently, one or more directors of ASML can be held liable for improper performance of duties pursuant to article 2:9 DCC. However, ASML will not be inclined to bring proceedings against itself. A shareholder will, therefore, force ASML to do so by means of a shareholders' resolution in the AGM. This resolution can only be made by reaching a quorum in the AGM.

Besides the possibility for a shareholder to be indirectly compensated for derivative damage through the company, the shareholder can claim direct compensation for derivative damage pursuant to article 6:162 DCC. This possibility will be discussed below.

5.3 Cyber liability of a director based on article 6:162 DCC

To directly claim derivative damage a shareholder should demonstrate a violation of a specific due diligence standard by a director. In addition, external liability of directors requires that serious blame be *personally* attributable to a director. This is the case, for example, if there has been a violation of a provision in the articles of association that is intended to protect the interest of the shareholder.[306] As has already been stated in the previous chapter, such default establishes, in principle, the liability of the director

[305] Bpp 1.5.1(iii), 1.5.3(iv) Code.

[306] Supreme Court 20 June 2008, ECLI:NL:HR:2008:BC4959, *NJ* 2009/21 with annotation by J.M.M. Maeijer and H.J. Snijders (*Willemsen Beheer/NOM*) para 5.4. This is in line with the rules for internal liability, which follows from the Supreme Court 29 November 2002, ECLI:NL:HR:2002:AE8459, *NJ* 2003/55, with annotation by J.M.M. Maeijer (*Schwandt/Berghuizer Papierfabriek*) para 3.4.5.

towards that individual shareholder.[307] I will set out two devised cases regarding liability of directors as a result of a cyber-incident based on article 6:162 DCC.

Firstly, envision there is a provision in the articles of association that states: "In the performance of its duties assigned to it by law or these articles of association, the board of a company must put the interests of the company and its affiliated enterprise first and take the interests of all parties involved, including those of shareholders, into account in its decision-making."[308] Suppose this provision has been violated by a director due to failing to take appropriate measures with regard to cyber-security management, and therewith serious blame can be attributed to this director.

Secondly, imagine a large IT company in the Netherlands wants to invest – as a shareholder – in a start-up that has one director. This director has no knowledge of IT and therewith of cyber-security management. It is very important for this IT company, and in particular for the investor (called "shareholder X"), to ensure that a certain article in the shareholders' agreement is dedicated to adequate cyber-security management. Because of this, the following clause is included in the shareholders' agreement: "the director performs his duties regarding cyber-security management carefully, diligently and faithfully and to the best of his ability in a manner that is beneficial to the interests of the company and its shareholder X." If, in a shareholders' agreement, such a clause has been incorporated and violated, a shareholder can claim direct compensation for derivative damage. As already mentioned in chapter 3, a shareholder can state additional circumstances to support his claim that a specific due diligence standard has been violated. For example, stating that the director *intended* to harm the shareholder[309] or the derivative damage has a definitive nature[310] can be considered as an additional circumstance to establish a violation of a due diligence standard.

Regarding these two devised cases, I will assume that both the *personal* serious blame standard and all the other requirements of article 6:162 DCC are met. Hence, in these cases a shareholder has a justified right to claim direct compensation for derivative damage from the negligent director. As mentioned in chapter 3, a shareholder can only claim derivative damage from one director at the time by invoking article 6:162 DCC. Because of this, it is of major importance for a shareholder to know who is responsible for cyber-security management within the board. Therefore, a clear division of tasks may support a shareholder.

5.4 Sub-conclusion

To return to the sub-question of this chapter, I have used three hypothetical cases regarding liability of directors with respect to a cyber-incident. In this chapter I applied the facts of the Yahoo, Home Depot and ASML case to the Dutch legal framework, which has been articulated in the previous chapters. This is because there is no case law pertaining to this matter. However, by analyzing these hypothetical cases in light of the Dutch legal liability framework and duties of directors regarding cyber-risks, I can

[307] Supreme Court 29 November 2002, ECLI:NL:HR:2002:AE8459, *NJ* 2003/55, with annotation by J.M.M. Maeijer (*Schwandt/Berghuizer Papierfabriek*) para 3.4.5.
[308] Supreme Court 9 July 2010, ECLI:NL:HR:2010:BM0976, *NJ* 2010/544 with annotation by P. van Schilfgaarde (*AMSI II*), para 4.4.1.
[309] Supreme Court 16 February 2007, ECLI:NL:HR:2007:AZ0419, *NJ* 2007/256 with annotation by J.M.M. Maeijer (*Tuin Beheer*), para 3.5; District Court Central-Netherlands 22 May 2019, ECLI:NL:RBMNE:2019:2203, *RO* 2019/57.
[310] Supreme Court 2 May 1997, ECLI:NL:HR:1997:ZC2365, *NJ* 1997/662 with annotation by J.M.M. Maeijer (*Kip/Rabobank*), para 3.6.

cautiously draw some conclusions. In the assessment of the serious blame standard of article 2:9 DCC all relevant circumstances of the case must be taken into account. More importantly, as I have shown while analyzing the three cases, the assessment of this standard depends on giving a certain weight to certain facts. The last part of the chapter discusses the external liability of a director (article 6:162 DCC) in case of a cyber-incident. For external liability of a director, a shareholder needs to be able to attribute *personal* serious blame to a specific director. In addition, to directly claim derivative damage, as a result of a cyber-incident, a shareholder has to demonstrate that one director in particular has violated a specific due diligence standard regarding an occurred cyber-risk towards the shareholder.

6. Conclusion and recommendations

6.1 Final conclusion

Every year, cyber-attacks cause significant damage to companies and third parties. One of these third parties are shareholders, since many of these hit companies have a depreciation of its shares because of these cyber-security failures. This depreciation is also referred to as derivative damage. One could question as to whether shareholder derivative lawsuits in light of a significant cyber-incident will become a predictable risk for directors in the Netherlands, as it is already in the US. To try to avoid this from happening Dutch companies and their boards should elevate cyber-security management as a top priority on their agendas.

The aim of my research was to gain insight into the relationship between the liability of directors established in the Netherlands in case of a cyber-incident and shareholders derivative damage (as a result of this cyber-incident). Therefore, the main research question is:

To what extent can a director of a Dutch company be held liable by a shareholder when a cyber-risk resulting in derivative damage has occurred within the current legal framework?

A shareholder has two possibilities to hold a director liable in case of an occurred cyber-risk. Firstly, he can claim indirect compensation through the company itself based on article 2:9 DCC. Secondly, by demonstrating a violation of a specific due diligence standard, he can claim direct compensation pursuant to article 6:162 DCC.

For a director of a Dutch company to be liable towards the company itself, in case a cyber-incident took place, first and foremost improper performance of duties must be established pursuant to article 2:9 paragraph 1 DCC. It can be deduced from this that a director has the *general* duty to properly perform his duties.

The Supreme Court in *Staleman/Van de Ven* ruled that internal liability only occurs if serious blame can be attributed to a director. This serious blame standard has been codified in article 2:9 DCC paragraph 2 DCC. This standard, which is considered an objective test, has to be assessed by taking into account all the relevant circumstances.[311] In this regard, the specific duties of directors pertaining to cyber-risks deriving from the Code and the Cyber Security Guides should be taken into account in the assessment of the serious blame standard. In addition, these specific duties determine the general duty of article 2:9 DCC. The most important duties of directors regarding cyber-risks that could be of great relevance for the relationship between cyber-risks and liability of directors are: (i) the requirement of adequate risk management of the Code, (ii) taking appropriate technical and organizational security measures of the Cyber Security Guide for Businesses, and (iii) the data breach notification obligation of the Cyber Security Guide for Businesses.

In chapter 5, I outlined three cases, Yahoo, Home Depot and ASML, which were affected by a cyber-incident. These cases show that it depends on all the

[311] (i) the nature of the activities carried out by the legal entity; (ii) the resulting risks generally related to those activities; (iii) the divisions of tasks within the board; (iv) any guidelines applicable to the management; (v) the information that was available to the director or that ought to have been available at the time of his actions; and (vi) the insight and diligence that may be expected from a director who is capable of his tasks and who fulfills these tasks meticulously. These circumstances follow from the *Staleman/Van de Ven* judgment.

circumstances of the case and the weight that will be given to these circumstances to conclude whether the serious blame standard has been met. In addition, these cases illustrate that the duties of directors regarding cyber-risks should also be taken into account in this assessment. However, there has been no Dutch case law with respect to internal liability of directors regarding cyber-incidents, and therefore no guidance on how to assess the serious blame standard in this regard.

In case a director is to be seriously blamed, he can try to exculpate himself from liability. For this, a director can try to rely upon a – whether formal or informal – division of tasks. There is no distinction between the directors of a one-tier- and two-tier board structure regarding exculpation possibilities as far as non-executive directors perform executive tasks. However, there is the general assumption that risk management, which covers cyber-security management, is considered a core task of the board. With regard to core tasks, it is, in principle, not possible to exculpate from liability.

Besides internal liability of a director, a director of a Dutch company can also be liable towards shareholders pursuant to article 6:162 DCC. This concerns external liability of a director. For this, serious blame has to be *personally* attributable to this director to establish external liability. In addition, a shareholder has to demonstrate a violation of a specific due diligence standard by a director. In this respect there has been some case law which ruled that, in any event, a violation of a provision in the articles of association intended to protect the interest of the shareholder establishes the violation of a specific due diligence standard.

As stated above, there are two ways to claim derivative damage from a negligent director.

First, when relying upon article 2:9 DCC, a shareholder should have suffered derivative damage. Consequently, internal liability of a director has to be established. As stated above, it depends on all the circumstances of the case to determine whether the serious blame standard is met. In case a shareholder is of the opinion that this standard is likely to be met, he can claim derivative damage through the company. However, the company will not be inclined to do so, since this could lead to the liability of its directors. Due to this conflict-of-interest of directors, a shareholder of a one-tier board can force the company by means of a shareholders' resolution in the AGM to start proceedings against a negligent director. However, there has been no case law on forcing the company to do so by means of a shareholders' resolution in the AGM.

Second, when invoking article 6:162 DCC a shareholder should, again, have suffered derivative damage. Such an appeal is only against one director in particular. Because of this, *personal* serious blame has to be attributable to this director. In addition, as mentioned above, the only way to possibly succeed is to demonstrate a violation of a specific due diligence standard by a director.

To conclude, the outlined duties regarding cyber-risks in this research are of great importance to assess whether the (personal) serious blame standard is met for respectively internal and external liability of directors. In case one of these liability forms has been established, a shareholder can claim derivative damage from the company itself or a specific director depending on the form of liability. The route which has to be followed by a shareholder to claim derivative damage, resulting from an occurred cyber-risk, also depends on which liability form can be established. It must be

said, however, that the route via the AGM by means of a shareholders' resolution will most likely be difficult.

In the past, also the possibility to directly claim derivative damage has been difficult for a shareholder. The reason for this is that a judge hardly ever came to the conclusion that a specific due diligence standard had been violated. However, recent case law shows that courts are more receptive towards accepting a violation of a specific due diligence standard. This development might lead to a more positive outlook for shareholders to directly claim derivative damage.

6.2 Recommendations

In the introductory chapter, I mentioned the GWK Travelex ransomware-attack. This money exchange company for a long time seems to have ignored important security updates. It is not yet clear whether the lack of security updates has led to the company's systems becoming infected with the malicious software. However, it appears to point in this direction. If it turns out that failing to update the company's security systems led to the ransomware-attack, this circumstance will most certainly be of importance in case the question arises as to whether directors of GWK Travelex, according to the Dutch legal liability framework, can be held liable for this negligent omission.

In addition, in chapter 4, I made a reference to the recent Facebook data breach of December 2019. In this regard, I also discussed the measures to be taken by Facebook as a result of earlier data breaches. In the wake of these earlier data breaches, the F.T.C. mandated Facebook to create an independently appointed privacy committee on its board that would review decisions affecting user privacy. It also ordered the company to designate compliance officers to oversee a privacy program, undergo regular privacy audits and appoint an outside assessor to monitor the handling of data. In my opinion, it would be interesting to assess whether, in light of the data breach of December 2019, a shareholder would have a stronger legal position to claim derivative damage, which occurred as a result of this data breach, in case Facebook did not comply with the mandatory measures imposed by the F.T.C. I assume it is just a matter of time before the Supreme Court in the Netherlands will have to deal with a case in which a shareholder claims derivative damage, as a result of poor cyber-security management, from a negligent director. When it does, it would be of great interest to learn from the considerations of the Supreme Court.

While in the US a bill has been drafted and introduced to the Senate, in which listed companies should acquire cyber-security expertise on the board, such legislation does not exist in the Netherlands. Including a similar provision in the Code would contribute to more prominently placing cyber-security on the agenda of the board.

I would recommend one other addition to the Code: adding the words "cyber" to Bpp 1.2.3 and 1.4.2 (i) of the Code.[312] This would imply that shareholders get insight into the cyber-risks and the level of cyber-security of a company. Because of this, shareholders may get a better understanding of the shortcomings of cyber-security management of a company and therefore urge companies to put the necessary security measures in place.

[312] See Appendix G and Appendix H.

Bibliography

Textbooks

Dortmond PJ, 'De One-Tier Board in Een Nederlandse Vennootschap' in LJ Hijmans van den Bergh (ed), *Nederlands ondernemingsrecht in grensoverschrijdend perspectief* (Instituut, Kluwer 2003)

Kosseff J, *Cybersecurity Law* (2nd edn, Wiley 2020)

Kroeze M, *Mr. C. Assers Handleiding Tot de Beoefening van Het Nederlands Burgerlijk Recht. 2. Rechtspersonenrecht. Deel I. De Rechtspersoon* (Kluwer 2015)

Maeijer JM., *Mr. C. Asser's Handleiding Tot de Beoefening van Het Nederlands Burgerlijk Recht. 2. Vertegenwoordiging En Rechtspersoon. Deel III. De Naamloze En de Besloten Vennootschap: Hoofdstuk X, XI, XII En XIV* (Kluwer 2000)

Mussche M, 'De Informele Taakverdeling Als Disculpatieverweer' in Bastiaan Assink (ed), *De vele gezichten van Maarten Kroeze's 'bange bestuurders'* (104th edn, Wolters Kluwer 2017)

Stolp MM and De Nijs Bik W, 'De Positie van Bestuurders En Commissarissen Ter Zake van Risicomanagement' in Arie Tervoort, Henk Bruisten and Suzanne Drion (eds), *Be (aware). Legal Risk Management & Compliance* (Sdu juridisch 2015)

Timmerman L, 'Van Afgeleide Schade Naar Afgeleide Actie' in AFJA Leijten (ed), *Conflicten rondom de rechtspersoon* (Kluwer 2000)

Van Solinge G and Nieuwe Weme MP, *Mr. C. Assers Handleiding Tot de Beoefening van Het Nederlands Burgerlijk Recht. 2. Rechtspersonenrecht. Deel II. De Naamloze En Besloten Vennootschap* (Kluwer 2013)

Veenstra F, 'Aantekeningen Bij Art. 2:346 BW' in Jan Bernd Huizink (ed), *Groene Serie Rechtspersonen* (Wolters Kluwer 2016)

Visée SWAM, 'Het Rechtskarakter van de Code Tabaksblat' in FB Falkena (ed), *Markten onder toezicht* (Kluwer 2004)

Theses

Huizink JB, 'Bestuurders van Rechtspersonen' (University of Groningen 1989)

Kroeze M, 'Afgeleide Schade En Afgeleide Actie' (University of Groningen 2004)

Strik D, 'Grondslagen Bestuurdersaansprakelijk, Een Maatpak Voor de Boardroom' (Erasmus University Rotterdam 2010)

Reports

ASML, ‘The ASML Code of Conduct & Business Principles’ (2016) <https://www.asml.com/en/company/governance/business-principles>

ASML, ‘ASML Integrated Report Corporate Governance’ (2018) <https://www.asml.com/en/company/governance>

ASML, ‘Report of the Annual General Meeting of Shareholders of ASML Holding N.V.’ (2019) <https://www.asml.com/en/investors/shares/shareholder-meetings/agm-2019>

‘Corporate Governance and the Financial Crisis: Key Findings and Main Messages’ (2009) <https://www.oecd.org/corporate/ca/corporategovernanceprinciples/43056196.pdf>

‘Cybersecurity Guide For Board Members’ (2019) <https://www.cybersecurityraad.nl/binaries/Handreiking_Bestuurders_ENG_DEF_2019_tcm107-323477.pdf>

‘Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1’ (2018) <http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

‘Global Risk Management Survey’ (2019) <https://www.aon.com/2019-top-global-risks-management-economics-geopolitics-brand-damage-insights/index.html>

‘Hiscox Cyber Readiness Report’ (2019) <https://www.hiscox.co.uk/sites/uk/files/documents/2019-04/Hiscox_Cyber_Readiness_Report_2019.PDF>

Kirkpatrick G, ‘The Corporate Governance Lessons from the Financial Crisis’ (2009) <https://www.oecd.org/finance/financial-markets/42229620.pdf>

KPMG, ‘Cyber Security Benchmark’ (2017) <https://assets.kpmg/content/dam/kpmg/pdf/2015/05/Cyber-Security-Benchmark.pdf>

National Coordinator for Security and Counterterrorism, ‘Cybersecuritybeeld Nederland CSBN 2019’ (2019) <https://www.rijksoverheid.nl/documenten/rapporten/2019/06/12/tk-bijlage-cybersecuritybeeld-nederland-csbn-2019>

Ponemon Institute, ‘2019 Cost of a Data Breach Report’ (2019) <https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf>

SpencerStuart, ‘2018 Netherlands Spencer Stuart Board Index’ (2018) <https://www.spencerstuart.com/-/media/2018/december/nlbi2018.pdf>

Van Wieren M and others, ‘Cyber Value at Risk in the Netherlands’ (2016) <https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-cyber-value-at-risk.pdf>

Williams C, ‘Cyber Risk and Risk Management’, *Cyber Risk Resources for Practitioners* (The Institute of Risk Management 2014) <https://www.theirm.org/media/7237/irm-cyber-risk-resources-for-practitioners.pdf>

Wolters P and Jansen C, ‘Cyber Security Guide for Businesses’ (2017) <https://www.cybersecurityraad.nl/binaries/Handreiking_Zorgplichten_ENG_DEF_tcm107-314471.pdf>

‘Yahoo! Inc. Annual Report 47 (Form 10-K)’ (2017) <https://www.sec.gov/Archives/edgar/data/1011006/000119312517065791/d293630d10k.htm>

Journals

Bushell S and Crawford G, ‘Cyber Security: Litigation Risk and Liability’ [2014] *Thomas Reuters Practical Law*

De Kraker HJ, ‘Het Praktisch Nut van de Herziene Corporate Governance Code Voor Het MKB’ (2017) 44 Bedrijfsjuridische Berichten 152

Dynkin B and Dynkin B, ‘Derivative Liability in the Wake of a Cyber Attack’ (2018) 28 Albany Law Journal of Science and Technology 23 <http://www.albanylawjournal.org/Documents/Articles/28.3.23_Dynkin.pdf>

Edwards BP, ‘Cybersecurity Oversight Liability’ (2019) 35 Georgia State University Law Review <http://www.albanylawjournal.org/Documents/Articles/28.3.23_Dynkin.pdf>

Goossens AE, ‘De Mogelijkheden Voor Vergoeding van Afgeleide Schade Verruimd’ (2016) 14 Maandblad voor Vermogensrecht 278 <http://www.bjutijdschriften.nl/doi/10.5553/MvV/157457672016014010004>

Hanegraaf CEJM, ‘De One-Tier Board En de Bestuurdersaansprakelijkheid van Niet-Uitvoerende Bestuurders’ (2019) 5 Maandblad voor Ondernemingsrecht 18 <http://www.bjutijdschriften.nl/doi/10.5553/MvO/245231352019005102003>

Jitta JMW, ‘(G)Een Code Voor Niet-Beursgenoteerde Ondernemingen?’ (2007) 135 Ondernemingsrecht 465

Kersten H, ‘De Rol van de Auditcommissie Bij Het Toezicht Door de Raad van Commissarissen Op Risicobeheer’ (2016) 14 Ondernemingsrecht 56

Moir A and others, ‘Cyber Security: Top Ten Tips for Businesses’ [2016] *Thomas Reuters Practical Law*

Olaerts M, ‘Bestuurdersaansprakelijkheid in Het Vernieuwde (BV-)Recht’ [2012] Tijdschrift voor Vennootschapsrecht, Rechtspersonenrecht en Ondernemingsbestuur 170

Oostwouder WJ, ‘Actualiteiten “Afgeleide Schade”’ (2018) 26 Onderneming en Financiering 5 <http://www.bjutijdschriften.nl/doi/10.5553/OenF/157012472018026004002>

Rothrock RA, Kaplan J and Van der Oord F, ‘The Board’s Role in Managing Cybersecurity Risks’ [2018] MITSloan Management Review <https://sloanreview.mit.edu/article/the-boards-role-in-managing-cybersecurity-risks/>

Schild AJP, ‘Ontwikkelingen Bestuurdersaansprakelijkheid: Een Overzicht’ (2015) 7087 Weekblad voor Privaatrecht, Notariaat en Registratie 1049
——, ‘Bestuurdersaansprakelijkheid In Theorie: Bespreking Van Het Proefschrift van Mr WA Westenbroek’ [2019] Maandblad voor Vermogensrecht 36

Schild AJP and Timmerman L, ‘Het Nieuwe Art 2:9 BW, Uitgelegd Voor Gewone Bestuurders’ [2014] Weekblad voor Privaatrecht, Notariaat en Registratie 270

Stocks L, ‘Panama Papers: Time to Firm up on Cyber Security?’ [2016] *Thomas Reuters Practical Law*

Strik D, ‘Aansprakelijkheid van Niet-Uitvoerende Bestuursleden: You Cannot Have Your Cake and Eat It’ [2003] Ondernemingsrecht 370
——, ‘Ernstige Verwijtbaarheid: Tussen Onrechtmatigheid En Toerekenbaarheid - over de “inkleuring” van Art. 6:162 BW Door Art. 2:9 BW’ (2009) 156 Ondernemingsrecht 660
——, ‘One Tier Board En Aansprakelijkheid’ (2012) 91 Ondernemingsrecht 496

Stulz RM, ‘Six Ways Companies Mismanage Risk’ [2009] Harvard Business Review <https://hbr.org/2009/03/six-ways-companies-mismanage-risk>
Timmerman L, ‘Kan Een Aandeelhouder of Vennootschapsschuldeiser Afgeleide Schade Vorderen?’ (1998) 50 Maandblad voor Ondernemingsrecht en rechtspersonen 97
——, ‘Pragmatisch Denken over Afgeleide Schade’ (2013) 6962 Weekblad voor Privaatrecht, Notariaat en Registratie 115

Trautman LJ, ‘Corporate Directorss and Officerss Cybersecurity Standard of Care: The Yahoo Data Breach’ [2016] SSRN Electronic Journal <http://www.ssrn.com/abstract=2883607>

Vaessen RTL, ‘Bestuurdersaansprakelijkheid En Corporate Governance’ (2017) 15 Maandblad voor Vermogensrecht 321 <http://www.bjutijdschriften.nl/doi/10.5553/MvV/157457672017015012003>

Veenstra F, ‘De Aandeelhouder En Zijn Afgeleide Schade’ (2008) 4 Ondernemingsrecht 140

Verdam AF, 'Over de Bestuurstaak, Taakverdeling En Individuele Verantwoordelijkheid van de Bestuurder' (2017) 7135 Weekblad voor Privaatrecht, Notariaat en Registratie 97

Westenbroek WA, 'Metaalmoeheid Na 88 Jaar "Externe" Bestuurdersaansprakelijkheid En Spaanse Villa, Het Is Tijd Voor Herbezinning: Laat de Ernstig Verwijt Maatstaf Los.' (2015) 69 Ondernemingsrecht 353 <http://deeplinking.kluwer.nl/docid/idpass8042a887508743da883e5f063e449e23>
——, 'Het Trustkantoor Als Bestuurder En "Omgaan" in Het Bestuurdersaansprakelijkheidsrecht (HR 30 Maart 2018, ECLI:NL:HR:2018:470)' (2018) 26 Onderneming en Financiering 14 <http://www.bjutijdschriften.nl/doi/10.5553/OenF/157012472018026003003>
——, 'Bestuurdersaansprakelijkheid in Theorie' (2019) 29 Maandblad voor Vermogensrecht 103 <http://www.bjutijdschriften.nl/doi/10.5553/MvV/157457672019029003004>

Weterings W, 'Persoonlijke Aansprakelijkheid Bestuurders Voor Onvoldoende IT-Governance' [2016] Aansprakelijkheid, verzekering en schade

Wezeman JB, 'Uitvoerende Bestuurders En Niet Uitvoerende Bestuurders van Naamloze En Besloten Vennootschappen' [2009] Ars Aequi 112

Online sources

Berkhout K, 'Nederland Is Kwetsbaar Voor Cyberaanvallen' *NRC Handelsblad* (Rotterdam, 12 June 2019) <https://www.nrc.nl/nieuws/2019/06/12/nederland-is-kwetsbaar-voor-cyberaanvallen-a3963381>

Bischoff P, 'How Data Breaches Affect Stock Market Share Prices' (*Comparitech*, 6 November 2019) <https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/#Long_term_effects_of_data_breach_on_share_price>

Bonjer J, 'Triodos Nomineert Risicodirecteur Na Aandringen DNB' *Financieel Dagblad* (Amsterdam, 13 April 2019) <https://fd.nl/ondernemen/1297194/triodos-nomineert-risicodirecteur-na-aandringen-dnb#%3E>

Boyd C, 'Business Email Compromise Scam Costs Pathé $21.5 Million' (*Malwarebytes labs*, 19 November 2018) <https://blog.malwarebytes.com/cybercrime/2018/11/business-email-compromise-scam-costs-pathe-21-5-million/>

'Carla Van Der Weerdt Nominated As Chief Risk Officer Triodos Bank' (13 April 2019) <https://www.triodos.com/press-releases/2019/carla-van-der-weerdt-nominated-as-chief-risk-officer-triodos-bank>

'Cyber Security Raad' <https://www.cybersecurityraad.nl/binaries/CSR_Flyer_NED_20191125_tcm107-314456.pdf>

Cyber Security Raad, ‘Bedrijven Doen Nog Te Weinig Aan Digitale Veiligheid’ (*Cyber Security Raad*, 2017) <https://www.cybersecurityraad.nl/010_Actueel/bedrijven-doen-nog-te-weinig-aan-digitale-veiligheid.aspx>

‘GM’s Code of Conduct’ (*General Motors*, 2019) 14 <https://investor.gm.com/static-files/265a1dc0-adc5-4d38-ab41-2c58e575692d>

Granville K, ‘Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens’ *The New York Times* (New York, 19 March 2018) <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>

Hawkins B, ‘Case Study: The Home Depot Data Breach’ (January 2015) <https://www.sans.org/reading-room/whitepapers/casestudies/case-study-home-depot-data-breach-36367>

Hay Newman L, ‘The Biggest Cybersecurity Crises of 2019 So Far’ (*Wired*, 7 May 2019) <https://www.wired.com/story/biggest-cybersecurity-crises-2019-so-far/>

Hueck H and Van Gils S, ‘Honderden Nederlandse Bedrijven Met Citrix-Servers Vatbaar Voor Hack’ *Financieel Dagblad* (Amsterdam, 14 Januart 2020) <https://fd.nl/ondernemen/1330985/honderden-nederlandse-bedrijven-met-citrix-servers-vatbaar-voor-hack#>

Isaac M and Singer N, ‘Facebook Agrees to Extensive New Oversight as Part of $5 Billion Settlement’ *The New York Times* (New York, 24 July 2019) <https://www.nytimes.com/2019/07/24/technology/ftc-facebook-privacy-data.html>

Jones R, ‘Travelex Forced to Take down Website after Cyber-Attack’ *The Guardian* (London, 2 January 2020) <https://www.theguardian.com/technology/2020/jan/02/travelex-forced-to-take-down-website-after-cyber-attack>
——, ‘Travelex Services Begin Again after Ransomware Cyber-Attack’ *The Guardian* (London, 13 January 2020) <https://www.theguardian.com/business/2020/jan/13/travelex-services-begin-again-after-ransomware-cyber-attack>

Lemstra D, ‘Act on Management and Supervision Will Enter into Force on 1 January 2013’ (*Stibbe*, 27 September 2012) <https://www.stibbe.com/en/news/2012/september/act-on-management-and-supervision-will-enter-into-force-on-1-january-2013>

Leupen J and Piersma J, ‘Bestuur ASML Steekt Hand in Eigen Boezem Na Chinese Spionagezaak’ *Financieel Dagblad* (Amsterdam, 25 April 2019) <https://fd.nl/ondernemen/1298537/asml-steekt-hand-in-eigen-boezem-rond-spionagezaak>

‘Maastricht University Paid Hackers to Get Back System Access’ (*DutchNews.nl*, 2 January 2020) <https://www.dutchnews.nl/news/2020/01/maastricht-university-paid-hackers-to-get-back-system-access/>

Matyus A, ‘Facebook Faces Another Huge Data Leak Affecting 267 Million Users’ (*Digital Trends,* 19 December 2019) <https://www.digitaltrends.com/news/facebook-data-leak-267-million-users-affected/>

Newman CA, ‘Lessons for Corporate Boardrooms from Yahoo’s Cybersecurity Settlement’ *The New York Times* (New York, 23 January 2019) <https://www.nytimes.com/2019/01/23/business/dealbook/yahoo-cyber-security-settlement.html?auth=login-facebook&login=facebook>

Perlroth N and Goel V, ‘Defending Against Hackers Took a Back Seat at Yahoo, Insiders Say’ *The New York Times* (New York, 28 September 2016) <https://www.nytimes.com/2016/09/29/technology/yahoo-data-breach-hacking.html>

Stempel J, ‘Home Depot Settles Consumer Lawsuit over Big 2014 Data Breach’ (*Reuters*, 8 March 2016) <https://www.reuters.com/article/us-home-depot-breach-settlement/home-depot-settles-consumer-lawsuit-over-big-2014-data-breach-idUSKCN0WA24Z>

Sterling T and Deutsch A, ‘ASML Says It Suffered Intellectual Property Theft, Rejects “Chinese” Label’ (*Reuters*, 11 April 2019) <https://www.reuters.com/article/us-asml-china-spying/asml-says-it-suffered-intellectual-property-theft-rejects-chinese-label-idUSKCN1RN0DK>

‘Stock Price Altaba (Former Yahoo)’ (*Markets Insider*) <https://markets.businessinsider.com/stocks/aaba-stock>

‘Stock Price Home Depot’ (*Markets Insider*) <https://markets.businessinsider.com/stocks/hd-stock>

Swinhoe D, ‘The Biggest Data Breach Fines, Penalties and Settlements so Far’ (*CSO*, 20 December 2019) <https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html>

Van Den Bergh M, ‘Universiteit Maastricht Kampt Met Ransomware-Aanval’ (*NOS Nieuws*, 24 December 2019) <https://nos.nl/artikel/2316120-universiteit-maastricht-kampt-met-ransomware-aanval.html>

Van Dijk B and Leupen J, ‘ASML Heeft Zijn Aandeelhouders Heel Wat Uit Te Leggen over de Chinese Technologieroof’ *Financeel Dagblad* (Amsterdam, 12 April 2019) <https://fd.nl/ondernemen/1297022/asml-heeft-zijn-aandeelhouders-heel-wat-uit-te-leggen-over-de-chinese-technologieroof>
——, ‘Wat Gaat ASML Vertellen over de Spionagezaak?’ *Financieel Dagblad* (Amsterdam, 24 April 2019) <https://fd.nl/ondernemen/1298270/wat-gaat-asml-zijn-aandeelhouders-vertellen-over-de-spionagezaak>

Van Gils S, ‘Door Ransomware Getroffen Travelex Negeerde Belangrijke Update’ *Financieel Dagblad* (Amsterdam, 8 January 2020) <https://fd.nl/ondernemen/1330410/door-ransomware-getroffen-geldwisselbedrijf-travelex-negeerde-belangrijke-update#>

Dutch Court Cases

Supreme Court 2 December 1994, ECLI:NL:HR:1994:ZC1564, *NJ* 1995/288 with annotation by J.M.M. Maeijer (*Poot/ABP*)

Supreme Court 10 January 1997, ECLI:NL:HR:1997:ZC2243, *NJ* 1997/360 with annotation by J.M.M. Maeijer and *JOR* 1997/29 (*Staleman/Van de Ven*)

Supreme Court 2 May 1997, ECLI:NL:HR:1997:ZC2365, *NJ* 1997/662 with annotation by J.M.M. Maeijer (*Kip/Rabobank*)

Supreme Court 15 June 2001, ECLI:NL:PHR:2001:AB2443, *NJ* 2001/573 with annotation by J.M.M. Maeijer (*Chipshol*)

Supreme Court 29 November 2002, ECLI:NL:HR:2002:AE7011**,** *NJ* 2003/55, with annotation by J.M.M. Maeijer (*Schwandt/Berghuizer Papierfabriek*)

Supreme Court 21 February 2003, ECLI:NL:PHR:2003:AF1486, *NJ* 2003/182 with annotation by J.M.M. Maeijer (*HBG*)

Supreme Court 8 April 2005, ECLI:NL:HR:2005:AS5010, *NJ* 2006/443 with annotation by G. van Solinge; *JOR* 2005/119 with annotation by M. Brink (*Laurus*)

Supreme Court 8 December 2006, ECLI:NL:HR:2006:AZ0758, *NJ* 2006/659 with annotation by J.M.M Maeijer (*Ontvanger/Roelofsen*)

Supreme Court 16 February 2007, ECLI:NL:HR:2007:AZ0419, *NJ* 2007/256 with annotation by J.M.M. Maeijer (*Tuin Beheer*)

Supreme Court 14 September 2007, ECLI:NL:HR:2007:BA4887, *NJ* 2007/612 with annotation by J.M.M. Maeijer (*Versatel*)

Supreme Court 2 November 2007, ECLI:NL:HR:2007:BB3671, *NJ* 2008/5 with annotation by J.M.M. Maeijer (*Kessock*)

Supreme Court 20 June 2008, ECLI:NL:HR:2008:BC4959, *NJ* 2009/21 with annotation by J.M.M. Maeijer and H.J. Snijders (*Willemsen Beheer/NOM*)

Supreme Court 9 July 2010, ECLI:NL:HR:2010:BM0976, *NJ* 2010/544 with annotation by P. van Schilfgaarde (*AMSI II*)

Supreme Court 5 September 2014, ECLI:NL:HR:2014:2628, *NJ* 2015/21 with annotation by P. van Schilfgaarde and *JOR* 2014/296 with annotation by M.J. Kroeze (*Hezemans Air*)

Supreme Court 5 September 2014, ECLI:NL:HR:2014:2627, *NJ* 2015/22 with annotation by P. van Schilfgaarde and *JOR* 2014/325 with annotation by S.C.J.J. Kortmann (*RCI/Kastrop*).

Supreme Court 29 September 2017, ECLI:NL:HR:2017:2521 (*Cross Options/ING)*

Supreme Court 30 March 2018, ECLI:NL:HR:2018:470, *NJ* 2018/330 with annotation by P. van Schilfgaarde (*Eisers/TMF c.s.*)

Supreme Court 12 October 2018, ECLI:NL:HR:2018:1899, *JIN* 2018/209 with annotation by E.S. Ebels, R.A.G. de Vaan (*Potplantenkwekerij)*

Enterprise Division of the Court of Appeal of Amsterdam 9 July 1998, *JOR* 1998/122 (*Vie d'Or*)

Enterprise Division of the Court of Appeal of Amsterdam 16 October 2003, ECLI:NL:GHAMS:2003:AM1450, *JOR* 2003/260 (*Laurus*)

Enterprise Division of the Court of Appeal of Amsterdam 6 January 2005, ECLI:NL:GHAMS:2005:AR8831, *JOR* 2005/6 with annotation by M.W. Josephus Jitta (*Ahold*)

Enterprise Division of the Court of Appeal of Amsterdam 9 October 2006, *JOR* 2007/9 with annotation by De Groot

Enterprise Division of the Court of Appeal of Amsterdam 9 December 2016, *JOR* 2017/93 with annotation by Fleming

District Court Rotterdam 17 June 1999, *JOR* 1999/244 with annotation by F.J.P. van den Ingh, para 3.11.b

District Court of The Hague 14 February 2001, *JOR* 2001/90A with annotation by M.J. Kroeze

District Court of Utrecht 12 December 2007, ECLI:NL:RBUTR:2007:BB9709, *JOR* 2008/10 (*Ceteco*)

District Court of Rotterdam 14 July 2010, ECLI:NL:RBROT:2010:BN7874, *JRV* 2011/14

District Court Amsterdam 30 July 2014, ECLI:NL:RBAMS:2014:4888

District Court of The Hague 28 April 2016, ECLI:NL:RBDHA:2016:8601, *RO* 2017/17

District Court Central-Netherlands 4 February 2019, ECLI:NL:RBMNE:2019:368, *RO* 2019/48

District Court Central-Netherlands 22 May 2019, ECLI:NL:RBMNE:2019:2203, *RO* 2019/57.

Appendices

Appendix A: English translation of article 2:9 DCC

Article 2:9 DCC Performance of tasks and liability of directors
1. Each director is responsible towards the legal entity for a proper performance of his duties. To the duties of all directors belong all duties that have not been assigned by or pursuant to law or the articles of association to one or more other directors.
2. Each director is responsible for the general conduct of affairs. He is fully liable for improper management, unless, also with regard to the tasks assigned to the other directors, serious blame cannot be attributed to him and he also has not been negligent in taking measures to avert the consequences of such improper management.

Appendix B: English translation of article 6:162 DCC

Article 6:162 DCC Definition of a 'tortious act'
1. A person who commits a tortious act (unlawful act) against another person that can be attributed to him, must repair the damage that this other person has suffered as a result thereof.
2. As a tortious act is regarded a violation of someone else's right (entitlement) and an act or omission in violation of a duty imposed by law or of what according to unwritten law has to be regarded as proper social conduct, always as far as there was no justification for this behavior.
3. A tortious act can be attributed to the tortfeasor [the person committing the tortious act] if it results from his fault or from a cause for which he is accountable by virtue of law or generally accepted principles (common opinion).

Appendix C: Glossary

Risk	The possibility that events will occur and affect the achievement of strategy and business objectives.[313]
Cyber-risk	Any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems.[314]
Cyber-security	The process of protecting information by preventing, detecting, and responding to attacks.[315]
Cyber-attack	A cyber-security change that may have an impact on organizational operations (including mission, capabilities, or reputation).[316]
Cyber-incident	A cyber-attack that has been determined to have an impact on the organization prompting the need for response and recovery.[317]
Personal data	Data that relates to an individual.[318]

[313] COSO, 'Enterprise Risk Management: Aligning Risk with Strategy and Performance (draft)' (June 2016) (henceforth "COSO") 9 <https://www.coso.org/Documents/COSO-ERM-draft-Post-Exposure-Version.pdf> accessed 1 December 2019.
[314] Carolyn Williams, 'Cyber Risk and Risk Management', *Cyber Risk Resources for Practitioners* (The Institute of Risk Management 2014) <https://www.theirm.org/media/7237/irm-cyber-risk-resources-for-practitioners.pdf> accessed 20 December 2019.
[315] 'Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1' (2018) 45 <http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> accessed 12 December 2019.
[316] ibid.
[317] ibid.
[318] 'Cyber Security Guide for Businesses' (n 183) 9.

Appendix D: Proposal of the Minister of Justice regarding a new article 2:9 DCC

The new article 2:9 DCC will consist of seven paragraphs of which the first three will state:

1. Unless the articles state otherwise, the board is to manage the legal entity.
2. Each director is responsible for the general conduct of affairs. To the duties of all directors belong all duties that have not been assigned by or pursuant to law or the articles of incorporation to one or more other directors.
3. Each director is responsible towards the legal entity for a proper performance of the tasks assigned to him. When doing so, the interest of the legal entity and the company or organization connected to it are central.

Appendix E: English translation of article 2:8 paragraph 2 DCC

Article 2:8 DCC Reasonableness and fairness within the organization of the legal person

2. A rule applicable between them pursuant to law, common practice (usage), the articles of incorporation, the internal regulations (by-laws) or a resolution (decision of a body of the legal person) has no effect as far as this would be unacceptable in the given circumstances to standards of reasonableness and fairness.

Appendix F: English translation of article 2:391 paragraph 5 DCC

Article 2:391 DCC Minimum requirements annual report
5. Additional requirements may be set by Order in Council regarding the content of the annual report. These additional requirements may relate particularly to the compliance with a code of conduct which is pointed out for this purpose in that Order in Council and to the content, disclosure and audit of an opinion (certificate) on corporate governance.

Appendix G: Suggested amendment to Bpp 1.2.3 Code

Bpp 1.2.3 Monitoring of effectiveness
The management board should monitor the operation of the internal risk management and control systems and should carry out a systematic assessment of their design and effectiveness at least once a year. This monitoring should cover all material control measures relating to strategic, operational, *cyber*, compliance and reporting risks. Attention should be given to weaknesses, instances of misconduct and irregularities, indications from whistleblowers, lessons learned and findings from the internal audit function and the external auditor. Where necessary, improvements should be made to internal risk management and control systems.

Appendix H: Suggested amendment to Bpp 1.4.2 Code

Bpp 1.4.2 Accountability in the management report
In the management report, the management board should render account of:

i. the execution of the risk assessment, with a description of the principal risks facing the company in relation to its risk appetite. These risks may include strategic, operational, *cyber,* compliance and reporting risks.