Hoe dient de Nederlandse bestuurdersaansprakelijkheidsnorm te worden uitgelegd en ingevuld ten aanzien van cyberrisico's en welke rol spelen verzekeringen hierin?

Tomas Uildriks

De verwachting bestaat dat de rol van het bestuur met betrekking tot de beheersing van cyberrisico's steeds belangrijker zal worden in bestuurdersaansprakelijkheidszaken. In deze bijdrage wordt aan de hand van het bestaande privaatrechtelijk kader omtrent bestuurdersaansprakelijkheid uiteengezet hoe de bestuurdersaansprakelijkheidsnorm moet worden uitgelegd en ingevuld ten aanzien van cyberrisico's. Zowel nationale als Europese wet- en regelgeving op het gebied van cybersecurity speelt daarbij een belangrijke rol. Daarnaast bevat deze bijdrage een rechtsvergelijking met de Verenigde Staten. Anders dan in Nederland zijn in de Verenigde Staten reeds de eerste bestuurders persoonlijk aansprakelijk gesteld nadat de vennootschap was getroffen door een cyberaanval. Tot slot komt de rol van verzekeringen aan bod. De traditionele verzekeringen lijken in sommige gevallen onvoldoende aan te sluiten bij de technologische ontwikkelingen. Dit heeft eraan bijgedragen dat er in de verzekeringsmarkt een nieuw product is ontworpen: de cyberverzekering. In deze bijdrage zal worden onderzocht of een bestuurder persoonlijk aansprakelijk kan worden gesteld voor het niet afsluiten van een cyberverzekering.

1.1 Inleiding

Veel organisaties zijn door nieuwe technologieën en de toenemende digitalisering afhankelijk geworden van computersystemen en/of het internet. Hierdoor zijn ze kwetsbaarder geworden voor cyberrisico's, waaronder datalekken en gijzelingssoftware.[1] Cyberrisico's zijn één van de vijf belangrijkste zorgen voor internationale organisaties.[2] Bestuurders beseffen steeds meer dat deze risico's een negatieve impact kunnen hebben op de groeiverwachtingen en het vertrouwen van aandeelhouders.[3] Daarnaast hebben cyberrisico's potentieel grote gevolgen voor de privacy van derden. Het is dan ook opmerkelijk dat uit een recent onderzoek onder beursgenoteerde vennootschappen blijkt dat slechts 36% van de bestuurders in Nederland cybersecurity als een verantwoordelijkheid van het bestuur beschouwt.[4] Cybersecurity wordt voornamelijk gezien als een eenzijdige verantwoordelijkheid van de IT-afdeling. Volgens de Cyber Security Raad, een onafhankelijk adviesorgaan van het kabinet, is het noodzakelijk om cybersecurity op de agenda van het bestuur te plaatsen.[5] Dit is niet alleen in het belang van de organisatie, maar ook van haar bestuurders. Niet de IT-afdeling, maar het bestuur is uiteindelijk verantwoordelijk voor een gezonde bedrijfsvoering. Dit brengt met zich dat zij inzicht heeft in cyberrisico's en daartegen adequate maatregelen treft. Om de gevolgen van cyberrisico's te beperken, is het afsluiten van een (cyber)verzekering van belang. Het is de verwachting van de Cyber Security Raad dat schade in de toekomst op bestuurders zal worden verhaald.[6] De rol van het bestuur met betrekking tot de beheersing van cyberrisico's zal waarschijnlijk steeds belangrijker worden in bestuurdersaansprakelijkheidszaken.[7] In de Verenigde Staten zijn reeds de eerste bestuurders persoonlijk aansprakelijk gesteld nadat de organisatie het slachtoffer was geworden van cyberaanvallen.

Dit brengt mij tot de volgende centrale onderzoeksvraag: hoe dient de Nederlandse bestuurdersaansprakelijkheidsnorm te worden uitgelegd en ingevuld ten aanzien van cyberrisico's en welke rol spelen verzekeringen hierin? Om deze vraag te kunnen beantwoorden zal in paragraaf 1.2 eerst het juridisch kader worden geschetst. Vervolgens komt in paragraaf 1.3 de vraag aan de orde of

[1] 'Wereldwijde cyberaanval legt talloze computersystemen plat', *NRC* 12 mei 2017.
[2] AON Risk Solutions, *Global Risk Management Survey* 2017, p. 3 en p. 26.
[3] PWC, *20th CEO Survey* 2017, p. 10 en p. 23.
[4] Het onderzoek is uitgevoerd onder achthonderd beursgenoteerde ondernemingen. Zie KPMG, *Cyber security benchmark* 2017.
[5] Cyber Security Raad, 'Ieder bedrijf heeft digitale zorgplichten', 2017, p. 4.
[6] Cyber Security Raad, 'Bedrijven doen nog te weinig aan digitale veiligheid', 5 april 2017.
[7] W.C.T Weterings, 'Persoonlijke aansprakelijkheid bestuurders voor onvoldoende IT-governance', *AV&S* 2016/42, afl. 6, p. 209-210.

cybersecurity een verantwoordelijkheid van het bestuur betreft. In dezelfde paragraaf zal mede aan de hand van specifieke wet- en regelgeving op het gebied van cybersecurity worden onderzocht of, en zo ja, wanneer, deze verantwoordelijkheid leidt tot de persoonlijke aansprakelijkheid van bestuurders. Daarna volgt in paragraaf 1.4 een rechtsvergelijkend perspectief met de Verenigde Staten. In paragraaf 1.5 komt de vraag aan de orde of een bestuurder aansprakelijk kan worden gesteld voor het niet afsluiten van een cyberverzekering. Ten slotte zal ik in paragraaf 1.6 afsluiten met een conclusie.

1.2 Juridisch kader

1.2.1 Algemeen

In deze paragraaf wordt het algemene juridisch kader omtrent bestuurdersaansprakelijkheid geschetst. Daarbij komen de wettelijke grondslagen van interne aansprakelijkheid van de bestuurder jegens de vennootschap, de afgeleide actie, alsmede de externe aansprakelijkheid van bestuurders jegens derden aan bod.

1.2.2 Interne aansprakelijkheid

Algemeen

Op grond van art. 2:9 lid 1 BW is elke bestuurder tegenover de rechtspersoon gehouden tot een behoorlijke vervulling van zijn taak. Het vervullen van de bestuurstaak is in beginsel een collectieve verantwoordelijkheid. In aansprakelijkheidsprocedures van de rechtspersoon jegens de bestuurder(s) is nader bepaald wanneer sprake is van een onbehoorlijke taakvervulling.
De Hoge Raad heeft in het standaardarrest *Staleman/Van de Ven* voor het eerst bevestigd dat voor aansprakelijkheid op de voet van art. 2:9 BW is vereist dat aan de bestuurder een ernstig verwijt van onbehoorlijk bestuur kan worden gemaakt.[8] Dit vereiste is sinds 2013 expliciet in art. 2:9 lid 2 BW opgenomen.[9] Uit art. 2:9 BW kan derhalve een gedragsnorm (behoorlijke taakvervulling) en een toetsingsnorm (ernstige verwijtbaarheid) worden gedestilleerd.[10]
Door het hanteren van een hoge drempel voor aansprakelijkheid wordt rekening gehouden met de beleidsvrijheid van het bestuur en het risico van wijsheid achteraf, ook wel *hindsight bias* genoemd. Daarnaast wordt voorkomen dat bestuurders hun handelen in onwenselijke mate door defensieve overwegingen laten bepalen.[11]
Uit het bovenstaande blijkt nog niet wanneer een bestuurder een ernstig verwijt kan worden gemaakt. Dit dient te worden beoordeeld aan de hand van alle omstandigheden van het geval. Hiertoe behoren onder meer de aard en de ernst van de normschending, de aard van de door de rechtspersoon uitgeoefende activiteiten, de in het algemeen daaruit voortvloeiende risico's, de taakverdeling binnen het bestuur, de eventueel voor het bestuur geldende richtlijnen, de gegevens waarover de bestuurder beschikte of behoorde te beschikken ten tijde van de aan hem verweten beslissingen of gedragingen, alsmede het inzicht en de zorgvuldigheid die mogen worden verwacht van een bestuurder die voor zijn taak berekend is en deze nauwgezet vervult.[12] Het handelen in strijd met statutaire bepalingen die de rechtspersoon beogen te beschermen, is tevens een omstandigheid die als een zwaarwegende omstandigheid moet worden aangemerkt en in beginsel de aansprakelijkheid van de bestuurder vestigt.[13] Andere situaties

[8] HR 10 januari 1997, ECLI:NL:HR:1997:ZC2243, r.o. 3.3.1, *NJ* 1997/360, m.nt. J.M.M. Maeijer (*Staleman/Van der Ven*).
[9] Wet van 6 juni 2011, *Stb*. 2012, 275.
[10] L. Timmerman, 'Toetsing van ondernemingsbeleid door de rechter, mede in rechtsvergelijkend perspectief. Over het onderscheid tussen gedragsnormen en toetsingsnormen', *Ondernemingsrecht* 2003/15, p. 555.
[11] HR 20 juni 2008, ECLI:NL:HR:2008:BC4959, r.o. 5.3, *NJ* 2009/21, m.nt. J.M.M. Maeijer (*Willemsen/NOM*).
[12] HR 10 januari 1997, ECLI:NL:HR:1997:ZC2243, r.o. 3.3.1, *NJ* 1997/360, m.nt. J.M.M. Maeijer (*Staleman/Van der Ven*) en HR 5 september 2014, ECLI:NL:HR:2014:2627, r.o. 4.3, *NJ* 2015/22, m.nt. P. van Schilfgaarde.
[13] HR 29 november 2002, ECLI:NL:HR:2002:AE7011, r.o. 3.4.5, *JOR* 2003/2, m.nt. S.M. Bartman (*Berghuizer Papierfabriek*).

waarin sprake kan zijn van een ernstig verwijt zijn het ongeoorloofd onttrekken van middelen aan de rechtspersoon, het nemen van onnodige en niet te rechtvaardigen risico's, het nemen van beslissingen met vergaande consequenties zonder deugdelijke voorbereiding, het verstrekken van leningen aan insolvente partijen of zonder adequate zekerheden en het nalaten om adequate verzekeringen ten behoeve van de rechtspersoon af te sluiten.[14] Laatstgenoemde situatie komt in paragraaf 1.5 uitvoerig aan bod.

Afgeleide actie

Aansprakelijkheid op grond van art. 2:9 BW ziet slechts op de verhouding van de bestuurder en de vennootschap. Dit neemt niet weg dat aandeelhouders een financieel belang hebben bij het vermogen van de vennootschap. Indien de vennootschap door een onbehoorlijke taakvervulling van het bestuur schade lijdt, dalen de aandelen in waarde. Hierdoor neemt het vermogen van de aandeelhouders af. Deze waardevermindering wordt ook wel afgeleide schade genoemd.[15] Het ligt niet voor de hand dat de vennootschap vergoeding van deze schade zal vorderen en het is ongebruikelijk dat (oud)collega-bestuurders tegen elkaar procederen.[16]
De Hoge Raad heeft in het *Poot/ABP*-arrest bepaald dat aandeelhouders afgeleide schade niet rechtstreeks op de bestuurders kunnen verhalen.[17] De vennootschap zal de schade vorderen die zij als gevolg van het handelen van de bestuurder(s) lijdt. Hierdoor worden de belangen van alle aandeelhouders beschermd en niet slechts die van de procederende aandeelhouder(s). In slechts enkele gevallen is een uitzondering mogelijk. Dit is bijvoorbeeld het geval indien de schade het gevolg is van schending van een jegens aandeelhouders geldende specifieke zorgvuldigheidsnorm.[18]

1.2.3 Externe aansprakelijkheid

In het kader van de externe aansprakelijkheid van bestuurders – dat wil zeggen aansprakelijkheid jegens derden – is een tweetal regelingen van belang.
De eerste regeling heeft betrekking op de aansprakelijkheid van bestuurders indien de vennootschap failliet is gegaan. Op grond van de artikelen 2:138/248 BW is iedere bestuurder jegens de boedel hoofdelijk aansprakelijk indien het bestuur zijn taak kennelijk onbehoorlijk heeft vervuld en aannemelijk is dat dit een belangrijke oorzaak van het faillissement is. Hoewel het hier gaat om een iets ander geformuleerde norm dan die van art. 2:9 BW is in de toepassing op het concrete geval weinig verschil in uitkomst te verwachten.[19] Van kennelijk onbehoorlijk bestuur in de zin van art. 2:138/248 BW is slechts sprake als geen redelijk denkend bestuurder onder dezelfde omstandigheden aldus gehandeld zou hebben.[20]
De tweede regeling ten aanzien van de externe aansprakelijkheid heeft betrekking op aansprakelijkheid uit hoofde van onrechtmatige daad. Het betreft een actie die door een derde, zoals een individuele schuldeiser, jegens de bestuurder wordt ingesteld. Ook voor deze aansprakelijkheid geldt een hogere drempel dan in het algemeen het geval is. De Hoge Raad heeft in het *Ontvanger/Roelofsen*-arrest een eerste stap gezet naar een algemene 'ernstig verwijt'-maatstaf door twee gevaltypen te onderscheiden voor aansprakelijkheid van een bestuurder jegens schuldeisers.[21] Deze gevaltypen zien op een bestuurder die (i) namens de vennootschap heeft gehandeld dan wel (ii) heeft bewerkstelligd of toegelaten dat de vennootschap haar wettelijke of contractuele verplichtingen niet nakomt. In beide gevallen mag in het

[14] SDU Commentaar Ondernemingsrecht art. 2:9 BW, D.A.M.H.W. Strik.
[15] M.J. Kroeze, *Afgeleide schade en afgeleide actie* (diss. Utrecht), Kluwer: Deventer 2004, p. 3-4.
[16] M.J. Kroeze, L. Timmerman en J.B. Wezeman, *De kern van het ondernemingsrecht*, Deventer: Kluwer 2017, p. 181.
[17] HR 2 december 1994, ECLI:NL:HR:1994:ZC1564, *NJ* 1995/288, m.nt. J.M.M. Maeijer (*Poot/ABP*).
[18] HR 2 december 1994, ECLI:NL:HR:1994:ZC1564, *NJ* 1995/288, m.nt. J.M.M. Maeijer (*Poot/ABP*). Zie tevens L. Timmerman, 'Beginselen van bestuurdersaansprakelijkheid', *WPNR* 2016/7105, p. 324-330.
[19] M.J. Kroeze, L. Timmerman en J.B. Wezeman, *De kern van het ondernemingsrecht*, Deventer: Kluwer 2017, p. 183.
[20] HR 8 juni 2001, ECLI:NL:HR:2001:AB2053, *NJ* 2001/454 (*Panmo*).
[21] HR 8 december 2006, ECLI:NL:HR:2006:AZ0758, r.o. 3.5, *NJ* 2006/659 (*Ontvanger/Roelofsen*).

algemeen volgens de Hoge Raad slechts worden aangenomen dat de bestuurder jegens de schuldeiser van de vennootschap onrechtmatig heeft gehandeld wanneer hem, mede gelet op zijn verplichting tot een behoorlijke taakuitoefening als bedoeld in art. 2:9 BW, een voldoende ernstig verwijt kan worden gemaakt.[22] Het is nog onduidelijk hoe het criterium van ernstig verwijtbaarheid van art. 2:9 BW moet worden ingepast in de structuur van art. 6:162 BW. Er wordt in de literatuur verschillend gedacht over de vraag of de ernstig verwijtbaarheid het onderdeel van de onrechtmatigheid of die van de toerekenbaarheid van art. 6:162 BW 'inkleurt'.[23] In de 'septemberarresten' van 2014 heeft de Hoge Raad nogmaals benadrukt dat er een hoge drempel voor aansprakelijkheid van bestuurders geldt. Indien een vennootschap een onrechtmatige daad pleegt, geldt als uitgangpunt dat alleen de vennootschap aansprakelijk is voor de daaruit voortvloeiende schade. Slechts onder bijzondere omstandigheden is, naast aansprakelijkheid van de vennootschap, ook ruimte voor aansprakelijkheid van een bestuurder van een vennootschap. Hier is voor vereist dat die bestuurder ter zake van de benadeling persoonlijk een ernstig verwijt kan worden gemaakt. De ernst van de normschending en de overige omstandigheden van het geval geven invulling aan het criterium van 'persoonlijk een ernstig verwijt'.[24]

1.3 Verantwoordelijkheid en aansprakelijkheid bij cyberrisico's

1.3.1 Algemeen

Op zowel nationaal als Europees niveau komt op het gebied van cybersecurity steeds meer wet- en regelgeving. Dit brengt verschillende verplichtingen met zich voor zowel beurs- als niet-beursgenoteerde vennootschappen en haar bestuurders. Zij zijn verantwoordelijk voor de naleving ervan. Het bestuur draagt namelijk naast de verantwoordelijkheid voor de dagelijkse gang van zaken ook de verantwoordelijkheid voor de naleving van wet- en regelgeving en de beheersing van de risico's die voortvloeien uit de ondernemingsactiviteiten.[25] Dit blijkt onder meer uit de Nederlandse Corporate Governance Code.[26] Deze gedragscode geeft invulling aan de bestuurstaak en bevat principes en best practice-bepalingen voor beursgenoteerde vennootschappen. Het onderwerp cybersecurity heeft, na advies van de Cyber Security Raad, een plaats gekregen bij de taken en verantwoordelijkheden van de auditcommissie.[27]
Met betrekking tot wet- en regelgeving op het gebied van cybersecurity zal ik mij richten op de beveiligingsplicht en de meldplicht datalekken uit de Wet bescherming persoonsgegevens (Wbp) en de Algemene Verordening Gegevensbescherming (AVG). Uit deze verplichtingen vloeit naar mijn mening de verantwoordelijkheid van bestuurders ten aanzien van cyberrisico's voort. Opgemerkt dient te worden dat de AVG de Wbp per 25 mei 2018 vervangt.[28]
Organisaties die persoonsgegevens verwerken, dienen op grond van art. 13 Wbp passende technische en organisatorische beveiligingsmaatregelen te nemen tegen verlies of enige vorm van onrechtmatige verwerking. Deze beveiligingsmaatregelen dienen een passend beveiligingsniveau te garanderen. Voorts geldt sinds 1 januari 2016 de meldplicht datalekken zoals vermeldt in art. 34a Wbp. In art. 33 AVG is een soortgelijke meldplicht opgenomen. In het geval van een inbreuk op de beveiliging dienen organisaties de Autoriteit Persoonsgegevens onverwijld in kennis te stellen, indien de inbreuk leidt tot de aanzienlijke

[22] HR 8 december 2006, ECLI:NL:HR:2006:AZ0758, r.o. 3.5, *NJ* 2006/659 (*Ontvanger/Roelofsen*).
[23] M.J. Kroezen en C. Assers, *Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 2. Rechtspersonenrecht. Deel I. De rechtspersoon*, Deventer: Kluwer 2015, p.187.
[24] HR 5 september 2014, ECLI:NL:HR:2014:2628, *NJ* 2015/21, m.nt. P. van Schilfgaarde en HR 5 september 2014, ECLI:NL:HR:2014:2627, r.o. 4.3, *NJ* 2015/22, m.nt. P. van Schilfgaarde.
[25] D.A.M.H.W. Strik, *Grondslagen bestuurdersaansprakelijkheid. Een maatpak voor de Board Room*, Deventer: Kluwer 2010, p. 275.
[26] Principe 1.2 van de Herziene Corporate Governance Code 2016.
[27] Principe 1.5.1 van de Herziene Corporate Governance Code 2016.
[28] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

kans op ernstige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. De Autoriteit Persoonsgegevens heeft per 1 januari 2016 de bevoegdheid gekregen om op grond van art. 66 Wbp aan een rechtspersoon en/of haar bestuurder een bestuurlijke boete op te leggen. De boete kan worden opgelegd voor het overtreden van de meldplicht datalekken en het niet op orde hebben van beveiligingsmaatregelen. De hoogte van de boete bedraagt maximaal € 820.000 of 10% van de jaaromzet van de rechtspersoon. Onder de AVG zal de boetebevoegdheid worden verhoogd tot maximaal € 20.000.000 of 4% van de wereldwijde jaaromzet. De Autoriteit Persoonsgegevens heeft tot op heden nog geen gebruik gemaakt van haar boetebevoegdheid.[29] Hoewel de boete primair aan de rechtspersoon kan worden opgelegd, blijkt uit de Parlementaire Geschiedenis dat daarnaast of in plaats daarvan de bestuurder kan worden beboet.[30] De bestuurlijke boete heeft een punitief karakter en valt derhalve buiten de privaatrechtelijke aansprakelijkheid.[31] Voor de vraag of de bestuurder kan worden beboet, dient dan ook te worden aangehaakt bij de strafrechtelijke jurisprudentie.[32]
De verantwoordelijkheid van bestuurders ten aanzien van cyberrisico's die uit bovenstaande wet- en regelgeving voortvloeit, impliceert een mogelijke aansprakelijkheid van het bestuur.

1.3.2 Interne aansprakelijkheid

De vordering van art. 2:9 BW wordt in de praktijk vooral gebruikt door de curator in geval van faillissement van de rechtspersoon. Dit gebeurt meestal samen met een vordering uit hoofde van art. 2:138/248 BW. Zittende bestuurders stellen hun medebestuurders in de regel niet aansprakelijk.[33]
Ten aanzien van cyberrisico's zijn de aard van de door de rechtspersoon uitgeoefende activiteiten en de in het algemeen daaruit voortvloeiende risico's mijns inziens de meest relevante omstandigheden voor de vaststelling van een 'ernstig verwijt'. Deze omstandigheden zijn namelijk van belang in het kader van risicobeheersing. Risicobeheersing impliceert dat het bestuur inzicht heeft in de mogelijke risico's om daar vervolgens adequaat op te reageren.
In de literatuur en rechtspraak worden verschillende voorbeelden genoemd waarin sprake kan zijn van een ernstig verwijt.[34] Een aantal van deze voorbeelden heb ik in het juridisch kader beschreven. Van de voorbeelden lijkt slechts het nemen van beslissingen met verregaande consequenties zonder deugdelijke voorbereiding een rol van betekenis te kunnen spelen. Het belang van risicoanalyses dient daarbij niet te worden onderschat, omdat ze het bestuur in staat stellen weloverwogen beslissingen te nemen. Besluitvorming zonder een zorgvuldige risicoanalyse kan tot gevolg hebben dat bestuurders een ernstig verwijt is te maken waarmee zij hun taak jegens de rechtspersoon kennelijk onbehoorlijk vervullen.[35] Dit kan bijvoorbeeld het geval zijn indien het bestuur de prioriteit geeft aan bezuinigingen op de IT-systemen, terwijl het onderkent dat deze systemen verouderd en/of verzwakt zijn.
Volgens Assink moet het bestuur er voor zorgen dat het tijdig van de juiste informatie wordt voorzien over de gang van zaken binnen de vennootschap.[36] De vennootschap dient hiervoor op grond van art. 2:141/251 BW over een systeem van risicobeheersing en interne controle te beschikken.[37] De vereisten die per onderneming aan dergelijke systemen mogen worden gesteld, zullen volgens Strik onder meer

[29] Te vinden via https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/overzichten-meldingen-datalekken.
[30] *Kamerstukken I* 2014/15, 33662, C, p. 20-21.
[31] T.F.E. Tjong Tjin Tai, 'Aansprakelijkheid bij datalekken', *WPNR* 2016/7110, p. 459-464.
[32] HR 16 december 1986, ECLI:NL:HR:1986:AC9607, *NJ* 1987/321, m.nt. A.C. 't Hart.
[33] M.J. Kroezen en C. Assers, *Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 2. Rechtspersonenrecht. Deel I. De rechtspersoon*, Deventer: Kluwer 2015, p. 190.
[34] Zie SDU Commentaar Ondernemingsrecht art. 2:9 BW, D.A.M.H.W. Strik en M.J. Kroezen en C. Assers, *Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 2. Rechtspersonenrecht. Deel I. De rechtspersoon*, Deventer: Kluwer 2015, p. 190.
[35] M.J. Kroezen en C. Assers, *Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 2. Rechtspersonenrecht. Deel I. De rechtspersoon*, Deventer: Kluwer 2015, p. 190 en Rechtbank Utrecht 12 december 2007, *JOR* 2008/10, r.o. 5.105.
[36] B.F. Assink, *Rechterlijke toetsing van bestuurlijk gedrag*, Deventer: Kluwer 2007, p. 519.
[37] Rechtbank Zwolle 11 december 2002, ECLI:NL:RBZWO:2002:AF4895, r.o. 4.5.

afhangen van de aard van de onderneming en de aard van de gelopen risico's.[38] Het bestuur heeft ter zake van de opzet en inrichting van het systeem een zekere mate van beleidsvrijheid. De algehele afwezigheid van – of aanwezigheid van gebrekkige – controlesystemen kan in het algemeen leiden tot de conclusie dat sprake is van onbehoorlijke taakvervulling.[39] Van een ernstig verwijt kan vervolgens sprake zijn als het bestuur bijvoorbeeld waarschuwingssignalen krijgt dat het systeem niet effectief is en nalaat daartegen op te treden.
De aanvoer van informatie met betrekking tot cyberrisico's zal bij grote ondernemingen vaak afkomstig zijn van de IT-afdeling. Deze afdeling zal dergelijke risico's dagelijks moeten signaleren en aanpakken. Communicatie met het bestuur hieromtrent is essentieel omdat het bestuur toezicht op dit proces dient te houden. Voor een effectieve aanpak van cyberrisico's is derhalve een top-down betrokkenheid en communicatie vereist.[40]

1.3.3 Externe aansprakelijkheid wegens schending van art. 13 Wbp?

Externe aansprakelijkheid jegens derden heeft betrekking op aansprakelijkheid uit hoofde van onrechtmatige daad. Deze vordering wordt door een derde jegens de bestuurder ingesteld. Bij de uiteenzetting van het juridisch kader heb ik beschreven dat slechts onder bijzondere omstandigheden, naast aansprakelijkheid van de vennootschap, ook ruimte voor aansprakelijkheid van een bestuurder van een vennootschap is. Het is derhalve van belang om te onderzoeken of een derde een vennootschap aansprakelijk kan stellen wegens schending van de beveiligingsplicht van art. 13 Wbp. Dit zal ik doen aan de hand van de vijf elementen die gelegen zijn in art. 6:162 BW: onrechtmatige daad, toerekenbaarheid, schade, causaliteit en relativiteit. Vervolgens zal worden onderzocht of er ook ruimte is voor aansprakelijkheid van een bestuurder van de vennootschap.
Het schenden van de beveiligingsplicht van art. 13 Wbp kan in het kader van art. 6:162 lid 2 BW worden aangemerkt als een doen of nalaten in strijd met een wettelijke plicht en kan dus als onrechtmatige daad worden aangemerkt. Wel geldt dat een bestuurder pas aansprakelijk kan worden gehouden indien sprake is van een ernstig verwijt: daar ga ik hierna nader op in.
Voor aansprakelijkheid krachtens art. 6:162 BW is tevens vereist dat de onrechtmatige daad aan de dader kan worden toegerekend. Mijns inziens dient de onrechtmatige daad op grond van art. 6:162 lid 3 BW krachtens de in het verkeer geldende opvattingen aan de rechtspersoon te worden toegerekend.
Ten aanzien van datalekken wordt in de Parlementaire Geschiedenis opgemerkt dat burgers door het verlies, onrechtmatig gebruik of misbruik van persoonsgegevens in hun belangen worden geschaad. De schade die daaruit voortvloeit kan zowel van materiële of immateriële aard zijn, zoals bijvoorbeeld onrechtmatige publicatie, aantasting in eer en goede naam, identiteitsfraude en discriminatie.[41] Bij materiële schade ingeval van datalekken moet vooral gedacht worden aan identiteitsfraude, zoals het kopen van spullen en het aanvragen van creditcards op andermans naam. De schade zal derhalve veelal gering zijn. Slechts bij hoge uitzondering zal een datalek tot immateriële schade leiden.[42] Naast materiële en immateriële schade kan een datalek ook tot gevolg hebben dat een derde kosten moet maken ter voorkoming of beperking van schade, zoals het voorkomen van (verdere) verspreiding van gegevens.[43] Deze kosten komen in beginsel op grond van art. 6:96 lid 2 sub a BW voor vergoeding in aanmerking.

[38] D.A.M.H.W. Strik, *Grondslagen bestuurdersaansprakelijkheid. Een maatpak voor de Board Room*, Deventer: Kluwer 2010, p. 283-284.
[39] D.A.M.H.W. Strik, *Grondslagen bestuurdersaansprakelijkheid. Een maatpak voor de Board Room*, Deventer: Kluwer 2010, p. 283-284.
[40] W.C.T. Weterings, 'Persoonlijke aansprakelijkheid bestuurders voor onvoldoende IT-governance', *AV&S* 2016/42, p. 209.
[41] *Kamerstukken II* 2013/2014, 33662, nr. 6, p. 19.
[42] T.F.E. Tjong Tjin Tai, 'Aansprakelijkheid bij datalekken', *WPNR* 2016/7110, p. 459-464.
[43] Rechtbank Amsterdam 10 augustus 2011, ECLI:NL:RBAMS:2011:BT1877, r.o. 4.7.

Met betrekking tot de causaliteit wijst Tjong Tjin Tai er op dat dit lastig te bewijzen kan zijn. Het is immers niet onmogelijk dat de gegevens via een andere weg zijn uitgelekt, al dan niet door het handelen van de betrokkenen individu zelf.[44]
Aan de relativiteitseis van art. 6:163 BW zal bij een datalek jegens de betrokkene worden voldaan.[45] De beveiligingsplicht van art. 13 Wbp strekt er immers onder andere toe persoonsgegevens te beveiligen tegen enige vorm van onrechtmatige verwerking. Hieruit kan worden afgeleid dat de norm van art. 13 Wbp de strekking heeft de benadeelde in het geschonden belang te beschermen.
Het voorgaande laat zien dat schending van art. 13 Wbp door de vennootschap een onrechtmatige daad jegens een derde kan opleveren. Voor aansprakelijkheid van een bestuurder van de vennootschap is vereist dat die bestuurder ter zake van de benadeling persoonlijk een ernstig verwijt kan worden gemaakt.[46] Van de twee gevaltypen zoals geformuleerd in het *Ontvanger/Roelofsen*-arrest zal ingeval van schending van de beveiligingsplicht mijns inziens niet snel sprake zijn. Beide gevaltypen zien op onbetaald gebleven schuldeisers.[47] Een datalek zal in beginsel niet een onbetaald gebleven schuld tot gevolg hebben.
Op grond van de rechtspraak wordt de invulling van art. 6:162 BW ingekleurd door de norm van art. 2:9 BW.[48] Dit betekent dat voor de vraag of de bestuurder ter zake van de benadeling een ernstig verwijt kan worden gemaakt, moet worden gekeken naar alle omstandigheden van het geval. Ook bij de externe aansprakelijkheid van de bestuurder ten aanzien van cyberrisico's, waaronder datalekken, zullen de aard van de door de rechtspersoon uitgeoefende activiteiten en de in het algemeen daaruit voortvloeiende risico's mijns inziens de meest relevante omstandigheden zijn. Deze omstandigheden zijn bepalend voor de redelijkerwijs te nemen maatregelen ter voorkoming van cyberrisico's.
Van de in de literatuur genoemde voorbeelden waarin sprake kan zijn van ernstig verwijtbaar handelen, is opvallend dat slechts het voorbeeld van het nemen van onnodige en niet te rechtvaardigen risico's een mogelijke rol speelt. [49] Daarbij kan gedacht worden aan de omstandigheid dat een bestuurder de welbewuste keuze maakt om te bezuinigen op IT-systemen, terwijl hij dat gezien de aard van de door de rechtspersoon uitgeoefende activiteiten niet had behoren te doen. Hiermee neemt hij een niet te rechtvaardigen risico dat de persoonsgegevens van derden worden gelekt. Indien een bestuurder deze veiligheidsrisico's laat voortbestaan en een cyberrisico zich vervolgens verwezenlijkt, kan dat mijns inziens een ernstig verwijt opleveren.

Uit het voorgaande kan worden geconcludeerd dat van een ernstig verwijt slechts in uitzonderlijke gevallen sprake zal zijn. Het blijkt lastig om de gevolgen van cyberrisico's in te passen in het bestaande privaatrechtelijke kader omtrent bestuurdersaansprakelijkheid. Daarnaast is gebleken dat de causaliteit en schade omtrent de externe aansprakelijkheid van bestuurders complicerende elementen zijn.

1.4 Rechtsvergelijkend perspectief

1.4.1 De situatie in de Verenigde Staten

Anders dan in Nederland zijn in de Verenigde Staten reeds de eerste bestuurders persoonlijk aansprakelijk gesteld nadat de vennootschap was getroffen door een cyberaanval. Dat is aanleiding om te onderzoeken

[44] T.F.E. Tjong Tjin Tai, 'Aansprakelijkheid bij datalekken', *WPNR* 2016/7110, p. 459-464.
[45] T.F.E. Tjong Tjin Tai, 'Aansprakelijkheid bij datalekken', *WPNR* 2016/7110, p. 459-464.
[46] HR 5 september 2014, ECLI:NL:HR:2014:2628, *NJ* 2015/21, m.nt. P. van Schilfgaarde en HR 5 september 2014, ECLI:NL:HR:2014:2627, r.o. 4.3, *NJ* 2015/22, m.nt. P. van Schilfgaarde.
[47] M.J. Kroeze, L. Timmerman en J.B. Wezeman, *De kern van het ondernemingsrecht*, Deventer: Kluwer 2017, p. 187-189.
[48] Zie bijvoorbeeld HR 2 maart 2007, ECLI:NL:HR:2007:AZ3535, *NJ* 2007/240, m.nt. J.M.M. Maeijer (*Holding Nutsbedrijf Westland NV*).
[49] Zie SDU Commentaar Ondernemingsrecht art. 2:9 BW, D.A.M.H.W. Strik en M.J. Kroezen en C. Assers, *Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 2. Rechtspersonenrecht. Deel I. De rechtspersoon*, Deventer: Kluwer 2015, p. 190.

op welke wijze in de Verenigde Staten invulling aan de bestuurdersaansprakelijkheidsnorm wordt gegeven. Dit deel van de bijdrage is derhalve rechtsvergelijkend van aard. Ik bespreek eerst de in de rechtspraak ontwikkelde *business judgment rule*. Dit rechtsfiguur speelt een centrale rol bij de persoonlijke aansprakelijkheid van bestuurders en bouwt voor een belangrijk deel voort op de op bestuurders rustende fiduciaire plichten jegens de vennootschap en haar aandeelhouders.[50] Deze fiduciaire plichten komen na de bespreking van de *business judgment rule* aan bod. Daarna volgt een analyse van de desbetreffende bestuurdersaansprakelijkheidszaken.

1.4.2 Business Judgment rule

Het Amerikaanse vennootschapsrecht wordt door iedere staat zelfstandig bepaald. De meeste vennootschappen in de Verenigde Staten zijn geïncorporeerd in de staat Delaware.[51] Dit geldt ook ten aanzien van vier van de vijf te bespreken vennootschappen waarvan de bestuurders aansprakelijk zijn gesteld. In het kader van deze bijdrage zal ik mij dan ook voornamelijk richten op het recht van deze staat. Het vennootschapsrecht van Delaware wordt beheerst door de Delaware General Corporation Law (DGCL). Op grond van § 141(a) van de DGCL geldt het uitgangspunt dat de vennootschap wordt bestuurd door of onder leiding van het bestuur. Bij de vervulling van deze taak rusten op het bestuur fiduciaire plichten jegens de vennootschap en haar aandeelhouders.[52] De *business judgment rule* is gebaseerd op bovenvermelde wettelijke bepaling. Het is een niet gecodificeerde vorm van rechterlijke toetsing van bestuurlijk gedrag.[53] De *business judgment rule* is derhalve een toetsingsnorm die bepaalt of bestuurders zich volgens de voor hen geldende gedragsnorm hebben gedragen.[54] De Supreme Court van Delaware heeft bepaald dat de *business judgment rule* een weerlegbaar vermoeden behelst dat bestuurders bij het maken van zakelijke beleidsafwegingen goed geïnformeerd en te goeder trouw handelden en dat zij in de volle overtuiging waren dat dit handelen in het belang van de vennootschap was.[55] Het is aan een eiser om dit vermoeden te ontzenuwen.[56] De rechter toetst het met de gemaakte zakelijke beleidsafweging verband houdende bestuurlijke gedrag slechts aan de op het bestuur rustende fiduciaire plichten. De zakelijke beleidsafweging wordt niet inhoudelijk beoordeeld.[57]

1.4.3 Fiduciaire plichten

Ten aanzien van de fiduciaire plichten wordt een onderscheid gemaakt tussen de loyaliteitsplicht (*duty of loyalty*) en de zorgvuldigheidsplicht (*duty of care*). De plicht om te goeder trouw te handelen (*duty of good faith)*, wordt sinds 2006 onder de bredere loyaliteitsplicht geschaard.[58] De loyaliteitsplicht behelst in essentie dat het bestuur de belangen van de vennootschap en haar aandeelhouders boven haar eigen persoonlijke belangen plaatst.[59] De Supreme Court van Delaware heeft in 2006 bepaald dat een bestuurder zijn *duty of good faith* schendt wanneer hij opzettelijk handelt met een ander doel dan het bevorderen van de belangen van de vennootschap.[60]

---

[50] B.F. Assink, *Rechterlijke toetsing van bestuurlijk gedrag*, Deventer: Kluwer 2007, p. 100-103.
[51] Meer dan 1.000.000 vennootschappen zijn in Delaware gevestigd. Daarnaast zijn meer dan 66% van alle beursgenoteerde vennootschappen in de Verenigde Staten in Delaware geïncorporeerd, inclusief 66% van de vennootschappen die deel uitmaken van de Fortune 500.
[52] *Cede & Co. v. Technicolor, Inc.*, 634 A.2d 345 (Del. 1993).
[53] *Omnicare, Inc. v. NCS Healthcare, Inc.*, 818 A.2d 914 (Del. 2003).
[54] M.A. Eisenberg, 'The divergence of standards of conduct and standards of review in corporate law', *Fordham Law Review* 1993, p. 437.
[55] *Aronson v. Lewis*, 437 A.2d 805 (Del. 1984).
[56] B.F. Assink, 'Kan de Delaware business judgment rule wat betekenen voor het Nederlandse vennootschapsrecht, specifiek het enquêterecht?', *Ondernemingsrecht* 2008/6, p. 232.
[57] *In re Caremark International, Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996). Zie tevens X. Li, *A comparative study of shareholders'derivative actions*, Deventer: Kluwer 2007, p. 146.
[58] *Stone v. Ritter*, 911 A.2d 362 (Del. 2006).
[59] *Cede & Co. v. Technicolor, Inc.*, 634 A.2d 345 (Del. 1993).
[60] *In re Walt Disney Co. Derivative Litigation*, 906 A.2d 27 (Del. 2006).

De zorgvuldigheidsplicht houdt onder meer in dat het bestuur voorafgaand aan het nemen van zakelijke beleidsafwegingen acht dient te slaan op alle materiële informatie die redelijkerwijs beschikbaar is.[61] De zorgvuldigheidsplicht hangt nauw samen met het toezicht van het bestuur. Deze component wordt ook wel de *duty of oversight* genoemd en speelt een centrale rol in de nog te bespreken procedures. De toezichthoudende functie van het bestuur houdt een verplichting in om ervoor te zorgen dat er een adequaat informatie- en rapportagesysteem bestaat.[62] In de zaak *In re Caremark International, Inc. Derivative Litigation* stelden de eisers dat de bestuurders hun *duty of oversight* hadden geschonden door een situatie in het leven te roepen waarin de vennootschap werd blootgesteld aan een groot aansprakelijkheidsrisico. De Supreme Court van Delaware heeft in de zaak *Stone v. Ritter* de redenering van *Caremark* bevestigd. Er is sprake van een schending van de *duty of oversight* indien: ''(a) the directors utterly failed to implement any reporting or information systems or control; or (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention."[63] Van persoonlijke aansprakelijkheid wegens schending van de *duty of oversight* is slechts sprake indien het bestuur deze plicht bewust negeert of te kwader trouw handelt.[64]

1.4.4 Derivative suits

Er is een beperkt aantal zaken waarin bestuurders persoonlijk aansprakelijk zijn gesteld in verband met cyberaanvallen. In alle gevallen zijn het aandeelhouders die jegens de bestuurders procederen en niet zozeer klanten: zie nader de in par. 1.2.2. besproken afgeleide acties. Daarbij dient in de Verenigde Staten een onderscheid te worden gemaakt tussen afgeleide en directe acties. De directe acties zien op misleidende mededelingen van bestuurders waardoor de aandelen van de vennootschap in waarde zijn gedaald. In het kader van deze bijdrage worden deze directe acties buiten beschouwing gelaten. De grondslag van de desbetreffende vorderingen ziet immers op handelingen van bestuurders na een cyberaanval.
Een afgeleide actie wordt een *derivative suit* genoemd. Een derivative suit is een rechtsvordering tot vergoeding van door de vennootschap geleden schade, ingesteld door een of meer aandeelhouders ten behoeve van de vennootschap. De rechtsvordering wordt ingesteld op eigen naam, maar de toegekende schadevergoeding komt in beginsel ten goede aan de vennootschap. Hierdoor profiteren ook de aandeelhouders die met het instellen van de vordering niets te maken hebben.[65]
Aandeelhouders hebben sinds 2014 derivative suits ingesteld jegens de bestuurders van de volgende vennootschappen: Target, Wyndham Worldwide, Home Depot, Wendy's en Yahoo. Al deze vennootschappen zijn getroffen door cyberaanvallen waarbij (creditcard)gegevens van klanten zijn gestolen. De grondslag voor persoonlijke aansprakelijkheid van bestuurders in alle derivative suits is gelegen in de schending van hun fiduciaire plichten, in het bijzonder de *duty of oversight*. De procedures zijn voor de eisende aandeelhouders tot op heden niet succesvol verlopen. Al in een vroeg stadium zijn de procedures jegens de bestuurders van Target, Wyndham Worldwide en Home Depot in een *motion to dismiss* afgewezen. Dit lijkt voornamelijk te komen door de hoge drempel die geldt voor het instellen van een derivative suit. In laatstgenoemde zaak is echter recent een schikking bereikt. De overige twee procedures zijn nog aanhangig.
Een belangrijke oorzaak voor het verloop van deze procedures is gelegen in de (strenge) procedurele vereisten. Deze spelen bij derivative suits vaak een belangrijkere rol dan de inhoud van de vordering.[66] Zo kan een derivative suit slechts worden ingesteld nadat een aandeelhouder het bestuur van de vennootschap schriftelijk heeft verzocht passende maatregelen te nemen, zoals het instellen van een vordering tot

[61] *Smith v. Van Gorkom*, 488 A.2d 858 (Del. 1985).
[62] *In re Caremark International, Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996).
[63] *Stone v. Ritter*, 911 A.2d 362 (Del. 2006).
[64] *In re Citigroup Inc. Shareholder Derivative Litigation*, 964 A2d 106 (Del. Ch. 2009).
[65] M.J. Kroeze, *Afgeleide schade en afgeleide actie*, Deventer: Kluwer 2004, p. 193-194.
[66] M.J. Kroeze, *Afgeleide schade en afgeleide actie*, Deventer: Kluwer 2004, p. 201.

schadevergoeding.[67] Een dergelijk verzoek kan achterwege worden gelaten indien het zinloos zou zijn. Om dit te bewijzen, dient de aandeelhouder aan te tonen dat de zakelijke beleidsafweging de *business judgment rule* niet zal doorstaan en er een aanmerkelijke kans bestaat dat de bestuurders aansprakelijk zullen worden gehouden.[68]
De rechter in de Home Depot-zaak erkende in zijn vonnis van 30 november 2016 dat dit voor de aandeelhouder een grote horde is om te nemen.[69] De aandeelhouder stelde primair dat niemand binnen de vennootschap door het bestuur was aangewezen voor de controle en rapportage ten aanzien van gegevensbeveiliging. Het bestuur had de toezichthoudende commissie voor cybersecurity ontbonden en de verantwoordelijkheid overgedragen aan de auditcommissie. Het handvest van de auditcommissie was echter niet gewijzigd. Dit argument vond de rechter te formeel. De auditcommissie ontving namelijk regelmatig verslag over cybersecurity en informeerde het bestuur hierover. Daarnaast stelde de aandeelhouder dat het bestuur er niet voor heeft gezorgd dat er een plan aanwezig was om de tekortkoming in het beveiligingssysteem onmiddellijk te verhelpen. De rechter vond dit argument onvoldoende om kwade trouw aan te nemen omdat er wel degelijk een plan aanwezig was. Dat dit plan achteraf gezien niet goed genoeg was, doet daar niet aan af. Nadat de aandeelhouder hoger beroep had ingesteld, is door partijen een schikking bereikt. De schikking is op 28 april 2017 ter goedkeuring aan de rechtbank voorgelegd. Blijkens het verzoek heeft Home Depot ingestemd met het nemen van verschillende corporate governance hervormingen met betrekking tot cybersecurity. Daarnaast zal Home Depot ruim een miljoen dollar aan proceskosten vergoeden.[70]
In de Target-zaak heeft de District Court van Minnesota zich op 7 juli 2016 aan het advies van een *special litigation committee* geconformeerd dat het niet in Target's belang was om namens de vennootschap tegen haar (ex)bestuurders te procederen.[71] Deze beoordeling staat los van een materiële beoordeling van de zaak en zal derhalve buiten beschouwing worden gelaten.
In de Wyndham Worldwide-zaak heeft het bestuur het verzoek van de aandeelhouder om een vordering tot schadevergoeding in te stellen, afgewezen. De aandeelhouder is er vervolgens niet in geslaagd om te bewijzen dat de zakelijke beleidsafweging op basis van onredelijk onderzoek is gemaakt. Volgens de rechter was er wel degelijk sprake van een redelijk onderzoek. Nog voor het verzoek van de aandeelhouder zijn de cyberaanvallen op veertien bestuursvergaderingen aan bod gekomen. Voorts zijn aanbevelingen met betrekking tot cybersecurity van ingehuurde IT-bedrijven uitgevoerd. Hieruit volgt dat de zakelijke beleidsafweging van het bestuur om geen vordering tot schadevergoeding in te stellen, wordt beschermd onder de *business judgment rule*. Dit heeft ertoe geleid dat de vorderingen van de aandeelhouder bij vonnis van 20 oktober 2014 zijn afgewezen.[72]

1.4.5 Betekenis voor Nederland

Uit bovenstaande procedures blijkt dat aandeelhouders (en hun advocaten) er tot op heden niet in zijn geslaagd om bestuurders van door cyberaanvallen getroffen vennootschappen met succes aansprakelijk te stellen. Dit komt voornamelijk door de hoge drempel die geldt voor het instellen van een derivative suit. Aan de materiële overwegingen ten aanzien van aansprakelijkheid kan derhalve slechts beperkte betekenis worden toegekend. De bereikte schikking in de Home Depot-zaak kan worden opgevat als een klein succes voor de eisende zijde. De recente dagvaardingen jegens de bestuurders van Wendy's[73] en

[67] Rule 23.1 van de *Federal Rules of Civil Procedure* en Rule 23.1 van de Court of Chancery van de staat Delaware. Zie tevens M.G. Kuijpers, 'Is toepassing van de Amerikaanse derivative suit in het Nederlandse recht zinvol?', *WPNR* 2002/6389, p. 101.
[68] *Aronson v. Lewis*, 437 A.2d 805 (Del. 1984).
[69] *In re The Home Depot, Inc. Shareholder Derivative Litigation*, 1:15-CV-2999-TWT (Northern District Court of Georgia 2016).
[70] Motion for preliminary approval of settlement *In re The Home Depot, Inc. Shareholder Derivative Litigation*, 1:15-CV-2999-TWT (Northern District Court of Georgia 2016).
[71] *Davis, et al. v. Steinhafel, et al.*, 14-CV-203-PAM/JJK (District Court of Minnesota 2016).
[72] *Palkon v. Holmes*, C.A. No. 2:14-CV-01234 (SRC) (District Court of New Jersey 2014).
[73] *Graham, et al. v. Peltz, et al.*, No. 1:16-cv-1153 (Southern District Court of Ohio 2016).

Yahoo[74] laten zien dat zij blijven proberen om bestuurders middels afgeleide acties verantwoordelijk te houden voor schending van hun fiduciaire plichten. De verplichting van het bestuur om te zorgen voor een adequaat informatie- en rapportagesysteem vervult ook in deze procedures een belangrijke rol. Naar mijn mening kan deze verplichting in Nederlandse procedures relevant zijn voor interne aansprakelijkheid van bestuurders op grond van art. 2:141/251 BW. Daarbij dient te worden opgemerkt dat schending van art. 2:141/251 BW geen grondslag voor externe aansprakelijkheid op grond van art. 6:162 BW kan zijn. Er zal niet worden voldaan aan het relativiteitsvereiste van art. 6:163 BW. De Hoge Raad heeft in het *Poot/ABP*-arrest immers bepaalt dat aandeelhouders slechts afgeleide schade kunnen vorderen indien de schade het gevolg is van schending van een jegens aandeelhouders geldende specifieke zorgvuldigheidsnorm. [75] Art. 2:141/251 BW strekt echter niet specifiek ter bescherming van aandeelhouders.[76] In het kader van de aansprakelijkheid van bestuurders benadrukken de zaken van Wyndham Worldwide en Home Depot het belang van een adequaat informatie- en rapportagesysteem. Zodra informatie over cyberrisico's het bestuur bereikt en zij serieus aandacht aan dit onderwerp besteden, worden zij in zekere mate beschermd.

1.5 Rol van (cyber)verzekering

1.5.1 Algemeen

Bij de beheersing van cyberrisico's vormt het afsluiten van een verzekering het sluitstuk van ICT-risicomanagement.[77] Het niet afsluiten van de gebruikelijke en noodzakelijke verzekeringen is een situatie waarin van een ernstig verwijt sprake kan zijn.[78] In dit deel van de bijdrage komt de vraag aan bod of een bestuurder persoonlijk aansprakelijk kan worden gesteld voor het niet afsluiten van een cyberverzekering.

1.5.2 Cyberschade

Cyberincidenten kunnen grote financiële gevolgen hebben voor organisaties. Uit het jaarrapport 2016 van het bedrijf Target blijkt bijvoorbeeld dat datalekken de organisatie al 292 miljoen dollar hebben gekost.[79] Er zijn verschillende vormen van cyberschade. Daarbij kan een onderscheid worden gemaakt tussen schade van de eigen organisatie en door derden geleden schade. Onder eigen schade kan gedacht worden aan bedrijfsstilstand, gederfde winst, kosten om schade aan systemen en/of processen te herstellen, boetes en crisismanagementkosten. Veelal is er ook sprake van reputatieschade.[80] Cyberincidenten kunnen tevens leiden tot schade aan derden, zoals schade door identiteitsfraude.[81] Bij zowel schade van derden als van de organisatie is het aannemelijk dat een bedrijf dat schade heeft geleden door datalekken, een beroep zal willen doen op een verzekering. Het is echter de vraag of de schade onder een traditionele verzekering is gedekt. Dit heeft te maken met de dekkingsomvang van deze verzekeringen. Voorts bevatten polissen steeds vaker een expliciete uitsluiting voor cybergerelateerde schade.[82]

---

[74] *Oklahoma Firefighters Pension and Retirement System v. Brandt, et al.*, C.A. No. 2017-0133-SG (Del. Ch. 2017).
[75] HR 2 december 1994, ECLI:NL:HR:1994:ZC1564, *NJ* 1995/288, m.nt. J.M.M. Maeijer (*Poot/ABP*). Zie tevens L. Timmerman, 'Beginselen van bestuurdersaansprakelijkheid', *WPNR* 2016/7105, p. 324-330.
[76] D.A.M.H.W. Strik, *Grondslagen bestuurdersaansprakelijkheid. Een maatpak voor de Board Room*, Deventer: Kluwer 2010, p. 312-313.
[77] W.C.T. Weterings, 'Verzekering van cyberschade en –aansprakelijkheid. Voorziet de cyberverzekering (voldoende) in een behoefte van organisaties?', *AV&S* 2015/2, p. 4.
[78] M.J. Kroezen en C. Assers, *Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 2. Rechtspersonenrecht. Deel I. De rechtspersoon*, Deventer: Kluwer 2015, p. 190 en W.C.T. Weterings, 'Persoonlijke aansprakelijkheid van bestuurders voor onvoldoende IT-governance', *AV&S* 2016/42, p. 210.
[79] Target Corporation (2017), 2016 *Annual Report*, Target Corporation, Minneapolis, p. 44.
[80] C.M.C. van Tetterode, 'Het verzekeren van cybersecurity', *Bb* 2015/54, p. 186.
[81] T.F.E. Tjong Tjin Tai, 'Aansprakelijkheid bij datalekken', *WPNR* 2016/7110, p. 459-464.
[82] W.C.T. Weterings, 'Verzekering van cyberschade en –aansprakelijkheid. Voorziet de cyberverzekering (voldoende) in een behoefte van organisaties?', *AV&S* 2015/2, p. 8-9.

1.5.3 Traditionele verzekeringen

Cyberrisico's kunnen mogelijk onder verschillende bestaande verzekeringen worden gebracht.[83] Dit zijn de fraudeverzekering, de inventaris- en goederenverzekering, de beroepsaansprakelijkheidsverzekering (BAV), de algemene aansprakelijkheidsverzekering bedrijven (AVB) en de bestuurdersaansprakelijkheidsverzekering. De dekking van de traditionele verzekeringen is echter vaak beperkt tot een specifieke categorie aangesproken organisatie, personen of (cyber)schade. Zo dekt een AVB-verzekering in de regel slechts aansprakelijkheid voor zaakschade en schade door letsel.[84] Cyberincidenten zullen echter vaak zuivere vermogensschade tot gevolg hebben. Met betrekking tot de bestuurdersaansprakelijkheidsverzekering dient te worden opgemerkt dat dergelijke Nederlandse verzekeringen cybergerelateerde schade (nog) niet expliciet uitsluiten. In de Verenigde Staten is dit in sommige gevallen al wel het geval. Het valt niet uit te sluiten dat Nederlandse verzekeraars dit op termijn ook zullen doen.[85]
De traditionele verzekeringen hebben meestal een first party-karakter (dekking eigen schade) óf een third party-karakter (dekking schade derden). De fraudeverzekering en de inventaris- en goederenverzekering hebben een first party-karakter omdat ze worden afgesloten ten behoeve van de risico's van de verzekerde in verband met het oplopen van schade. De drie aansprakelijkheidsverzekeringen hebben een third party-karakter omdat die door de verzekerde worden afgesloten voor het dekken van aansprakelijkheid jegens een derde. De traditionele verzekeringen lijken onvoldoende aan te sluiten bij de technologische ontwikkelingen.[86] Dit heeft tot gevolg dat er leemten in de dekking (kunnen) ontstaan en dat schade als gevolg van cyberrisco's niet onder de dekking van een traditionele verzekering valt. Deze ontwikkelingen hebben eraan bijgedragen dat er in de verzekeringsmarkt een nieuw product is ontworpen: de cyberverzekering. Het afsluiten van een cyberverzekering is een mogelijkheid om in bovenstaande leemte te voorzien.

1.5.4 Cyberverzekering

Cyberverzekeringen zijn specifiek toegesneden op het afdekken van cyberrisico's en bevatten idealiter de volgende dekkingsonderdelen: aansprakelijkheid, crisismanagement, boetes, reconstructiekosten, bedrijfsstilstand, afpersing en cloud/outsourcing.[87] Hierdoor heeft de cyberverzekering zowel een first party-karakter als een third party-karakter, hetgeen betekent dat zowel eigen schade en de schade wegens aanspraken van derden is gedekt. Een ander verschil met de traditionele verzekeringen is het verzekeren van boetes. De bestuurlijke boete die de Autoriteit Persoonsgegevens aan de rechtspersonen kan opleggen, valt bij verschillende cyberverzekeringen onder de dekking.[88] Uit het bovenstaande blijkt dat cyberverzekeringen meer dekking bieden tegen cyberrisico's dan de traditionele verzekeringen.

1.5.5 Noodzakelijke en gebruikelijke verzekering

Indien een bestuurder geen cyberverzekering afsluit en daarmee onvoldoende dekking voor cyberschade wordt geboden, is de vraag of een bestuurder een ernstig verwijt kan worden gemaakt. Deze vraag is relevant voor zowel de interne als de externe aansprakelijkheid van bestuurders, dus zowel voor aanspraken van de vennootschap zelf, als voor derden die schade hebben geleden. Het ernstig verwijt

[83] W.C.T. Weterings, 'Verzekering van cyberschade en –aansprakelijkheid. Voorziet de cyberverzekering (voldoende) in een behoefte van organisaties?', *AV&S* 2015/2, p. 6-8.
[84] A.Ch.H. Franken, 'De aard van het verzekerd risico', *AV&S* 2017/1, p. 2.
[85] W.C.T. Weterings, 'Persoonlijke aansprakelijkheid van bestuurders voor onvoldoende IT-governance', *AV&S* 2016/42, p. 211.
[86] C.M.C. van Tetterode, 'Het verzekeren van cybersecurity', *Bb* 2015/54, p. 186.
[87] P. Hartman, 'Organisaties nog onvoldoende bewust van gevolgen cyberrisico's', *De Beursbengel* december 2013, p. 7.
[88] E. Thole, C. Solms-Sonnenwalde en C. Moll, 'De algemene meldplicht datalekken en de cyberverzekering', *TAV* 2015/2, p. 25 en W.C.T. Weterings, 'Verzekering van cyberschade en –aansprakelijkheid. Voorziet de cyberverzekering (voldoende) in een behoefte van organisaties?', *AV&S* 2015/2, p. 10.

criterium is voor beide immers van belang. Een bestuurder kan een ernstig verwijt worden gemaakt indien hij niet de – gezien de bedrijfsvoering – noodzakelijke en gebruikelijke verzekeringen heeft afgesloten.[89] Zo achtte de Rechtbank Den Haag in 2011 een bestuurder aansprakelijk doordat hij geen aansprakelijkheidsverzekering had afgesloten. Er was sprake van een ernstig verwijt omdat de bestuurder welbewust besloot om de risicovolle activiteiten door te zetten, terwijl hij wist dat de organisatie geen verhaal kon bieden bij eventuele schade van haar bezoekers.[90]
De eerste vraag die moet worden beantwoord, is of het afsluiten van een cyberverzekering noodzakelijk is. Het Verbond van Verzekeraars merkte in een rapport uit 2013 op dat een cyberverzekering vooral interessant zou zijn voor bedrijven die in sterke mate afhankelijk zijn van IT-systemen of die veel gegevens beheren.[91] In de inleiding van deze bijdrage heb ik beschreven dat dit tegenwoordig voor veel bedrijven geldt. Hoewel het afsluiten van een cyberverzekering interessant kan zijn voor deze bedrijven, is daarmee nog niet gezegd dat dit ook noodzakelijk is. Vooropgesteld kan worden dat bij dekking van cyberrisico's onder de afgesloten schadeverzekeringen er geen noodzaak zal bestaan tot het afsluiten van een cyberverzekering. Of er dekking bestaat, hangt vooral af van de soort schade. Hoe groter de afhankelijkheid van IT-systemen, hoe aannemelijker dat een verzekeraar de kosten van cyberrisico's niet zal dekken. Mijns inziens betekent het voorgaande niet dat iedere bestuurder een cyberverzekering ten behoeve van de vennootschap dient af te sluiten. Voor een bakkerij acht ik het minder noodzakelijk dan voor een ICT-organisatie. De aard van de onderneming is derhalve van essentieel belang omdat het de afhankelijkheid van IT-systemen bepaalt.
Ten tweede dient de vraag te worden beantwoord of het gebruikelijk is om een cyberverzekering af te sluiten. Het Verbond van Verzekeraars sprak in hetzelfde rapport uit 2013 haar verwachting uit dat cyberverzekeringen op den duur de normaalste zaak van de wereld zullen worden.[92] Die verwachting lijkt (nog) niet te zijn uitgekomen. Cyberverzekeringen vormen volgens een directeur van hetzelfde Verbond een kans voor de Nederlandse verzekeringsmarkt, maar komen desondanks maar langzaam op gang.[93] Een van de grootste Nederlandse assuradeuren gaf recent aan ''een paar honderd'' klanten met een cyberpolis te hebben.[94] Uit een door AON verricht onderzoek blijkt dat de Europese cyberverzekeringsmarkt nog in de kinderschoenen staat. [95] De verwachting bestaat echter dat de (Europese) markt voor cyberverzekeringen snel zal groeien. Dit komt mede door een toenemend bewustzijn van de (financiële) gevolgen van cyberrisico's en de toekomstige inwerkingtreding van de AVG.[96]

Uit het voorgaande concludeer ik dat het niet afsluiten van een cyberverzekering slechts in uitzonderlijke gevallen tot een ernstig verwijt kan leiden en dus niet snel de persoonlijke aansprakelijkheid van een bestuurder tot gevolg zal hebben. Daarbij moet men bijvoorbeeld denken aan een bestuurder van een ICT-organisatie die na herhaaldelijke waarschuwingen van zijn verzekeringsmakelaar omtrent dekkingsuitsluitingen van cyberrisico's op de traditionele schadeverzekeringen, welbewust besluit om geen cyberverzekering af te sluiten. Vervolgens dient zich een cyberincident voor te doen met schade aan de vennootschap en/of derden tot gevolg.

[89] M.J. Kroezen en C. Assers, *Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 2. Rechtspersonenrecht. Deel I. De rechtspersoon*, Deventer: Kluwer 2015, p. 190 en W.C.T. Weterings, 'Persoonlijke aansprakelijkheid van bestuurders voor onvoldoende IT-governance', *AV&S* 2016/42, p. 210.
[90] Rechtbank Den Haag 1 juni 2011, ECLI:NL:RBSGR:2011:BR6132, r.o. 4.6.
[91] Verbond van Verzekeraars, 'Virtuele risico's, echte schade. Over het verzekeren van cyberrisico's', *Position paper* oktober 2013, p. 9.
[92] Verbond van Verzekeraars, 'Virtuele risico's, echte schade. Over het verzekeren van cyberrisico's', *Position paper* oktober 2013, p. 9.
[93] L. de Boer, 'Zo fris als een hoentje het nieuwe jaar is', *VVP* 2016/7, p. 15.
[94] 'Cyberincidenten kosten 10 miljard euro, maar niemand verzekert zich', *NRC* 4 januari 2017.
[95] AON, *Global cyber market overview: uncovering the hidden opportunities* 2017, p. 4.
[96] AON, *Global cyber market overview: uncovering the hidden opportunities* 2017, p. 7.

1.6 Conclusie

De kwetsbaarheid van organisaties voor cyberrisico's zal door nieuwe technologieën toenemen. Door de impact van cyberrisico's op zowel de bedrijfsvoering van organisaties en de privacy van derden zal de rol van het bestuur bij de beheersing van deze risico's belangrijk worden in bestuurdersaansprakelijkheidszaken. Uit de voorgaande paragrafen is echter gebleken dat cyberrisico's moeilijk zijn in te passen in het bestaande privaatrechtelijk kader van bestuurdersaansprakelijkheid. Met betrekking tot cybersecurity hebben bestuurders op dit moment privaatrechtelijk gezien dan ook weinig om voor te vrezen. Om bestuurders in de toekomst met succes aansprakelijk te stellen, zal het privaatrechtelijk kader moeten worden aangevuld. Daarbij kan gedacht worden aan het toevoegen van een situatie, specifiek gericht op cybersecurity, waarin van een ernstig verwijt sprake kan zijn. Dit is van belang om bestuurders hun verantwoordelijkheid te laten nemen. De bestuurdersaansprakelijkheidszaken in de Verenigde Staten hebben laten zien dat bestuurders in een zekere mate worden beschermd wanneer zij die verantwoordelijkheid wel nemen. Deze bescherming is gezien de beleidsvrijheid van het bestuur en het risico van wijsheid achteraf naar mijn mening gerechtvaardigd en zou derhalve ook in Nederlandse procedures moeten gelden. Naast de toenemende impact van cyberrisico's zal de inwerkingtreding van de Algemene Verordening Gegevensbescherming er voor zorgen dat het afsluiten van een cyberverzekering op termijn voor bepaalde organisaties noodzakelijk en gebruikelijk wordt. Deze verzekering zal mijns inziens een belangrijke rol gaan spelen bij de invulling van de bestuurdersaansprakelijkheidsnorm in toekomstige bestuurdersaansprakelijkheidszaken.