Aansprakelijkheid, Verzekering & Schade, Verzekering van cyberschade en -aansprakelijkheid. Voorziet de cyberverzekering (voldoende) in een behoefte van organisaties?

Samenvatting

Cyberaansprakelijkheid en cyberschade vormen een steeds grotere bedreiging voor organisaties, zeker nu bij veel bedrijven de bedrijfsvoering (groten)deels online plaatsvindt. Bij het beheersen van deze cyberrisico' s vormt verzekering het sluitstuk van ICT-risicomanagement. De verwezenlijking van cyberrisico' s is namelijk nooit volledig uit te sluiten. De traditionele schadeverzekeringen bieden echter geen of beperkt dekking tegen de schadelijke gevolgen van cyberincidenten. Daarom zijn en worden cyberpolissen ontwikkeld. De vraag is, of deze cyberverzekeringen (voldoende) voorzien in de behoeften van organisaties. Tevens komt in deze bijdrage de toekomst van de cyberverzekeringsmarkt aan de orde.

1.Inleiding

Er is een toenemend risico voor niet alleen e-commerce bedrijven maar ook ' gewone' ondernemingen en overheidsorganisaties om geconfronteerd te worden met cyberschade en cyberaansprakelijkheid.[2] Een organisatie kan in de eerste plaats zelf schade lijden ten gevolge van het gebruik van internet, computernetwerken of digitale informatie. Bijvoorbeeld verlies van belangrijke bedrijfsgegevens, schade aan een netwerk of schade aan computergestuurde machines ten gevolge van een cyberaanval.[3] Daarnaast kan een organisatie aansprakelijk zijn voor schade van contractuele wederpartijen en/of derden in verband met het zich realiseren van cyberrisico' s. Bijvoorbeeld aansprakelijkheid van een organisatie in geval van schade bij een afnemer als gevolg van een doorgegeven computervirus of aansprakelijkheid vanwege fraude met elektronische betalingstransacties.

Deze cyberrisico' s worden ingeschat als één van de belangrijkste bedreigingen voor organisaties.[4] Daarmee wordt het voor organisaties ook belangrijker om deze schaderisico' s te beheersen.[5] Naast preventieve (veiligheids)maatregelen en procedures door de organisatie op het gebied van informatie- en communicatietechnologie kan een verzekering daarbij – als beschermingsmaatregel en sluitstuk van risicobeheersing – van groot belang zijn. Ook bij goed ICT-risicomanagement is de verwezenlijking van cyberrisico' s namelijk niet uit te sluiten. Innoveren is echter belangrijk voor organisaties en zij kunnen daar niet vanwege de digitale risico' s te terughoudend in zijn. Verschillende verzekeringsmaatschappijen bieden sinds

kort in Nederland een cyberverzekering aan. De vraag die rijst, is of een aparte cyberverzekering toegevoegde waarde heeft en of de cyberrisico's niet reeds onder een algemene aansprakelijkheidsverzekering bedrijven (AVB) of een andere traditionele schadeverzekering zijn gedekt. Ook komt de vraag op, of de aparte cyberverzekeringen die worden aangeboden, de benodigde bescherming bieden. Op deze vragen zal in de volgende paragrafen worden ingegaan. Ook zal de toekomst van de cyberverzekering(smarkt) aan de orde komen.

2.Cyberrisico's en schade

2.1 Directe en indirecte schade organisatie na een cyberincident

Digitalisering levert organisaties veel snelheid en gemak op bij hun processen, besluitvorming en dienstverlening. Dat laatste geldt zeker voor de informatie-uitwisseling met afnemers en leveranciers. Informatie wordt toegankelijker, is eenvoudiger uit te wisselen en te delen, en gaat gepaard met minder kosten. Tegelijkertijd brengt digitalisering voor die organisaties ook nieuwe risico's mee. Een voorbeeld is een computerstoring die het treinverkeer ontregelt, het administratieve proces bij een ziekenhuis platlegt, of mobiele telefonie onmogelijk of onveilig maakt.[6] Andere cyberincidenten die het nieuws hebben gehaald, zijn vertrouwelijke gegevens van klanten en leveranciers die in handen van hackers zijn gekomen, problemen met betalingen via internet, en diefstal van handelsgegevens.[7]

De oorzaken van digitale risico's zijn divers en complex. Het realiseren van een cyberrisico kan worden veroorzaakt door moedwillig handelen, technisch falen of menselijke fouten.[8] In het eerste geval gaat het om cybercriminaliteit, zoals hacking en verspreiden van kwaadaardige software.[9] Een cyberrisico kan zich ook verwezenlijken als gevolg van falende systemen, bijvoorbeeld ICT-storingen en -uitval. Verder is menselijk falen een belangrijke oorzaak. Een cyberrisico wordt dan bijvoorbeeld werkelijkheid omdat de ICT-infrastructuur niet afdoende is beheerd of beveiligd en daardoor vertrouwelijke gegevens van klanten bij derden terechtkomen.

Indien een cyberrisico zich realiseert, levert dat een organisatie dikwijls aanzienlijke directe en indirecte schade op.[10] Directe schade ontstaat doordat de organisatie zelf technische schade heeft en mogelijk ook gevolgschade. Deze gevolgschade kan verschillende vormen aannemen. Naast onderzoekskosten en kosten in verband met herstel van systemen en/of processen, kan een organisatie ook stagnatieschade ondervinden vanwege aantasting en onderbreking van het informatie- en productieproces.[11] Daarnaast kan directe schade ontstaan doordat de organisatie schadeclaims van klanten of andere partijen ontvangt.

Vaak is er ook sprake van meer indirecte schade zoals aantasting van de reputatie of het merk.[12] Dit kan uiteindelijk verstrekkende financiële gevolgen hebben (winstderving). Bijvoorbeeld klanten van een financiële instelling of een telecombedrijf die na een lek in de beveiliging massaal overstappen naar een concurrent. Een getroffen organisatie moet daarom geregeld ook public relations-kosten en crisis management-kosten maken. Ook zullen cyberincidenten die in de openbaarheid komen vaak een negatieve invloed hebben op de

waarde/koers van aandelen.[13] Dat is in de Verenigde Staten in 2009 gebeurd met Heartland Payment Systems (HPS). Nadat HPS had geopenbaard dat zij het slachtoffer was geworden van cybercriminaliteit, daalde de waarde van de aandelen van $ 18 naar $ 5,34.[14] Behalve dat dit schade voor het bedrijf opleverde, werd door de aandeelhouders ook via een collectieve actie een aansprakelijkheidsclaim ingediend.[15]

Ook kan een cyberincident schade meebrengen in de zin dat een organisatie wet- en regelgeving overtreedt en als gevolg daarvan een boete moet betalen.[16] Er is thans een nieuwe Europese privacyverordening in voorbereiding, bij overtreding waarvan (bijvoorbeeld het niet tijdig melden van datalekken) toezichthouders hoge boetes op kunnen leggen.[17] In de Angelsaksische landen is men al langer bekend met het opleggen van boetes in cyberkwesties. Zo heeft de Financial Services Authority in 2009 drie verzekeringsmaatschappijen behorende tot de HSBC groep een boete van £ 3,2 miljoen opgelegd wegens het verzenden van data van klanten zonder encryptie (overtreding FSA Principles for Business and Specific Rules) die vervolgens in criminele handen kwamen.[18]

2.2 Aansprakelijkheid bestuurders voor cyberrisico's

Naast de organisatie kunnen ook de directeuren en commissarissen geconfronteerd worden met de gevolgen van een cyberincident. In de Verenigde Staten zijn ook bestuurders van bedrijven door aandeelhouders persoonlijk aansprakelijk gesteld in verband met de schade die deze aandeelhouders zouden hebben geleden als gevolg van 'cyber-tekortkomingen'.[19] De aandeelhouders stelden dat de bestuurders wisten/zouden hebben moeten weten dat de onderneming en daarmee ook hun klanten kwetsbaar waren voor cyberaanvallen, doch hebben nagelaten om adequate veiligheids- en controlemaatregelen in te voeren.[20] Daarmee hebben volgens de benadeelden de bestuurders hun taak onbehoorlijk vervuld en zijn zij niet alleen persoonlijk aansprakelijk voor de schade van de klanten maar ook voor de gevolgschade van het bedrijf (lagere verkoopcijfers) en de gevolgschade van de aandeelhouders (lagere waarde aandelen). Tevens werd vergoeding van onderzoekskosten, advieskosten en juridische kosten gevorderd.

Ook in Nederland zijn dergelijke schadeclaims zeker niet ondenkbaar. De curator in het faillissement van Diginotar heeft bijvoorbeeld een onderzoek ingesteld naar de persoonlijke aansprakelijkheid van de bestuurders voor de schade ten gevolge van het netwerk van Diginotar, de dienstverlener met betrekking tot elektronische certificaten. Er zou de bestuurders een ernstig verwijt gemaakt kunnen worden van de onvoldoende netwerkbeveiliging. Naar verwachting zal (vermeende) bestuurdersaansprakelijkheid vanwege onvoldoende ICT-governance in de komende jaren een vlucht nemen. Gezien de toename van online bedrijfsactiviteiten zal de verantwoordelijkheid voor cyberrisico's en het investeren in veiligheidsmaatregelen en -procedures binnen een organisatie (meer) verschuiven van het technische

niveau naar (ook) het bestuursniveau. Het beheer van de risico's van online bedrijfsvoering dient een onderdeel te zijn van het algemene risicomanagement van een organisatie.[21]

3.Beheersing van gevolgen cyberincidenten door traditionele schadeverzekeringen

3.1 Verschillende verzekeringsmogelijkheden

Organisaties kunnen op verschillende manieren trachten de cyberrisico's te beheersen.[22] In de eerste plaats kan en moet risicomanagement binnen de organisatie plaatsvinden door de digitale risico's te identificeren en analyseren, door prioriteiten bij de aanpak van cyberrisico's aan te geven, door preventieve ICT-maatregelen te nemen, door richtlijnen en protocollen op te stellen, en door medewerkers te trainen.[23] Ofschoon een dergelijke wijze van ICT-risicomanagement veel cyberincidenten kan voorkomen, bestaat er toch altijd de mogelijkheid dat een cyberrisico zich realiseert met alle consequenties van dien.[24] Organisaties kunnen als onderdeel van hun risicomanagement de financiële gevolgen van een cyberincident afdekken door middel van verzekering.

Daarbij zijn er verschillende verzekeringsmogelijkheden. Een organisatie kan ervoor kiezen om via de reeds langere tijd bekende (algemene) schadeverzekeringen de financiële gevolgen van cyberrisico's te beperken. Ook kan sinds kort een specifieke cyberverzekering worden afgesloten.[25] De bestaande schadeverzekeringen waar de cyberrisico's (deels) kunnen worden ondergebracht, zijn de fraudeverzekering, de beroepsaansprakelijkheidsverzekering (BAV), de algemene aansprakelijkheidsverzekering bedrijven (AVB), de bestuurdersaansprakelijkheidsverzekering, en de inventaris- en goederenverzekering.

3.2 Fraudeverzekering

Fraudeverzekeringen hebben als voornaamste doel een organisatie te beschermen tegen de schade als gevolg van fraude door een medewerker of een derde partij. De standaarddekking omvat diefstal, verduistering, valsheid in geschrifte, computerfraude en oplichting. Er is vooral sprake van fraudegevoeligheid bij organisaties waar met (contant of virtueel) geld wordt gewerkt, waar veel verhandelbare goederen aanwezig zijn, of waar gevoelige informatie wordt bewaard.[26] Veel financiële

instellingen, zoals banken en verzekeraars, beschikken daarom over een dergelijke fraudedekking.[27] In andere branches komt de fraudeverzekering minder voor. Bij cyberrisico's die onder de omschrijving van het begrip 'computerfraude' in de polis vallen, kan een dergelijke verzekering (deels) uitkomst bieden. Bij de grote groep van andere cyberincidenten zal de fraudeverzekering geen bescherming opleveren.

Er zal met name dekking zijn voor aansprakelijkheid van de verzekerde organisatie jegens derden indien er sprake is geweest van ongeautoriseerde toegang tot het netwerk en/of computerbestanden, of van een cyberaanval bij die organisatie, en dat heeft geleid tot fraude waardoor derden schade hebben geleden. Als er alleen sprake is van eigen schade van de organisatie zal de computerfraude-dekking vaak louter aan de orde zijn in geval van fraude na diefstal van gegevens.

De dekking bij fraudeverzekeringen is doorgaans beperkt tot kosten (zoals onderzoeks-, verdedigings-, PR- en herstelkosten) en directe vermogensschade.[28] Wat het laatste betreft, in een fraudeverzekering wordt vaak bepaald dat er alleen dekking is voor schade die het rechtstreekse en onmiddellijke gevolg is van een (computer)fraude, niet zijnde gevolgschade. Dat betekent dat meer indirecte vermogensschade als gevolg van computerfraude – zoals schade vanwege bedrijfsstilstand, boetes, winstderving, en kosten van crisismanagement – dikwijls niet gedekt zal zijn. Dat was in de ogen van de fraudeverzekeraar het geval bij een Amerikaanse schoenenketen (Designer Shoe Warehouse), waar hackers via frauduleuze toegang tot het computernetwerk de credit card- en bankrekeninggegevens van 1,4 miljoen klanten hadden bemachtigd. De verzekerde schoenenketen kreeg als gevolg daarvan te maken met grote schadeposten (in totaal meer dan 6,8 miljoen dollar), waaronder onderzoekskosten, PR-kosten, kosten van communicatie met klanten, juridische kosten, schadevergoeding aan klanten en boetes van toezichthouders. De verzekeraar weigerde echter dekking met betrekking tot de betalen schadevergoeding en de boetes omdat er sprake was van indirecte schade.[29] Tevens was volgens de verzekeraar de uitsluiting voor vertrouwelijke gegevens van toepassing.

3.3 Inventaris- en goederenverzekering

Een uitgebreide zakelijke brandverzekering dekt materiële schade aan gebouwen, inventaris en goederen van de verzekerde organisatie door een gedekte gebeurtenis (brand, ontploffing, storm, vandalisme etc.). Als een cyberincident bij de organisatie materiële schade aan goederen of inventaris veroorzaakt, dan zal dat gedekt kunnen zijn mits het schadeveroorzakende evenement kan worden gekwalificeerd als vandalisme of een andere volgens de polis gedekte gebeurtenis.[30] Bijvoorbeeld schade aan de computerhardware (zoals een gecrashte harddisk) ten gevolge van een cyberaanval. Het Verbond van Verzekeraars heeft in dit verband het voorbeeld genoemd van een hacker die via een computerverbinding een machine of de lopende band van een bedrijf in elkaar laat draaien.[31] Geregeld zal een cyberaanval echter geen gedekte

gebeurtenis in de zin van de polis zijn.

Bovendien is er alleen dekking voor materiele schade ten gevolge van een cyberincident. Schade aan data en software wordt in Nederland doorgaans niet als materiële schade in de zin van de verzekeringsvoorwaarden gezien terwijl juist dergelijke schade zich vaak zal voordoen bij een cyberincident.[32] Ook is er geregeld een uitsluiting voor schade als gevolg van computervirussen opgenomen. Andere schade van de organisatie dan materiele schade aan goederen en inventaris, zoals stagnatieschade en herstelkosten, is in ieder geval niet gedekt. Voorts valt aansprakelijkheid jegens derden niet onder de dekking van de inventaris- en goederenverzekering.

Een goederen- en inventarisverzekering geeft derhalve geen of beperkt bescherming tegen cyberrisico' s. Bij gelijksoortige verzekeringen als de elektronicaverzekering, de computerverzekering, de machinebreukverzekering en andere technische verzekeringen is materiele schade aan de computerapparatuur en kosten gedekt maar gaat de dekking in beginsel niet verder. Er kunnen vaak wel extra dekkingen worden afgesloten, bijvoorbeeld voor schade aan het netwerk bij een computerverzekering of een bedrijfsschadedekking bij een commerciële opstalverzekering (zogenaamde ' Property Damage/Business Interruption' -dekking), maar ook dan worden zeker niet alle cyberrisico' s en alle schadelijke gevolgen daarvan ondervangen. Zo zal bij de hiervoor bedoelde bedrijfsschadeverzekering omzetverlies alleen voor vergoeding in aanmerking komen als de bedrijfsactiviteiten zijn vertraagd als direct gevolg van materiële schade aan het gebouw, machines, inventaris of de goederen. Zoals hierboven aangegeven, is er bij cyberincidenten nu juist vaak geen sprake van een gedekte materiële schade. Bovendien dient meestal ook door de verzekerde te worden aangetoond dat de winstderving is geleden als een noodzakelijk gevolg van het stilvallen van de bedrijfsactiviteiten.

3.4 Algemene aansprakelijkheidsverzekering (bedrijven)

Schade als gevolg van een cyberincident zal ook niet altijd gedekt zijn onder een algemene aansprakelijkheidsverzekering van de getroffen organisatie, zoals de algemene aansprakelijkheidsverzekering bedrijven (AVB). De eigen schade van een organisatie, zoals schade wegens de uitval van een webwinkel van een grote modeketen, valt hier in ieder geval niet onder.

Verder zal de AVB-verzekering (of vergelijkbare verzekering) ook niet elke vorm van cyberaansprakelijkheid jegens derden dekken. Daarbij is ook een belangrijke beperking dat een AVB-verzekering ' slechts' dekking biedt bij letselschade of zaakschade. Bij de meeste cyberincidenten zal geen sprake zijn van beschadiging van zaken van derden maar van zuivere vermogensschade.[33] Verzekeringsrechtelijk is sprake van zaaksbeschadiging, zo wordt doorgaans in de literatuur aangenomen, indien er sprake is van een objectieve aantasting van de stoffelijke structuur van een zaak.[34] Dat zal zich bij cyberschades, waar

vaak ‘ alleen’ sprake is van het verdwenen of beschadigd zijn van (elektronische) gegevens, niet snel voordoen, althans zal daar sterk over gediscussieerd kunnen worden.[35] Er is bijvoorbeeld in beginsel geen sprake van zaakschade als een verzekerde nalaat om zijn computersysteem voldoende te beveiligen en dit resulteert in infectie van zijn computer(s) en ook de computers van klanten met een virus, een worm, een Trojaans paard, malware, spyware of andere ongewenste en schadelijke software.[36] Daarbij komt het geregeld voor dat bij de definitie van zaakschade expliciet wordt aangegeven dat hier niet onder valt ‘ het disfunctioneren van informatiedragers (zoals diskette, harde schijf of Cd-rom), alsmede verlies of verminking van op informatiedragers opgeslagen data (‘ bits’ en ‘ bytes’) of programmatuur’ . Ook komen software-uitsluitingen voor. Bijvoorbeeld:

“ Uitgesloten is de aansprakelijkheid voor schade die het gevolg is van het beschadigen of het verloren (doen) gaan van elektromagnetisch en/of optisch opgeslagen gegevens.”

In de Verenigde Staten is wel dekking aangenomen bij aansprakelijkheid van het verzekerde bedrijf jegens klanten in verband met een inbreuk op het recht op privacy. De rechter zag het openbaren door een bedrijf van credit card-gegevens als een privacyinbreuk en oordeelde dat de schade van de klanten als gevolg daarvan was gedekt als ‘ personal injury’ onder de AVB-verzekering.[37] Gezien de omschrijving van personenschade in Nederlandse AVB-verzekeringen, zal er echter veelal geen dekking zijn bij privacy-aansprakelijkheid. Veel AVB-polissen beperken gedekte personenschade tot fysieke schade door letsel of aantasting van de gezondheid van personen. Schade wegens een inbreuk op de privacy valt hier niet onder.

3.5 Beroepsaansprakelijkheidsverzekering

Een beroepsaansprakelijkheidsverzekering kan een ruimere bescherming bieden tegen cyberrisico’ s. Wel zal dat slechts gelden voor een specifieke groep verzekerde organisaties, namelijk bedrijven die diensten en (aanvullend) producten leveren die te maken hebben met activiteiten op het terrein van internet en/of informatie technologie, zoals dienstverleners in de telecom- en de ICT-sector.[38]

Een beroepsaansprakelijkheidsverzekering geeft de verzekerde in beginsel geen dekking voor eigen schade. Aansprakelijkheidsclaims van derden en juridische verweerkosten zijn mogelijk wel gedekt indien het een beroepsfout in de zin van de polisvoorwaarden betreft, bijvoorbeeld een fout advies over netwerkbeveiliging of een programmeerfout. Ook is er in beginsel ruime dekking voor zuivere vermogensschade van derden, zoals stagnatieschade vanwege netwerkuitval of dataverlies. Wel kunnen er dekkingsuitsluitingen gelden, zoals de uitsluiting met betrekking tot kosten voor het opnieuw verrichten van de werkzaamheden en de uitsluiting voor schade als geen aansprakelijkheidsbeperkende contractsvoorwaarden door de verzekerde dienstverlener zijn gehanteerd. Ook kunnen er dekkingsproblemen ontstaan door een uitsluiting voor schade

ten gevolge van fraude en vermogensdelicten, een uitsluiting voor schade als gevolg van een inbreuk op intellectuele eigendomsrechten, of een uitsluiting voor aansprakelijkheidsverhogende bedingen (waaronder garantiebedingen).

3.6 Bestuurdersaansprakelijkheidsverzekering

Ofschoon er in Nederland nog nauwelijks bestuurders van organisaties persoonlijk aansprakelijk zijn gesteld voor schade ten gevolge van cyberrisico's, is de verwachting, zoals hierboven aangegeven, dat ICT-governance en de beheersing van cyberrisico's niet alleen op het niveau van de ICT-afdeling van een organisatie maar ook op niveau van de bestuurders van een organisatie een belangrijke rol gaat spelen.[39] Indien een bestuurder aansprakelijk wordt gesteld in verband met het nemen van onvoldoende preventieve maatregelen tegen het zich realiseren van cyberrisico's, zal er in beginsel dekking zijn onder de bestuurdersaansprakelijkheidsverzekering, tenzij er sprake is geweest van opzet of persoonlijke bevoordeling van de betrokken bestuurder.[40] Vooralsnog sluiten Nederlandse bestuurdersaansprakelijkheidsverzekeringen cybergerelateerde aanspraken niet expliciet uit, waar dat in de Verenigde Staten wel geregeld het geval is voor 'privacy violations' en 'data breaches' door bestuurders. Uiteraard is de dekking wel beperkt tot de persoonlijke aansprakelijkheid van directeuren en commissarissen en omvat het niet de andere cyberrisico's van de organisatie. Daarbij kan er ook alleen dekking zijn voor de zuivere vermogensschade van derden in verband met het handelen van de bestuurders.

4. Beheersing van gevolgen cyberincidenten door een cyberverzekering

4.1 Omvangrijkere dekking cyberverzekering

Uit het voorgaande volgt dat de traditionele schadeverzekeringen vaak óf een first party-karakter (dekking eigen schade verzekerde) hebben, óf een third party-karakter (dekking schade derden; aansprakelijkheid). Daarnaast is de dekking dikwijls beperkt tot een specifieke categorie aangesproken organisaties of personen en ook tot een bepaalde categorie (cyber)schade.[41] Geen enkele verzekering geeft een alomvattende dekking voor de schadelijke gevolgen van cyberincidenten.[42] Ook in geval van een combinatie van traditionele verzekeringen blijven er (grote) leemtes bestaan. Op zich is dat ook niet vreemd aangezien deze schadeverzekeringen zijn ontworpen voor de tijd van de cyberincidenten en ook met een ander doel. Zij zijn niet gericht op de additionele risico's van de digitale economie.[43]

De leemtes in de traditionele verzekeringen creëren een markt in cyberverzekeringen. Door verzekeraars en makelaars zijn en worden specifieke cyberverzekeringen ontwikkeld en sinds enige tijd op de markt gebracht. Deze verzekeringen zouden meer moeten voldoen aan de dekkingsbehoeften van verzekerden en meer zijn gericht op de digitale risico's van organisaties.[44] De gedachte is dat een aparte cyberverzekering idealiter de volgende dekkingsonderdelen omvat:

- Aansprakelijkheid:
  - aansprakelijkheid wegens onvoldoende netwerkbeveiliging
  - privacy-aansprakelijkheid
  - media-aansprakelijkheid
  - verdedigingskosten/juridische bijstand
  - schadevergoeding
- Crisismanagement:
  - kosten (forensisch) onderzoek
  - public relations-kosten
  - klantnotificatie-kosten
- Boetes
  - kosten van onderzoek en verdediging in verband met bestuurlijke boetes
  - betaling boetes opgelegd door toezichthouders of andere overheidsinstanties
- Reconstructiekosten
- Bedrijfsstilstand-schade
- Afpersing
- Cloud/outsourcing[45]

Onder een cyberverzekering is in de eerste plaats privacy-aansprakelijkheid gedekt. Deze mogelijke

aansprakelijkheid van een verzekerde jegens derden in verband met privacyinbreuken en/of onzorgvuldig gebruik van persoonsgegevens (schade door openbaar worden van vertrouwelijke informatie) valt doorgaans niet onder de dekking van de traditionele schadeverzekeringen. Ook de aansprakelijkheid van de verzekerde organisatie voor schade van derden wegens het tekortschieten van de netwerkbeveiliging is gedekt. Hetzelfde geldt vaak ook voor media-aansprakelijkheid, dat wil zeggen: aansprakelijkheid wegens smaad en laster bij het gebruik van elektronische media of wegens inbreuk op auteursrechten, merkenrechten en andere intellectuele eigendomsrechten. Tegenwoordig vormt digitale media een belangrijk aspect bij de marketing van en distributie door organisaties en ook hierbij kunnen dan (vermeend) zorgvuldigheidsgrenzen worden overschreden. Naast de te betalen schadevergoeding zijn ook de verweerkosten bij bovengenoemde categorieën aansprakelijkheidsclaims verzekerd. Daarbij wordt (ook) de financiële schade gedekt die is veroorzaakt door computer- en/of ICT-systemen, zonder dat er sprake is van materiële schade.

Ook eigen schade van de organisatie is in ruime(re) mate gedekt, zoals stagnatieschade als gevolg van een cyberincident alsook kosten van onderzoek, kosten van herstel van het netwerk, kosten van vervangen van data en software, kosten van preventie en PR-kosten. Tevens kan schade van de verzekerde organisatie in verband met IT-outsourcing en het gebruik van cloud computing (beschikbaar stellen van hardware, software en gegevens op internet) onder de dekking vallen. Hetzelfde geldt voor schade door hackers die de website of data van de organisatie gijzelen (vergoeding kosten beveiligingsexpert en eventueel losgeld).

4.2 Cyberverzekering nog sterk in ontwikkeling

Op dit moment heeft ongeveer 40% van de ondernemingen in de Verenigde Staten een aparte cyberverzekering.[46] Naar verwachting zal dit percentage de komende jaren nog sterk toenemen. In 2013 is het percentage afgesloten cyberverzekeringen in Amerika met 20%-40% gestegen ten opzichte van 2012 (waar dat het jaar ervoor 1%-4% was).[47] In Nederland worden op dit moment cyberverzekeringen door slechts enkele verzekeraars aangeboden, waarbij het opvallend is dat het met name buitenlandse maatschappijen zijn (onder meer AIG, ACE, Allianz, Chubb, CNA, Hiscox, Liberty, XL en Zurich).[48] Er schijnen ook nog maar een paar honderd/paar duizend polissen te zijn afgesloten.[49] De verwachting is echter dat de Amerikaanse situatie en ontwikkelingen, zoals vaker (bijvoorbeeld bij de bestuurdersaansprakelijkheidsverzekering), ook naar Europa en in het bijzonder Nederland zullen overwaaien. Organisaties zullen daarbij niet alleen zelf een cyberverzekering afsluiten, maar mogelijk ook van hun businesspartners verlangen dat zij dat doen, aangezien zij geconfronteerd kunnen worden met de gevolgen van een cyberincident dat bij een leverancier, afnemer of een andere zakenrelatie is ontstaan. Uiteindelijk zal de cyberverzekering wellicht net zo gebruikelijk worden als de AVB-verzekering.

De Nederlandse cyberpolissen staan ook inhoudelijk nog relatief in de kinderschoenen. Een cyberverzekering geeft zeker meer dekking tegen cyberrisico’ s dan de traditionele schadeverzekeringen en

zal voor organisaties een toegevoegde waarde (kunnen) hebben. De cyberverzekering is echter nog steeds in ontwikkeling en zal thans nog niet altijd volledig op de behoeften van (aspirant)verzekerden aansluiten. De verzekeringen die thans worden aangeboden, bevatten ook leemten in de dekking. Bovendien valt bij een vergelijking op dat (de omvang van) de dekking, insluitingen en uitsluitingen in de polissen die door de verschillende verzekeraars in Nederland worden aangeboden behoorlijk verschillend zijn.[50] Bij de ene verzekeraar zijn veel cyberrisico's in ruime mate gedekt, waar dat bij de andere verzekeraar meer beperkt is.

De cyberverzekering bestaat doorgaans uit verschillende dekkingsmodules/-rubrieken. Voor elke (sub)rubriek geldt dan vaak een aparte sublimiet en een apart eigen risico. Daarbij wordt geregeld gewerkt met een basisdekking, waarbij zijn verzekerd de aansprakelijkheid, de kosten in verband met een administratieve procedure, de kosten in verband met herstel van de reputatie en de kosten in verband met een reactie naar klanten, afnemers en instanties.

De aansprakelijkheidsdekking wordt vaak ruim en specifiek omschreven. Zo wordt in één van de aangeboden polissen expliciet aangegeven dat is verzekerd de aansprakelijkheid jegens derden in verband met het tekortschieten van de netwerkbeveiliging, het verlies van persoonsgegevens/bedrijfsinformatie, of outsourcing. Bij de aansprakelijkheid wegens onvoldoende netwerkbeveiliging wordt ook vermeld dat schade aan persoonsgegevens of bedrijfsinformatie van derden door een besmetting met een virus, niet-geautoriseerde sofware of een computercode bij de verzekerde organisatie is gedekt, zodat geen discussie over de aanwezigheid van een materiële beschadiging hoeft te worden gevoerd. Tevens wordt bepaald welke schadegevallen onder de dekking vallen, zoals schade bij derden als gevolg van:

– een DDoS aanval tegen de verzekerde organisatie;

– ontvreemding van toegangscodes van de verzekerde organisatie;

– de wederrechtelijke toe-eigening van de hardware van de verzekerde organisatie;

– openbaarmaking van gegevens door een werknemer van de verzekerde organisatie;

– vernietiging, verwijdering of beschadiging van persoons- of bedrijfsgegevens opgeslagen op een computersysteem;

– ontzegging van een derde van toegang tot diens eigen gegevens.

Een dergelijke omschrijving, die overigens bij de meeste verzekeraars korter is, is goed voor de rechtszekerheid en het voorkomen van interpretatiediscussies. Tegelijkertijd houdt het ook een beperking van de dekking in, zeker gezien de snelle ontwikkelingen op het terrein van de cyberrisico's.

Datzelfde geldt bij dekking van aansprakelijkheid in geval van outsourcing, die bijvoorbeeld soms alleen de orde is in geval van overtreding van een verplichting die ziet op het verwerken van persoonsgegevens of bedrijfsinformatie (privacy-aansprakelijkheid). Voorts valt multimedia-aansprakelijkheid niet altijd onder de basisdekking, maar is eventueel aanvullend te verzekeren.

Ook bij de dekking van de kosten en schade bij administratieve procedures gelden beperkingen. Zo komt het voor dat ‘slechts’ een gedeelte – bijvoorbeeld 75% of 90% – van een bestuursrechtelijke boete door de verzekeraar wordt vergoed doordat een eigen risico van 10% of 25% wordt gehanteerd, en/of dat boetes een minimale omvang moeten hebben (bijvoorbeeld EUR 50.000) om voor vergoeding in aanmerking te komen.[51] Ook vallen bij sommige cyberverzekeringen ‘alleen’ boetes in verband met de overtreding van wetgeving ter zake van verwerking van persoonsgegevens onder de dekking. Voorts geldt steeds, zoals hierboven aangegeven, bij een module een sublimiet. Eén van de cyberverzekeraars hanteert bijvoorbeeld bij boetes een maximaal verzekerde som van EUR 250.000, hetgeen enerzijds een behoorlijk bedrag is en anderzijds bij de invoering van de Europese privacyverordening en de daarin genoemde boetebedragen (maximaal € 100 miljoen) te laag zal kunnen zijn.[52] Dat geldt ook gezien het wetsvoorstel meldplicht datalekken dat beoogt een nieuw artikel 34a (meldplicht) in de Wet bescherming persoonsgegevens door te voeren alsook een artikel 66 Wbp, op grond waarvan het College bescherming persoonsgegevens een bestuurlijke boete kan opleggen van maximaal € 810.000 bij overtreding van artikel 34a Wbp.[53]

Ook bij de andere eigen kosten en schade van de verzekerde(n) gelden beperkingen. Zo zijn soms onderzoekskosten, kosten van verwijdering van virussen en PR- en communicatiekosten gedekt bij een inbreuk op beveiliging van gegevens maar niet in andere gevallen, of er wordt een maximumvergoeding van bijvoorbeeld € 20.000 gehanteerd. Kosten ter zake van herstel van de reputatie zijn verzekerd voor zover het gaat om onafhankelijk advies over de acties die redelijkerwijs nodig zijn om de potentieel negatieve gevolgen van een nieuwswaardige gebeurtenis te voorkomen of te beperken. Eventuele reputatieschade en omzetschade zijn niet gedekt en ook de kosten van de ‘schadebeperkende’ acties en de andere eigen kosten van de verzekerde niet. Ofschoon dat lastig verzekerbaar zal zijn, vormen reputatieschade en omzetschade in verband daarmee de grootste zorg van risk & insurance managers van organisaties.[54]

Stagnatieschade is (aanvullend) te verzekeren, maar daarbij wordt geregeld gewerkt met een maximum uren aan stilstand en een minimale schade, of juist een eigen risico aan uren stilstand van bijvoorbeeld 8 of 10 uur. Ook is er soms een beperking tot vergoeding van gederfde internetinkomsten en een maximale vergoeding per uur.

Bij de module cyberafpersing wordt vaak expliciet en limitatief omschreven welke vormen van afpersing onder de dekking vallen, bijvoorbeeld het dreigement om elektronische niet-openbare informatie van de organisatie te verspreiden of te vernietigen, om door middel van een virus, worm of andere kwaadaardige code het computersysteem of de website van de organisatie te beschadigen, of om de toegang tot het computersysteem te belemmeren. Daarmee vallen niet opgesomde afpersingsbedreigingen niet onder de dekking. De (omvang van de) lijst met wel gedekte gevallen verschilt per verzekeraar.

Verder valt op dat bij de meeste cyberverzekeraars bepaalde branches niet standaard een dekking kunnen

krijgen vanwege de grotere kans op cyberincidenten en (omvangrijke) schade. Dat geldt bijvoorbeeld voor financiële instellingen, medische instellingen, call centers, telecombedrijven, internetproviders en telemarketingbureaus. Dergelijke bedrijven hebben of geen verzekeringsmogelijkheid bij de betreffende verzekeraar, of zullen wel een cyberverzekering kunnen krijgen maar met een andere premie en tegen andere voorwaarden en uitsluitingen.

Voorts worden door sommige verzekeraars in het acceptatieproces meerdere vragen gesteld over de gegevens- en informatiebeveiliging en de back-up systemen en processen.[55] Dat is met name het geval als de organisatie groter is en de verzekerde som serieuzer. In het aanvraagformulier wordt dan gevraagd naar onder meer de online activiteiten, firewalls, toegangpreventiesystemen, antivirussoftware en -updates, back-up- en herstelsystemen, versleuteling van data, het informatiebeveiligingsbeleid, en een ‘clean desk’ en ‘clear screen’ beleid. Ook wordt door enkele verzekeraars bij grotere organisaties wel een audit uitgevoerd. Een cyberverzekeraar wil dan, alvorens een verzekering met een behoorlijke verzekerde som af te sluiten, eerst meer inzicht hebben in de kwetsbaarheid van de organisatie met betrekking tot cyberrisico’s, in het risicomanagement en in de veiligheidsmaatregelen. Tegelijkertijd zijn de verkrijgbare verzekerde sommen op de Nederlandse cyberverzekeringsmarkt niet heel hoog en zijn niet alle cyberrisico’s (geheel) verzekerbaar. Overigens hebben veel cyberverzekeraars bij kleinere organisaties juist opvallend weinig acceptatie-eisen, maar dat valt terug te zien in de dekkingsomvang en de verzekerde sommen.

5. Ontwikkeling cyberzekering via cyberveiligheidsmaatregelen en -procedures

5.1 Meer informatie over beheersing cyberrisico’s nodig: moreel risico en averechtse selectie

De cyberverzekering staat dus in Nederland nog enigszins in de kinderschoenen en dient doorontwikkeld te worden teneinde meer aan de behoeften en verwachtingen van verzekerden te kunnen voldoen. Problematisch voor de ontwikkeling van een meer optimale cyberverzekeringsmarkt is mogelijk dat er thans sprake is van informatieproblemen bij verzekeraars. Als gevolg daarvan weten cyberverzekeraars niet goed welke risico’s zij binnenhalen en zijn zij begrijpelijkerwijs voorzichtig met de dekkingsvoorwaarden en de verzekerde sommen.

Een verzekeraar streeft naar het overeenkomen van een adequate premie die in evenwicht is met de dekking van het risico. Het vaststellen van de premie is echter op dit moment zeer lastig bij cyberverzekeringen. Daarvoor is een lange geschiedenis van actuariële data vereist. Verzekeraars kijken dan naar schade-evenementen in het verleden teneinde te bepalen – aan de hand van verschillende

factoren – hoe groot de kans is dat dergelijke evenementen in de toekomst (bij een bepaalde verzekerde) zullen voorkomen. Dergelijke gegevens zullen echter in het kader van de cyberverzekering niet ruimschoots aanwezig zijn gezien het relatief korte bestaan van digitale technologie (internet), cyberincidenten en cyberverzekeringen. Daarbij speelt ook een rol dat organisaties vaak niet op de hoogte zijn van een cyberaanval en als zij dat wel zijn niet graag details daarover aan een verzekeraar prijsgeven.[56] Ook als er meer ervaring is met cyberrisico's en cyberverzekeringen zal er mogelijk steeds enige achterstand in voldoende actuariële gegevens zijn aangezien de digitale risico's – qua aard en omvang – in snel tempo veranderen. Een cyberverzekeraar loopt als gevolg daarvan bij het bepalen van de premie aan tegen de bekende informatieproblemen van averechtse selectie en moreel risico.

Het probleem van averechtse selectie ('verkeerde selectie') ontstaat wanneer de informatieasymmetrie tussen de verzekeraars en zijn verzekerden met betrekking tot de concrete risico's dusdanig groot is dat de verzekeraar geen goed onderscheid kan maken tussen de verschillende verzekerden en hun risico's.[57] Daarbij zullen organisaties met een grote(re) kans op cyberaansprakelijkheid en -schade eerder een verzekering willen afsluiten dan organisaties met een lage(re) kans op cyberincidenten.[58] Als een verzekeraar niet afdoende de verschillende verzekerde organisaties met hun verschillende cyberrisico's kan onderscheiden (goede risico's en slechte risico's), is het voor hem ook lastig om bij een verzekerde een passende premie in rekening te brengen.[59] Gezien het gebrek aan betrouwbare actuariële data is averechtse selectie bij cyberrisico's een reëel probleem.[60]

Daarnaast bestaat het gevaar van moreel risico: een verzekerde handelt vanwege de aanwezigheid van een verzekering risicovoller dan hij normaal zou doen en neemt niet de optimale voorzorgsmaatregelen.[61] In het kader van de cyberverzekering betekent dit dat de prikkels afnemen voor een verzekerde organisatie om de cyberveiligheid te verbeteren.[62] Een organisatie wordt namelijk geprikkeld om de veiligheidsmaatregelen en -procedures op het niveau te brengen dat nodig is om een cyberverzekering te kunnen krijgen in plaats van het niveau dat nodig is om klanten, derden en zichzelf adequaat te beschermen tegen cyberincidenten. Het is dus voor een cyberverzekeraar van belang dat die niveaus zoveel mogelijk samenvallen.

Er zijn verschillende manieren om het moreel risico te reduceren. Een verzekeraar kan een eigen risico en dekkingslimieten hanteren. Een andere methode is het geven van een korting op de premie aan verzekerde organisaties die passende cyberveiligheidsmaatregelen en -procedures hebben en andersom toeslagen wanneer de maatregelen en procedures onder de maat zijn (bonus-malus systeem).[63] Een verzekerde organisatie wordt dan meer geprikkeld om te investeren in veiligheidsmaatregelen en -processen die cyberincidenten kunnen voorkomen of beperken. Ook in het kader van de dekking stellen van zorgvuldigheidseisen door een verzekeraar kan het moreel risico beperken.[64] Een organisatie moet dan bepaalde veiligheidsmaatregelen en -procedures realiseren alvorens een verzekeringsovereenkomst te kunnen aangaan en/of na het sluiten van de verzekering dergelijke maatregelen treffen en op peil houden om voor dekking in aanmerking te komen. In de ideale wereld verhogen cyberverzekeringen derhalve het ICT-veiligheidsniveau.[65]

Een cyberverzekeraar dient om deze manieren ter beperking van het moreel risico op de juiste manier te

kunnen inzetten, echter wel te weten wat een adequaat beschermingsniveau is en richtlijnen te hanteren met betrekking tot de vereiste cyberveiligheid bij verzekerden. Verzekeraars lijken echter thans op beide aspecten tekort te schieten. Enerzijds is dit ook weer terug te voeren op het tekort aan actuariële data. Anderzijds is er nog te weinig kennis over en geen consensus tussen verzekeraars (en de andere betrokkenen) over wat effectieve cyberveiligheidsmaatregelen en -procedures zijn.

Dat is jammer omdat dit ook behulpzaam kan zijn bij het beperken van averechtse selectie. Een mogelijkheid voor een cyberverzekeraar om het probleem van averechtse selectie te beperken, is namelijk het uitvoeren van een uitgebreide risicobeoordeling en een fysieke en technische analyse (inspectie/audit) van de IT-veiligheidsmaatregelen, het netwerk en de procedures bij aspirant-verzekerden voorafgaande aan het aangaan van een verzekering. De mate waarin en de wijze waarop een verzekerde heeft geïnvesteerd in cyberveiligheid bepaalt de kans op cyberincidenten, net zoals bij een zorgverzekering een verzekerde die veel/weinig sport een kleinere/grotere kans heeft op diabetes of hartklachten. Als verzekeraars kunnen differentiëren tussen verzekerde organisaties en hun cyberveiligheidsniveau, kunnen zij de premie en de dekking(seisen) daarop afstemmen.[66] Voorwaarde is dan echter wel dat er een goed toetsingskader is.

5.2 Belang (kennis) effectieve veiligheidsmaatregelen verzekeraars, organisaties en maatschappij

Verzekeraars hebben er dus een groot belang bij om beter de relatie tussen enerzijds bepaalde strategieën en technologische maatregelen en anderzijds de schade door cyberincidenten te doorgronden. Slechts dan is het goed mogelijk om de cyberveiligheid bij verzekerden te beoordelen en adequate eisen te stellen aan de veiligheidsmaatregelen en -procedures. Ook voor organisaties is meer kennis over cyberveiligheid van grote betekenis. Een deel van het risico zal vaak niet verzekerd zijn en voor eigen rekening blijven.[67] Cyberevenementen kunnen verstrekkende gevolgen hebben en de verzekerde som zal geregeld niet toereikend zijn om alle schade en kosten te vergoeden. Dat zal ook bij een beter ontwikkelde cyberverzekeringsmarkt het geval zal zijn. Daarnaast zijn bepaalde vormen van cyberschade niet (goed) verzekerbaar, zoals de reputatieschade van een organisatie. Voorts zullen organisaties sterker(er) worden geprikkeld om te investeren in bescherming tegen cyberrisico’ s als verzekeraars meer eisen gaan stellen aan cyberveiligheid. De mate van het veiligheidsniveau bepaalt dan immers de hoogte van de premie.

Maar ook los van de cyberverzekering hebben organisaties een belang bij meer kennis over effectieve cyberveiligheidsmaatregelen en -praktijken. Een verzekering is immers ‘ slechts’ het sluitstuk van ICT-risicomanagement. Gezien de Europese privacyverordening en de aanpassing van de Wbp zullen organisaties meer moeten gaan investeren in ICT-maatregelen, aangezien enerzijds op het niet (tijdig) melden van datalekken hoge boetes komen te staan en anderzijds het openbaar worden van

cyberincidenten (zeer) ongunstig is voor een organisatie.[68] De relevante vraag is dan wel hoeveel en op welke wijze een organisatie gaat investeren in het beheersen van cyberrisico's.

Er is ook sprake van een publiek belang. Het voorkomen van cyberincidenten heeft maatschappelijke relevantie gezien de schade die ook buiten de getroffen organisatie kan ontstaan. Deze schade van derden zal niet altijd (daar) verzekerd zijn dan wel niet altijd bij de organisatie verhaald kunnen worden. Daar komt nog bij dat veel consumenten en bedrijven vaak niet op de hoogte zijn van een cyberincident, althans van/via welke partij zij een virus hebben doorgekregen.

Bij het bestrijden van cybercriminaliteit en cyberterrorisme is nog evidenter een overheidsbelang aanwezig. Bovendien heeft de overheid er zelf ook belang bij om inzicht te hebben in adequate cyberveiligheid, gezien de eigen organisatie die beschermd dient te worden doch ook om eisen te kunnen stellen aan partijen waarmee men samenwerkt.

5.3 Delen van informatie over cyberveiligheidsprocedures en -maatregelen nodig

Zowel organisaties, verzekeraars als de maatschappij hebben derhalve een gedeeld en groot belang bij kennis over goede cyberveiligheid. Er is op dit moment echter (te) weinig informatie en weinig overeenstemming over wat effectieve procedures en maatregelen zijn.[69] Dat is naar het zich laat aanzien wel nodig om de cyberverzekeringsmarkt beter tot ontwikkeling te (kunnen) laten komen.[70] Als verzekeraars de effectiviteit van verschillende veiligheidsmaatregelen en -procedures beter kunnen beoordelen, zullen zij eerder bereid zijn om meer en/of andere dekking te geven.

Voor organisaties en de maatschappij is meer informatievergaring en -uitwisseling over cyberveiligheid en een ontwikkeling van de cyberverzekeringsmarkt ook relevant. De technologische en digitale ontwikkelingen geven bedrijven kansen om te innoveren en om – ondanks de toenemende concurrentie – vooruitgang te boeken (bijvoorbeeld webwinkels en automatisering van bedrijfsprocessen). Er is echter goed risicomanagement nodig om ervoor te zorgen dat het innovatiepotentieel wordt benut en tegelijkertijd de schaduwzijde van de moderne technologie – in de zin van cyberrisico's – zich zo min mogelijk realiseert. Met andere woorden, effectieve cyberveiligheidsprocedures en -maatregelen maar ook goede cyberverzekeringen zijn noodzakelijk om op verantwoorde wijze met innovatie en de daaruit voortvloeiende risico's om te gaan.

Het is dan ook wenselijk dat binnen een onafhankelijke organisatie of werkgroep aanbevelingen worden opgesteld over effectieve cyberveiligheidsprocedures en -maatregelen. Binnen deze organisatie/werkgroep kunnen dan anoniem ervaringen en gegevens worden uitgewisseld over cyberrisico's, de frequentie en de schade als gevolg daarvan.[71] Niet alleen private organisaties maar zeker ook overheidsorganisaties kunnen een belangrijke rol hebben bij het delen van dergelijke informatie. Aan de hand daarvan kunnen

richtlijnen voor technische veiligheidsmaatregelen worden ontwikkeld die verzekeraars in het acceptatieproces kunnen hanteren.[72] Ook kunnen binnen zo' n werkgroep ' best practices' worden ontwikkeld met betrekking tot cyberrisicomanagement en cyberveiligheidsprocedures. Verzekeraars hebben dan meer handvaten bij het (laten) onderzoeken hoe deze procedures bij aspirant-verzekerden intern zijn en werken.[73]

Een en ander brengt eveneens mee dat organisaties de cyberveiligheid op een adequaat niveau kunnen brengen. Zij kunnen dan beter een afweging maken tussen hun investeringen in interne risicomanagement-maatregelen en het afsluiten van een cyberverzekering (en de omvang daarvan). In het kader van de cyberverzekering heeft het investeren in effectievere maatregelen en procedures een positief effect op de premie maar ook op de niet-verzekerde en niet-verzekerbare risico' s.

Aangezien private organisaties niet uit zichzelf bovenbedoelde informatie zullen gaan delen, dienen verzekeraars en eventueel de overheid het voortouw te nemen – gezien hun eigen belang maar ook het belang van de Nederlandse economie – bij het vergaren van informatie en het opstellen van richtlijnen en benchmarks. Verzekeraars werken voor wat betreft hun eigen cyberveiligheidsmaatregelen en -processen samen met het Nationaal Cyber Security Centrum (NCSC) van het Ministerie van Veiligheid en Justitie.[74] Mogelijk zou dit ook een geschikte omgeving zijn, mede gezien het overheidsbelang, om de verschillende betrokkenen bij elkaar te laten komen en informatie te delen.

6.Conclusie

Cyberrisico' s vormen een steeds grotere bedreiging voor organisaties, zeker nu bij veel bedrijven de bedrijfsvoering (groten)deels online plaatsvindt. Cyberincidenten kunnen op verschillende manieren worden veroorzaakt en tot verschillende soorten en omvangrijke schade voor organisaties leiden. Daarmee wint het zoeken naar manieren om deze cyberrisico' s te beheersen aan belang en zal het ook steeds meer op het bordje van de bestuurders van organisaties terechtkomen. Verzekering vormt daarbij het sluitstuk van ICT-risicomanagement. De reeds langere tijd bekende schadeverzekeringen, zoals de inventarisverzekering en de AVB-verzekering, zijn echter niet toegesneden op cyberrisico' s en bieden slechts beperkt dekking tegen de schadelijke gevolgen van cyberincidenten. Gezien de leemten in de dekking van de traditionele schadeverzekeringen zijn en worden door verzekeraars en makelaars cyberpolissen ontwikkeld. Deze cyberverzekeringen geven meer dekking tegen cyberrisico' s en hebben toegevoegde waarde, maar staan in Nederland nog in de kinderschoenen. De cyberverzekering dient daarom nog te worden doorontwikkeld om meer aan de dekkingsbehoeften van een grotere groep organisaties te kunnen voldoen. Daarvoor zal wel nodig zijn dat er meer informatie beschikbaar komt over effectieve cyberveiligheid en dat door (onder meer) verzekeraars richtlijnen en benchmarks worden opgesteld over veiligheidsmaatregelen en -procedures. Slechts dan kunnen

verzekeraars op goede wijze de verschillende verzekerden met hun verschillende cyberrisico's onderscheiden en nadere eisen aan de cyberveiligheid stellen. Als verzekeraars minder onzekerheid hebben over de juistheid van de premie, de dekkingsvoorwaarden en de ingeschatte risico's, kan de cyberverzekeringsmarkt meer tot ontwikkeling komen.

Voetnoten

[1] Mr. dr. W.C.T. Weterings is advocaat bij Dirkzwager Advocaten & Notarissen, sectie Aansprakelijkheid, Schade en Verzekering, en als universitair docent verbonden aan de Universiteit van Tilburg, vakgroep Business Law. Citeerwijze: W.C.T. Weterings, 'Verzekering van cyberschade en -aansprakelijkheid. Voorziet de cyberverzekering (voldoende) in een behoefte van organisaties?', AV&S 2015/2, afl. 1.

[2] Aon, Cyberrisico's onder controle. Risicomanagement in het digitale tijdperk, White paper Juni 2012. Zie ook Marsh, Cyber risk and corporate governance, rapport februari 2014, p. 4 en Willis, How technology and telecom companies describe their cyber liability exposures, rapport februari 2014, p. 1 en p. 7. Het blijkt ook uit de toename van het aantal gevallen van data-inbreuk dat in het Verenigd Koninkrijk is gemeld bij UK's Information Commissioner's Office. In de periode 2007-2008 zijn er 79 gevallen gemeld, waar in de eerste periode van 2013-2014 reeds 723 meldingen zijn verricht. Zie Bank of England Financial Stability Report, 26 November 2013; Information Commissioner's Office (www.ico.org.uk).

[3] Verbond van Verzekeraars, Virtuele risico's, echte schade. Over het verzekeren van cyberrisico's, Position paper oktober 2013, p. 4.

[4] Aon Global Risk Management Survey 2011 en Aon Security Management Survey 2011.

[5] Zo hebben in 2011 80% van de 200 onderzochte IT-medewerkers aangegeven dat zij een of meer cyberaanvallen hebben ontdekt. Zie McAfee, In the Dark: Critical Industries Confronting Cyberattacks, 2011 (www.mcafee.com/us/about/news/2011/q2/20110419-01.aspx). In een ander onderzoek in 2011 van het Ponemon Institute kwam zelfs een percentage van 90% naar voren. Zie Ponemon Institute, Perceptions about network security, (www.juniper.net/us/en/local/pdf/additional-resources/ponemon-perceptions-network-security.pdf). Uit een wereldwijd onderzoek onder 2152 MKB-bedrijven volgde dat in een jaar tijd 73% van de bedrijven was getroffen door een cyberaanval en bij grote bedrijven lag het percentage op 75%. Zie Symantec, SMB Information Protection Survey, 2010 (www.symantec.com/content/en/us/about/media/pdfs/SMB_ProtectionSurvey_2010.pdf) en Symantec, State of Enterprise Security, 2010 (www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf). Uit het National Computer Security Survey in 2005 in opdracht van de Amerikaanse overheid bleek dat 67% van de 36.000 onderzochte bedrijven te maken had gehad met tenminste één cyberaanval en 43% zelfs met meer dan 10 aanvallen. Zie www.rand.org/content/dam/rand/pubs/technical_reports/2008/RAND_TR544.pdf.

[6] Aon, Cyberrisico's onder controle. Risicomanagement in het digitale tijdperk, White paper Juni 2012, p. 2.

[7] Zie over identiteitsdiefstal, B. McKelvey, Financial institutions' duty of confidentiality to keep customer's personal information secure from the threat of identity theft, University of California at Davis Law Review, 2001, p. 1077-1128.

[8] Verbond van Verzekeraars, Virtuele risico's, echte schade. Over het verzekeren van cyberrisico's, Position paper oktober 2013, p. 4.

[9] P. Hartman, Organisaties nog onvoldoende bewust van gevolgen cyberrisico' s, De Beursbengel december 2013, p. 7.

[10] J. Winn & K. Govern, Indentity theft: risks and challenges to business of data compromise, Temple Journal of Science, Technology & Environmental Law 2009, p. 52.

[11] Marsh, Cyber risk and corporate governance, rapport februari 2014, p. 10.

[12] Willis, How technology and telecom companies decribe their cyber liability exposures, rapport februari 2014, p. 3 en Verbond van Verzekeraars, Virtuele risico' s, echte schade. Over het verzekeren van cyberrisico' s, Position paper oktober 2013, p. 7.

[13] M.C. Arcuri, M. Brogi & G. Gandolfi, The effect of information security breaches on stock returns: Is the cyber crime a threat to firms?, EFMA workingpaper 2014, L.A. Gordon, M.P. Loeb & I. Zhou, The impact of information security breaches: Has there been a downward shift in costs? Journal of Computer Security 2011, p. 33-56, en A. Garg, J. Curtis & H. Halper, Quantifying the financial impact of IT security breaches, Information Management and Computer Security 2003-2, p. 74-83.

[14] ' Payment Processor Breach May Be Largest Ever' , Washington Post 20 januari 2009.

[15] Heartland Payment Systems Inc, Securities Litigation, 2009 WL 4798148 (D.N.J. 7 december 2009). De schadeclaim werd uiteindelijk door de rechtbank afgewezen maar heeft wel tot hoge juridische kosten geleid.

[16] P. Hartman, Organisaties nog onvoldoende bewust van gevolgen cyberrisico' s, De Beursbengel december 2013, p. 8.

[17] (Concept)Verordening 25 januari 2012, COM (2012) 11, artikel 79.

[18] Zie ' What Does the Heartland Data Breach Mean for the Future of Value in Merchant Acquiring?' , www.transactionworld.net/articles/2009/july/cover_story.asp. Zie ook Financial Times 23 juli 2009.

[19] Zie http://blog.willis.com/2014/02/directors-sued-for-cyber-breach en ook Marsh, Cyber risk and corporate governance, rapport februari 2014, p. 16.

[20] Advisen, D&O Claims Trends Q2 2013, p. 8 en bijl. 4.

[21] Zie ook J. Aikens, De gevolgen van cyberrisico' s worden sterk onderschat, Tijdschrift Administratie 2014-3, p. 14.

[22] L.A. Gordon, M.P. Loeb & T. Sohail, A framework for using insurance for cyber-risk management, Communications of the ACM 2003-3, p. 81-85.

[23] P. Hartman, Organisaties nog onvoldoende bewust van gevolgen cyberrisico' s, De Beursbengel december 2013, p. 7.

[24] Verbond van Verzekeraars, Virtuele risico' s, echte schade. Over het verzekeren van cyberrisico' s, Position paper oktober 2013, p. 7.

[25] Marsh, Cyber risk and corporate governance, rapport februari 2014, p. 14.

[26] Zie www.owm-ovo.nl/fraudeverzekering_bij_ovo.

[27] Aon, Cyberrisico' s onder controle. Risicomanagement in het digitale tijdperk, White paper Juni 2012, p. 9.

[28] Verbond van Verzekeraars, Virtuele risico' s, echte schade. Over het verzekeren van cyberrisico' s, Position paper oktober 2013, p. 8.

[29] Retail Ventures Inc. v. National Union Fire Insurance Company of Pittsburgh, 691 F.3d 821 (10-4576/4608), 6th Cir. (23 augustus 2012). Overigens werd hier uiteindelijk na uitleg van de polisbepaling door de rechter aangenomen dat ook indirecte schade onder de dekking viel, omdat een beperking tot directe schade hier niet expliciet (genoeg) was omschreven. Behalve dat het terug te voeren is op de specifieke omschrijving, zijn er ook veel andere uitspraken waarin die beperking tot dekking van directe schade wel werd aangenomen.

[30] J.W. Stempel, Stempel on insurance contracts, Aspen Publishers 2007, p. 23-45.

[31] Verbond van Verzekeraars, Virtuele risico' s, echte schade. Over het verzekeren van cyberrisico' s, Position paper oktober 2013, p. 8.

[32] In de Verenigde Staten is daar bij first party-verzekeringen veel discussie over. In Ward General Insurance Services Inc. v. Employers Fire Insurance Company, 114 Cal. App. 4th 548, 7 Cal. Rptr. 3d 844 (4th Dist. 2003) is beslist dat schade aan de software geen zaakschade is. In NMS Services Inc. v. The Hartford, 62 Fed.Appx. 511 (4th Cir. 2003) besliste de rechtbank echter dat het wissen van bestanden door een voormalige werknemer die de computer van het verzekerde bedrijf had gehackt, moet worden gezien als een materiële beschadiging in de zin van de polis. In American Guarantee & Liability Insurance Company v. Ingram Micro Inc., 2000 U.S. Dist. (D. Ariz. Apr. 18, 2000) is eveneens – in het kader van een bedrijfsschadeverzekering – overwogen dat het verlies van computer data moest worden gezien als materiële schade aan de computer van de verzekerde. In vergelijkbare zin: Lambrecht & Associates Inc. v. State Farm Lloyds, 119 S.W.3d 16 (Ct. App. Tex. 2003) en Southeast Mental Health Center Inc. v. Pacific Insurance Company Ltd., 439 F. Supp. 2d 831 (W.D. Tenn. 2006). Overigens is de Amerikaanse rechter bij third party-aansprakelijkheidsverzekeringen minder snel geneigd om zaakschade aan te nemen. ' Physical loss' van een verzekerde (vereist bij first party-opstal- en inventarisverzekering) wordt gezien als iets anders dan schade aan ' tangible property' van derden (vereist bij de third party aansprakelijkheidsverzekering). Bij alleen softwareproblemen is er in ieder geval geen zaakschade in de zin van de AVB-polis. Dit is in de Verenigde Staten ook beslist in America Online Inc. v. St. Paul Mercury Insurance Company, 347 F.3d 89 (4th Cir.2003). In Amerika wordt daar wel anders over gedacht als de computer-hardware wordt beschadigd of niet bruikbaar meer is als gevolg van een virus, worm, malware etc. Zie bijvoorbeeld Eyeblaster Inc. v. Federal Insurance Company, 613 F.3d 797 (8th Cir. 2010). Zie in dit verband ook Zurich American Insurance Company v. Sony Corporation of America, No. 651982/2011 (N.Y. Sup. Ct. New York Cty. 2011). Zie ook P.J. Kalis, T.M. Reiter & J.R. Segerdahl, Policyholder' s Guide to the Law of Insurance Coverage, Wolters Kluwer Law & Business 2003, p. 27-33 e.v.

[33] J. Aikens, De gevolgen van cyberrisico' s worden sterk onderschat, Tijdschrift Administratie 2014-3, p. 14 en Verbond van Verzekeraars, Virtuele risico' s, echte schade. Over het verzekeren van cyberrisico' s, Position paper oktober 2013, p. 8.

[34] J.H. Wansink, De algemene aansprakelijkheidsverzekering, Deventer: Kluwer 2006, p. 36 e.v.

[35] Er kan echter wel over getwist worden of dan geen sprake is van een verzekeringsrechtelijke zaaksbeschadiging, zie J.H. Wansink,

De algemene aansprakelijkheidsverzekering, Deventer: Kluwer 2006, p. 49 e.v.

[36] Bij alleen softwareproblemen is er in ieder geval geen zaakschade in de zin van de AVB-polis. Dit is in de Verenigde Staten ook beslist in America Online Inc. v. St. Paul Mercury Insurance Company, 347 F.3d 89 (4th Cir.2003). In Amerika wordt daar wel anders over gedacht als de computer-hardware wordt beschadigd of niet bruikbaar meer is als gevolg van een virus, worm, malware etc. Zie bijvoorbeeld Eyeblaster Inc. v. Federal Insurance Company, 613 F.3d 797 (8th Cir. 2010). Zie in dit verband ook Zurich American Insurance Company v. Sony Corporation of America, No. 651982/2011 (N.Y. Sup. Ct. New York Cty. 2011). Zie ook P.J. Kalis, T.M. Reiter & J.R. Segerdahl, Policyholder' s Guide to the Law of Insurance Coverage, Wolters Kluwer Law & Business 2003, p. 27-33 e.v.

[37] Creative Hospitality Ventures Inc. v. United States Liability Insurance Company, 655 F.Supp.2d 1316 (Second District Florida (2009). Hetzelfde werd geoordeeld bij het bijhouden door een internetprovider van de internetactiviteiten van klanten. Dit was eveneens een inbreuk op de privacy waarvoor het verzekerde bedrijf aansprakelijk was en ook hier werd de schade gezien als gedekte personenschade onder de AVB-verzekering. Zie Netscape Communications Corp. v. Federal Insurance Company, 343 F.App' x. 271 (9th Cir. 2009). Zie ook Hartford Casualty Insurance Company v. Corcino & Associates, 2013 WL 5687527 (C.D. Cal. 7 oktober 2013).

[38] J.W. Stempel, Stempel on insurance contracts, Aspen Publishers 2007, p. 23-63. Zie ook Willis, How technology and telecom companies describe their cyber liability exposures, rapport februari 2014, p. 8-9.

[39] Zie hierover L.J. Trautman & K. Altenbaumer-Price, The board' s responsibility for information technology governance, The John Marshall Journal of Computer & Information Law 2011-3, p. 313 e.v.

[40] J.W. Stempel, Stempel on insurance contracts, Aspen Publishers 2007, p. 23-61. Zie ook Aon, Cyberrisico' s onder controle. Risicomanagement in het digitale tijdperk, White paper Juni 2012, p. 10.

[41] Zie ook A. Lee, Insuring cyberspace, why traditional insurance policies are not enough: the nature of potential e-commerce losses & liabilities, Vanderbilt Journal of Entertainment Law and Practice 2001, p. 84-94.

[42] Verbond van Verzekeraars, Virtuele risico' s, echte schade. Over het verzekeren van cyberrisico' s, Position paper oktober 2013, p. 8.

[43] Vergelijk L.A. Gordon, M.P. Loeb & T. Sohail, A framework for using insurance for cyber-risk management, Communications of the ACM 2003-3, p. 82.

[44] ENISA, Incentives and barriers of the cyber insurance market in Europe, 2012, p. 8.

[45] P. Hartman, Organisaties nog onvoldoende bewust van gevolgen cyberrisico' s, De Beursbengel december 2013, p. 7 en ENISA, Incentives and barriers of the cyber insurance market in Europe, 2012, p. 8.

[46] Towers Watson Risk and Finance Manager Survey 2013, p. 1.

[47] Marsh, Cyber risk and corporate governance, rapport februari 2014, p. 15 geeft aan een stijging van 21% (klanten van Marsh die een cyberverzekering hebben afgesloten). In het Towers Watson Risk and Finance Manager Survey 2012, p. 1 wordt een

dekkingspercentage van 28% genoemd en een jaar later is dat percentage met 11% gestegen naar 39% (zie Towers Watson Risk and Finance Manager Survey 2013, p. 1 en p. 3; onderzoek bij 123 ondernemingen). De stijging in 2012 beliep slechts 1% aangezien 27% van de deelnemende ondernemingen in 2011 een cyberverzekering had (zie Towers Watson Risk and Finance Manager Survey 2011, p. 1).

[48] Vergelijk ENISA, Incentives and barriers of the cyber insurance market in Europe, 2012, p. 1, p. 14-15.

[49] R. Van de Laar, Cyberrisico' s: meer dan ICT, AMplus 2013-10, p. 50.

[50] Vergelijk met betrekking tot de Verenigde Staten The Betterley Cyber/Privacy Insurance Market Survey 2013, p. 2.

[51] Overigens is het onduidelijk of boetes (in alle gevallen) verzekerd kunnen/mogen worden. Er is discussie over of dat niet in strijd is met de openbare orde of goede zeden (artikel 3:40 BW). Zie A. Hendrikse, When public policy halts Dutch D&O fine coverage, Insurance Day 27 april 2011, p. 7, R. van Heffen, K. Lieverse en A. Schoonbeek, Risico' s op persoonlijke beboeting nemen toe, Goed Bestuur 2010-4, p. 32-33 en A. Walden, The publicly held corporation and the insurability of punitive damages, Fordham Law Review 1985-6, p. 1383 e.v.

[52] (Concept)verordening 25 januari 2012, COM (2012) 11, artikel 79.

[53] Kamerstukken II 2012/13, 33662, 3. Als de Europese privacyverordening wordt ingevoerd, zal deze de Privacyrichtlijn 95/46/EG vervangen en daarmee ook de Wbp (aangezien daarin deze richtlijn is geïmplementeerd). Er is toch in juni 2013 voor gekozen om het wetvoorstel meldplicht datalekken in te dienen (waarmee de Wbp wordt aangepast) omdat de verordening in dat stadium nog veel aanleiding tot vragen gaf (reikwijdte) en de verwachting was dat het nog geruime tijd zou duren voor de ontwerpverordening wordt vastgesteld (op zijn vroegst 2016).

[54] Dit volgt bijvoorbeeld uit een onderzoek van Marsh in India onder 150 risk & insurance managers van organisaties uit verschillende branches. Zie Financial Express 23 juni 2014.

[55] P. Hartman, Organisaties nog onvoldoende bewust van gevolgen cyberrisico' s, De Beursbengel december 2013, p. 7.

[56] L.A. Gordon, M.P. Loeb & T. Sohail, A framework for using insurance for cyber-risk management, Communications of the ACM 2003-3, p. 82. Zie ook ENISA, Incentives and barriers of the cyber insurance market in Europe, 2012, p. 1 en p. 19 en T. Bandyopadhyay, V.S. Mookerjee & R.C. Rao, Why IT managers don' t go for cyber-insurance products, Communications of the ACM 2009, p. 73.

[57] R.P. Majuca, W. Yurcik & J.P. Kesan, The evolution of cyberinsurance, working paper 2006 (http://arxiv.org/abs/cs/0601020), p. 8.

[58] L.A. Gordon, M.P. Loeb & T. Sohail, A framework for using insurance for cyber-risk management, Communications of the ACM 2003-3, p. 82.

[59] De verzekeraar kan dan bij iedere verzekerde een gemiddelde premie in rekening brengen in plaats van een individuele, op de karakteristieken van de verzekerde afgestemde premie. Dat betekent echter dat verzekerden met lage cyberrisico' s meebetalen aan de verzekering van verzekerden met hoge cyberrisico' s, met als mogelijk gevolg dat de verzekerden met lage cyberrisico' s van een verzekering afzien en de verzekeraar met verzekerden met hoge risico' s blijft zitten, tegen waarschijnlijk een te lage premie.

[60] A. Jain, Cyber crime: issues and threats, Delhi: Isha Books 2005, p. 25.

[61] Zie in het algemeen over moreel risico M.G. Faure & W.H. van Boom, Hoe houdbaar zijn gedragsveronderstellingen in verzekeringsrecht en -economie?, in: W.H. van Boom, I. Giesen, A.J. Verheij (red.), Gedrag en Privaatrecht – Over gedragspresumpties en gedragseffecten bij privaatrechtelijke leerstukken, Den Haag: BJU 2008, p. 311 e.v., M.G. Faure, Verzekeringen, in: W.C.T. Weterings (red.), De economische analyse van het recht, Den Haag: Boom juridische uitgevers 2007, p. 114 en L. Visscher, De economische rationale van het (nieuwe) verzekeringsrecht, Ars Aequi 2006, p. 486. Zie ook S. Shavell, On moral hazard and insurance, Quarterly Journal of Economics, p. 541-562.

[62] A. Jain, Cyber crime: issues and threats, Delhi: Isha Books 2005, p. 25. Zie ook T.M. Bandyopadhyay, S. Vijay & R.C. Rao, Why IT Managers don' t go for cyber-insurance products, Communications of the ACM 2009-11, p. 68-73.

[63] L.A. Gordon, M.P. Loeb & T. Sohail, A framework for using insurance for cyber-risk management, Communications of the ACM 2003-3, p. 83. Vergelijk ook O. Ben-Shahar & K.D. Logue, Outsourcing regulation: How insurance reduces moral hazard, Michigan Law Review 2012, p. 205.

[64] R.P. Majuca, W. Yurcik & J.P. Kesan, The evolution of cyberinsurance, working paper 2006 (http://arxiv.org/abs/cs/0601020), p. 3 en p. 11.

[65] W.S. Baer & A. Parkinson, Cyberinsurance in IT security management, IEEE Security & Privacy 2007, p. 50-56 en W. Yurcik & D. Doss, CyberInsurance: a market solution to the internet security market failure, WEIS Working paper 2002.

[66] R.P. Majuca, W. Yurcik & J.P. Kesan, The evolution of cyberinsurance, working paper 2006 (http://arxiv.org/abs/cs/0601020), p. 8-9 en L.A. Gordon, M.P. Loeb & T. Sohail, A framework for using insurance for cyber-risk management, Communications of the ACM 2003-3, p. 82.

[67] S.J. Shackelford, Should your firm invest in cyber risk insurance?, Business Horizons 2012-4, p. 349-356.

[68] P. Hartman, Organisaties nog onvoldoende bewust van gevolgen cyberrisico' s, De Beursbengel december 2013, p. 8.

[69] ENISA, Incentives and barriers of the cyber insurance market in Europe, 2012, p. 11 en A Friedman, Economic and policy framework for cybersecurity risks, The Center for Technology Innovation at Brookings working paper 2011 (www.brookings.edu/~/media/research/files/papers/2011/7/21%20cybersecurity%20friedman/0721_cybersecurity_friedman.pdf), p. 11.

[70] National Protection and Programs Directorate, U.S. Department of Homeland Security, Cybersecurity insurance workshop readout report, November 2012, p. 15 en p. 31.

[71] National Protection and Programs Directorate, U.S. Department of Homeland Security, Cybersecurity insurance workshop readout report, November 2012, p. 4 en p. 39.

[72] National Protection and Programs Directorate, U.S. Department of Homeland Security, Cybersecurity insurance workshop readout report, November 2012, p. 5.

[73] ENISA, Incentives and barriers of the cyber insurance market in Europe, 2012, p. 27.

[74] Verbond van Verzekeraars, Virtuele risico's, echte schade. Over het verzekeren van cyberrisico's, Position paper oktober 2013, p. 10.