Bernold Nieuwesteeg, Louis Visscher en Bob de Waard[1]

De Rechtseconomie van Cyberverzekeringen

Dit artikel onderzoekt de Nederlandse markt voor cyberverzekeringen voor het MKB. De resultaten duiden erop dat de bijdrage van de cyberverzekeringsmarkt aan de maatschappelijke welvaart haar volledige potentieel nog niet heeft bereikt. Het onderzoek mondt uit in een viertal aanbevelingen voor verzekeraars.

1. Inleiding

Cyberveiligheid staat steeds hoger op de agenda van grote en kleinere organisaties in Nederland. De recente cyberaanvallen Wannacry en Petya lieten zien dat cybercriminelen genadeloos suboptimale veiligheid afstraffen met grote (maatschappelijke) schade als gevolg.[2] Voor veel organisaties begint het cyberrisico een dusdanige proportie aan te nemen dat het verzekeren ervan economisch gezien rationeel kan zijn.
Grote organisaties hebben vaak al de mogelijkheid om 'op maat' cyberverzekeringen aan te schaffen als onderdeel van hun intensieve relatie met verzekeraars. Er is echter een kennislacune over de markt voor cyberverzekeringen voor het midden- en kleinbedrijf (MKB).[3] Het is belangrijk dat er goede instrumenten zijn voor het managen van het cyberrisico voor het MKB. Niet alleen omdat het MKB het merendeel van de Nederlandse economie beslaat, maar ook omdat de mate van cyberveiligheid grotendeels wordt bepaald door de zwakste schakel. Het zijn juist MKB'ers die kwetsbaar kunnen zijn voor cyberaanvallen. Er worden mogelijk onvoldoende specifieke beschermingsmaatregelen aan het MKB aangeboden en MKB'ers hebben wellicht onvoldoende inzicht in cybergerelateerde risico's.[4] Een suboptimale cyberveiligheid van het MKB kan door gecorreleerde risico's ook negatieve effecten hebben voor burgers, overheden en grotere bedrijven.

Het hoofddoel van dit artikel is het presenteren van een empirische rechtseconomische analyse van de cyberverzekeringscontracten voor het MKB. Het artikel is als volgt gestructureerd. Paragraaf 2 zal eerst uiteenzetten wat de redenen zouden kunnen zijn voor MKB'ers om te kiezen voor een cyberverzekering. We gaan ook in op de maatschappelijke baten van cyberverzekering en de huidige knelpunten in cybersecurity die het bereiken van

[1] Mr. ir. B.F.H. Nieuwesteeg is promovendus law and economics of cyber security bij het European Doctorate in Law and Economics (EDLE); Prof. mr. dr. L.T. Visscher is hoogleraar legal economic analysis of torts and damages bij het Rotterdam Institute of Law and Economics (RILE); B.R.J. de Waard Bsc LL.B is masterstudent ondernemingsrecht en econometrie.
[2] Lawrence and Robertson (2017) <https://www.bloomberg.com/news/articles/2017-05-18/the-wannacry-global-hack-could-have-been-much-much-worse> (bezocht op 29 september 2017); Sedee (2017) <https://www.nrc.nl/nieuws/2017/06/27/volg-hier-de-ontwikkelingen-rond-de-wereldwijde-randsomware-aanval-a1564740)> (bezocht op 28 september 2017).
[3] Belangrijke publicaties zoals Böhme and Schwartz (2010); Rawlings (2015); ENISA (2012); Biener, Eling and Wirfs, (2015) laten het MKB buiten beschouwing of noemen het marginaal.
[4] PGI Cyber, *SMEs are Vulnerable to Cyber Attacks* (augustus 2015), https://pgicyber.com/NewsandEvents/SMEs-are-vulnerable-to-Cyber-Attacks (bezocht op 20 september 2016).

die sociale baten nog deels verhinderen. Paragraaf 3 gaat in op de empirische strategie en methodologische benadering van dit onderzoek, presenteert de resultaten en analyseert deze in het licht van de knelpunten uit Paragraaf 2. Paragraaf 4 concludeert.

2. Het verzekeren van het cyberrisico

Waarom zouden MKB'ers cyberrisico's willen verzekeren? Een eerste, en meest traditionele benadering, is om een cyberverzekering te beschouwen als een oplossing voor risico-aversie.[5] Organisaties kunnen een aversie hebben tegen cyberrisico's met een lage kans en een hoge impact.[6] De verwezenlijking van sommige cyberrisico's, zoals DDoS- en ransomwareaanvallen en inbreuken op persoonsgegevens, kan tot grote schade leiden voor bedrijven.[7] Het is hier wel van belang de potentiële schade af te zetten tegen de solvabiliteit van het bedrijf. Het type risico dat bedrijven zouden willen verzekeren hangt dus van het feit af of deze in de lage kans-hoge schade categorie valt en of die schade de solvabiliteit van het bedrijf te boven gaat. Het informatietekort in cybersecurity, dat we hieronder zullen behandelen, bemoeilijkt deze afweging.
Een tweede reden die de vraag naar cyberverzekeringen zou kunnen verklaren is de reductie van transactiekosten voor de verzekerde.[8] Verzekeraars zijn potentieel beter in staat informatie te verzamelen met betrekking tot het op een efficiënte manier investeren in cyberveiligheid en eventuele schade af te handelen. De onderliggende aanname is dat verzekeraars meer informatie over de markt hebben dan de verzekerde, of deze tegen lagere kosten kunnen verzamelen.

Dat brengt ons bij een van de voornaamste maatschappelijke voordelen van de cyberverzekering. Zodra de verzekeraar de informatie over efficiënte wijzen om te investeren in cyberveiligheid, bijvoorbeeld door eigen onderzoek maar ook door de verzamelde claim-data, kan terug laten vloeien naar de verzekerden, ontstaan er maatschappelijke baten.[9] Die verzekerden kunnen hun gedrag nu immers aanpassen op basis van informatie die ze zelf niet, of alleen tegen hogere kosten, hadden kunnen verkrijgen.
Een tweede maatschappelijk voordeel van de cyberverzekering is dat het kan bijdragen aan het internaliseren van externe effecten.[10] Als een organisatie investeert in cyberveiligheid dan heeft dit vaak positieve effecten op andere organisaties. Een voorbeeld is het investeren in het reduceren van het risico op botnetinfectie. Een botnet is een netwerk van geïnfecteerde computers dat gebruikt kan worden voor DDoS aanvallen. In principe is een botnetinfectie zo ontworpen dat de eigenaar van de computer er geen last van heeft. De baten van het detecteren en verwijderen van zo'n infectie liggen dus niet bij de eigenaar van de

[5] Zie Shavell (2004, pp. 258-259).
[6] Koller, Lovallo and Williams (2012) <http://www.mckinsey.com/client_service/corporate_finance/latest_thinking/~/media/D2CF206B82C34F1FBB87FE591599A958.ashx> (bezocht op 29 september 2017). Vooral MKB'ers hebben een relatief beperkte mogelijkheid om te diversifiëren. Zeker van deze groep bedrijven kan worden aangenomen dat ze risico-avers zijn.
[7] Menno Sedee, 'Cyberaanval-blog: ook tweede terminal APM in Rotterdam deels open' (NRC) <https://www.nrc.nl/nieuws/2017/06/27/aanval-met-ransomware-op-containerbedrijf-haven-rotterdam-a1564693> (bezocht op 29 September 2017).
[8] Skogh (1989); Faure en Porrini (2017).
[9] Skogh (1991), pp. 360-370; Kesan et al. (2004); Biener, Eling en Wirfs (2015), pp. 131-158.
[10] Gordon, Loeb en Lucyshyn (2003), pp. 461-485

geïnfecteerde computer zelf, maar bij derden. Hierdoor krijgen eigenaren van computers te weinig prikkels (vergeleken met het maatschappelijke optimum) om te investeren in cyberveiligheid, omdat ze hiervan de kosten volledig zouden dragen, terwijl de baten vooral bij derden terecht komen. Een verzekering verzekert zowel organisaties die geïnfecteerd kunnen worden door het botnet, als ook organisaties die het risico lopen slachtoffer te worden van een DDoS aanval. Doordat de verzekeraar beide soorten schade overneemt, heeft hij betere prikkels om de verzekerde aan te sporen de wenselijke veiligheidsmaatregelen te treffen, dan deze uit zichzelf heeft..

Er is, zo bleek hierboven, dus voor bepaalde typen cyberrisico's een potentiële vraag naar verzekeringen en het verzekeren van die risico's brengt maatschappelijke baten met zich mee. Er zijn echter knelpunten, gerelateerd aan de aard van het cyberrisico, die de totstandkoming en ontwikkeling van een markt voor cyberverzekeringen bemoeilijken. We bespreken er twee.[11]
Het eerste knelpunt is het tekort aan data.[12] Om een premie te berekenen moet een cyberverzekeraar weten wat de verwachtingswaarde van het risico is bij de verzekerde. Het datatekort is niet alleen het gevolg van de relatief jonge leeftijd van de cyberverzekering, maar ook van de snel veranderende aard van kwetsbaarheden in soft- en hardwareproducten. Het tweede knelpunt is het feit dat door de verwevenheid van het internet, risico's sterk aan elkaar gecorreleerd zijn.[13] Dit bemoeilijkt het businessmodel van verzekeraars. Als een groot deel van het totaalrisico zich tegelijkertijd verwezenlijkt, dan zal een verzekeraar geen dekking meer kunnen bieden voor alle schade. De mate waarin gecorreleerde risico's het businessmodel van cyberverzekeraars aantasten is echter nog niet goed onderzocht in de literatuur.

De markt voor cyberverzekeringen groeit wereldwijd, al lopen de schattingen over de omvang van de groei uiteen.[14] Er zijn met name weinig empirische data beschikbaar over de groei van de Nederlandse markt, en meer specifiek voor het MKB. Dit artikel koppelt de empirie van de Nederlandse cyberverzekeringscontracten aan hun rechtseconomische wenselijkheid. Wij onderzoeken in hoeverre de contracten in staat zijn bij te dragen aan de ontwikkeling van de cyberverzekeringsmarkt voor het MKB en (daarmee) aan de maatschappelijke welvaart. We analyseren hoe en in welke mate verzekeraars omgaan met de inherente knelpunten in de cyberverzekeringsmarkt.

3. Empirische analyse: methode, resultaten en synthese

[11] Behalve de hier te bespreken knelpunten, zijn voorts te onderscheiden de voor verzekeringen meer algemene problemen van (omgekeerde) averechtse selectie als gevolg van informatie-asymmetrie, en de gedragsverandering van verzekerde: moreel risico. Deze problematiek komt in par. 3 aan de orde maar wordt hier kortheidshalve niet verder besproken.
[12] ENISA (2012); Biener et al. (2015)
[13] Baer en Parkinson (2007) (bezocht op 21 maart 2016).
[14] In de cyberverzekeringsmarkt in de VS zijn de jaarlijke brutopremies ongeveer geschat op 1.3 miljard USD met een jaarlijks groeipercentage van 10-25%. (Betterley (2013) <http://betterley.com/samples/cpims13_nt.pdf> (bezocht op 21 maart 2016) en 32% in 2014. Beshar (2015) <http://www.hsgac.senate.gov/hearings/protecting-america-from-cyber-attacks-the-importance-of-information-sharing> (bezocht op 21 maart 2016). Ook de Europese verzekeringsmarkt heeft zich ontwikkeld over de laatste jaren, mogelijk gedreven door steeds stringentere meldplichten van datalekken. (ENISA, 2012).

Methode

De kern van onze empirische strategie bestaat uit het opvragen van polisvoorwaarden voor cyberverzekeringen namens zes Nederlandse bedrijven.[15]

- Arbinn is een consultant voor de energie- en nutssector;
- Banketbakkerij de Waal (geconstrueerd) is een lokale bakkerij;
- Desiderius (geconstrueerd) is een belastingadvieskantoor voor het Nederlandse MKB;
- Eigensteil is een grafisch designbureau en softwareontwikkelaar, gericht op online ondernemen;
- FaceXXX (geconstrueerd) is een pornowebsite;
- Unibarge is een logistiek dienstverlener in de Rotterdamse haven.

Om eventuele differentiatie in premies en voorwaarden door verzekeraars waar te kunnen nemen, verschillen de ondernemingen in grootte en afhankelijkheid van IT-infrastructuur: Desiderius en Unibarge hebben een omzet van meer dan € 1 mln. terwijl de andere bedrijven daar onder zitten; Banketbakkerij de Waal heeft een lage afhankelijkheid van IT-infrastructuur; Unibarge, Arbinn en Desiderius hebben een gemiddelde afhankelijkheid en FaceXXX en Eigensteil zijn zeer afhankelijk van IT.

Voor elk van de ondernemingen hebben we offertes en polisvoorwaarden aangevraagd bij de verzekeraars of verzekeringsdistributeurs die op het moment van onderzoek cyberverzekeringen aanboden aan het Nederlandse MKB:[16] ACE, AIG, Allianz, AON, CNA, Chubb, Hiscox, HDI-Gerling en XL, waarbij HDI-Gerling ten tijde van het onderzoek slechts een verzekering aanbood tegen fraude bij online internet. Om een zuivere vergelijking tussen de verzekeraars mogelijk te maken, hebben we steeds gelijke dekking, eigen risico en maximale uitkering aangevraagd. In sommige gevallen was dit niet mogelijk doordat verzekeraars slechts standaard polissen met beperkte keuze aanboden.

Resultaten

In onze presentatie van de resultaten van het empirische onderzoek bespreken we eerst de aanvraagprocedure, gevolgd door de premies, gedekte schade, maximale uitkering en eigen risico, en risicoverlagende maatregelen. We analyseren op welke wijze de verkregen verzekeringscontracten de hierboven beschreven maatschappelijke baten van de cyberverzekering kunnen bewerkstelligen. We sluiten af met een overkoepelende synthese over de gepercipieerde strategie van verzekeraars in de markt en beantwoorden de vraag in hoeverre cyberverzekeringsproducten op dit moment bijdragen aan de maatschappelijke welvaart.

Aanvraagprocedure

[15] Drie zijn operationeel in Nederland en drie zijn geconstrueerd. Een uitgebreide beschrijving van de bedrijven is op aanvraag verkrijgbaar bij de auteurs.

[16] Voor zover wij hebben kunnen nagaan, waren dit alle verzekeraars die op het moment van onderzoek actief waren op de Nederlandse cyberverzekeringsmarkt voor het MKB.

In de aanvraagprocedure kan de verzekeraar informatieproblemen die reeds bestaan voorafgaand aan het tekenen van het contract, dus averechtse selectie, proberen te ondervangen.[17] De verzekerde kan namelijk proberen voordat het contract getekend wordt zijn cyberrisico (deels) te verhullen, waardoor de verzekeraar niet alle informatie heeft die hij nodig zou hebben om de premie te bepalen. Daardoor baseert de verzekeraar de premie op de gemiddelde risicoverdeling in zijn verzekeringspoule. Gevolg is dat de premie voor potentiële verzekerden met een laag risico te hoog is en zij zich niet verzekeren. Het gemiddelde risico in de poule loopt, de premie volgt, en de nu relatief goede risico's kunnen besluiten uit de poule te stappen. Dit kan erin resulteren dat uiteindelijk alleen de slechtste risico's zich willen verzekeren terwijl de betere risico's onverzekerd zijn. Hierdoor kunnen de maatschappelijke baten van verzekeringen dus niet ten volle bereikt worden. Voor een cyberverzekeraar is zowel belangrijk als complex om averechtse selectie tegen te gaan, omdat er een grote informatie-asymmetrie tussen de verzekerde en de verzekeraar bestaat.
Een manier om averechtse selectie tegen te gaan is het uitsluiten van bepaalde categorieën bedrijven die een hoger risico hebben. De onderzochte verzekeraars sluiten echter niet op voorhand bedrijven uit. In plaats daarvan sluiten ze *schade* die gerelateerd is aan bepaalde activiteiten uit van dekking. Drie van de door ons ontvangen polissen bevatten dergelijke clausules voor activiteiten op het gebied van gokken en pornografie. Het resultaat kan zijn dat het voor bedrijven in deze sectoren niet loont een verzekering af te sluiten nu zij (waarschijnlijk) geen dekking zullen krijgen vanwege de activiteiten die zij uitoefenen.
Hoewel twee verzekeraars cyberverzekeringen aanbieden die middels een eenvoudig webformulier zijn af te sluiten, bleek het aanvragen van een verzekering in 80% van de onderzochte gevallen een lastige en tijdrovende aangelegenheid. Niettemin heeft geen van de verzekeraars blijk gegeven van enige vorm van premiedifferentiatie op basis van de verstrekte risico-informatie. Ook hebben we geen aanwijzing gevonden van het bestaan van andere maatregelen tegen averechtse selectie dan de hierboven besproken uitsluiting van bepaalde activiteiten.

Premies
Tabel 1 presenteert de premies die door verzekeraars worden gehanteerd voor cyberverzekeringen voor het MKB in Nederland. De resultaten laten zien dat de premies voor bedrijven met een omzet tot €1 mln. tussen 0,26% en 0,53% van de verzekerde som ligt. Voor bedrijven met een omzet van meer dan € 1 mln. is dit 0,32% tot 0,99%. De premies voor cyberverzekeringen voor het MKB in Nederland variëren dus tussen 0,26% en 0,99% van de verzekerde som. In vergelijking met de meest recente premies die ons bekend zijn, afkomstig uit de Verenigde Staten en gemeten in 2004,[18] zijn de premies in de Nederlandse markt twee keer zo laag aan de onderkant, en zes keer zo laag aan de bovenkant van de bandbreedte.

Dat de gemiddelde prijs van een cyberverzekering voor het MKB met € 1.000 per jaar voor € 250.000 dekking nog steeds aanzienlijk duurder is dan een aansprakelijkheidsverzekering

[17] Böhme en Schwartz (2010) betogen dat het probleem van averechtse selectie een belemmering is voor de groei van de cyberverzekeringsmarkt.
[18] Kesan, Ruperto en Yurcik (2004). De onderzoekers vinden premies van 0,50% tot 6,00% van het verzekerde bedrag.

van €150 per jaar voor €2 mln. dekking,[19] impliceert nog niet dat de cyberverzekering 'te duur' is. Voor een dergelijke stelling is kennis over de verlies ratio (dat is, verliezen door geaccepteerde claims gedeeld door de ontvangen premies) noodzakelijk. Van deze *loss ratio* hebben we echter geen verifieerbare cijfers kunnen achterhalen. In gesprek met verzekeraars kregen we - "off the record" - de indicatie dat deze rond de 10% ligt, hetgeen kan betekenen dat de premie inderdaad te hoog is in vergelijking met de blootstelling aan verliezen.

De kleine verschillen tussen de aangeboden premies voor verschillende omzetten kunnen er op duiden dat verzekeraars niet gericht zijn op het differentiëren van premies of simpelweg niet de juiste data en methoden hebben om dit te doen.

Tabel 1: Premies als Percentage van de Verzekerde Som

Verzekeraar	*Klein (<€ 1 mln.)*	*Groot (>€ 1 mln.)*
ACE	0,53%	0,53% - 0,75%
AIG	0,33%	0,40% - 0,56%
Allianz	*Geen reactie - wel dekkingsvoorwaarden ontvangen*	
AON	0,26%	0,32% - 0,36%
Chubb	0,35%	0,35% - 0,99%
CNA	> 0,50% (*onvolledige informatie*)	
HDI-Gerling	*Slechts dekking voor fraude bij online bankieren*	
Hiscox	0,34%	0,34% - 0,74%
XL	*Geen reactie*	

Gedekte schade

Alle verzekeraars dekken in beginsel eigen schade en aanspraken van derden, hoewel er duidelijke verschillen bestaan in de specifieke dekkingsvoorwaarden en -limieten. Deze verschillen zien bijvoorbeeld op de dekking voor verliezen veroorzaakt door medewerkers, systemen of derden. Mogelijk is een achterliggende reden voor deze verschillen het verlangen van (sommige) verzekeraars om onzorgvuldige gedragingen van de verzekerde te ontmoedigen.

De dekking door Allianz en Chubb voor verliezen veroorzaakt door bedrijfsdiscontinuïteit is een concreet voorbeeld van de verschillen in de details. Allianz verschaft alleen dekking als gedragingen van een derde de oorzaak zijn van de verliezen, terwijl Chubb ook dekking verleent in het geval van een beveiligingsfout. Dergelijke details zijn niet te verwaarlozen - denk bijvoorbeeld aan de situatie waarin een bedrijf op zoek is naar dekking tegen uitbestede IT activiteiten. Slechts twee van de zeven onderzochte verzekeraars dekken deze schadeoorzaak, terwijl het voor vele MKB'ers vaste gewoonte is om hun IT-systemen zo te structureren.

De gedekte cyberschade lijkt dus op het eerste gezicht vergelijkbaar, maar bij een verdere beoordeling blijkt dat wel degelijk belangrijke verschillen bestaan. Een directe vergelijking op meerdere criteria zoals prijs, dekking en eigen risico, is complex. Elke verzekeraar heeft een eigen benadering voor de opzet van het contract; dezelfde juridische termen worden

[19] Zoals de 'MKB Meerkeuzepolis' van verzekeraar Achmea in 2015 met een verzekerd bedrag van € 5 mln. Details zijn op verzoek verkrijgbaar bij de auteurs.

anders uitgelegd, en uitgebreide uitsluitingsclausules zijn geen uitzondering. Het is voor MKB'ers lastig om voldoende (accurate) informatie te verzamelen om een geïnformeerde keuze te maken voor een cyberverzekering. Ter illustratie: het kostte ons vier maanden om een compleet overzicht van de markt te verkrijgen. Mogelijk zorgen de complexe aard van de cyberverzekering en de onbekendheid van verzekeraars met (de risico's van) het product ervoor dat de dekking zo tot in de details wordt bepaald.

Maximale uitkering en eigen risico

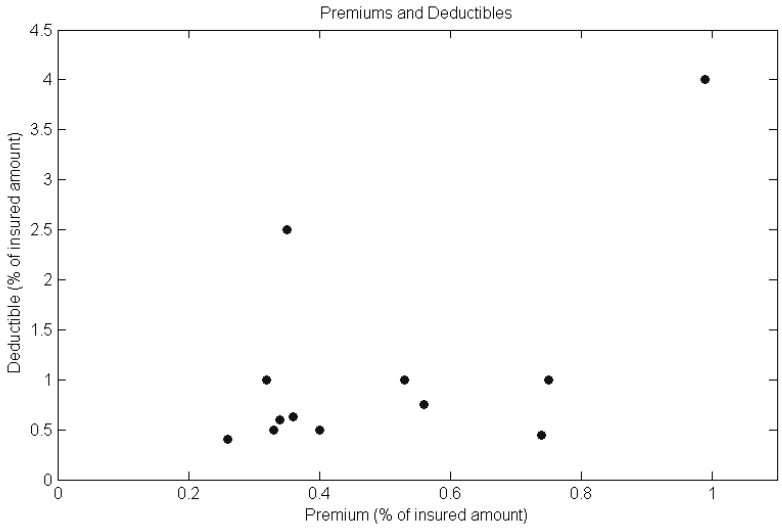
Met het instellen van een maximale uitkering en een eigen risico beogen verzekeraars het moreel risico te bestrijden. Moreel risico ziet op de mogelijkheid dat verzekerde zich minder zorgvuldig gaat gedragen nadat hij (een deel van) zijn risico heeft overgedragen aan de verzekeraar en dus niet langer volledig zelf hoeft op te draaien voor de gevolgen van zijn handelen. Door het instellen van een maximale uitkering en een eigen risico, kunnen verzekeraars verzekerden blootstellen aan een gedeelte van het risico en zo moreel risico proberen terug te dringen.

Alle verzekeraars maken gebruik van limieten op de uitkering. Bij de meeste cyberverzekeraars kunnen verzekerden zelf de verzekerde som en de maximale uitkering bepalen, welke bepalend zijn voor de hoogte van de premie. Voor kleine bedrijven varieert de maximale uitkering tussen de € 250.000 en € 1 mln.; voor grotere ondernemingen kregen we maximale uitkeringen aangeboden tot € 2,5 mln. Verzekeraars proberen dus hun verzekerden gedeeltelijk bloot te stellen aan het risico via een maximum op de uit te keren som.

Figuur 1 zet het eigen risico af tegen de verschuldigde premie, en laat zien dat het eigen risico tussen € 1.000 en € 100.000 ligt, ofwel tussen 0,40% en 4,00% van het verzekerde bedrag. Het loont dus voor verzekerden om het eigen risico een rol te laten spelen in hun keuze. De vraag blijft niettemin in hoeverre MKB'ers hun risico kennen en kunnen doen aan een dergelijke zelfselectie.

Hoewel de precieze polisvoorwaarden van verzekeraar tot verzekeraar verschillen en moeilijk te vergelijken zijn, verraadt het verschil van een factor 10 in het eigen risico dat de verzekeraars wel degelijk verschillen in hun risicoperceptie, dat zij hun pijlen richten op verschillende delen van de markt, en/of dat zij verschillende indrukken hebben van het moreel risico.

Figuur 1: Premies en Eigen Risico's



Vanuit het gezichtspunt van maatschappelijke welvaart zou het te verwachten zijn dat verzekeraars producten aanbieden met een hoog eigen risico en hoge maximale uitkering omdat verzekerden graag hun lage kans-hoge schade risico's willen afdekken. Niettemin bevatten de geobserveerde contracten relatief lage maximale uitkeringen en een laag eigen risico. Relatief lage maximale uitkeringen kunnen ongunstig zijn voor de vraag naar cyberverzekeringen, omdat hoge schade risico's onvoldoende worden afgedekt terwijl er juist behoefte is om catastrofale cyberaanvallen te dekken. Bovendien kan het de bereidheid om schade te declareren negatief beïnvloeden wanneer deze slechts voor een klein deel gedekt wordt maar bedrijven wel de administratieve lasten en de negatieve publiciteit hebben wanneer zij met hun schade in de openbaarheid moeten treden om te kunnen claimen. Een laag eigen risico is op het eerste gezicht gunstig voor kopers van cyberverzekeringen, maar niet echt nodig, omdat hiervoor eenvoudig een bedrag op de balans gereserveerd kan worden. Een hoog eigen risico daarentegen kan leiden tot lagere premies, meer klanten en dus meer beschikbare data, hetgeen weer kan leiden tot een aantrekkelijker product met lagere prijzen.

Risicoverlagende maatregelen

Alleen verzekeraars AIG en ACE hebben moreel risico clausules in hun polis die aan verzekerden verplichtingen opleggen om in aanmerking te komen voor dekking van schade.[20] We hebben geen relatie gevonden tussen het hebben van dergelijke clausules en de hoogte van de premie. Geen van de contracten bevat een *bonus-malus* systeem waarin no-claim gedrag beloond wordt met lagere premies en vice versa. AIG verlangt van de verzekerde dat die "*all reasonable steps"* neemt om aan de standaarden van het aanvraagformulier te voldoen, zoals elke zes maanden de dataherstelmogelijkheden testen. ACE verlangt onder meer van de verzekerde dat deze elke week een back-up maakt en antivirussoftware installeert en updatet.

De verplichting voor de verzekerde om bepaalde risico-verlagende maatregelen te treffen, is een belangrijke manier waarop de verzekeraar kan bijdragen aan de maatschappelijke

[20] Zie hierboven onder *Maximale uitkering en eigen risico* voor een korte beschrijving van het begrip ‘moreel risico’.

welvaart. In dat opzicht is de beperkte mate waarin risico-verlagende vereisten aanwezig zijn een gemiste kans. Een achterliggende verklaring kan zijn het gebrek aan claim data uit het verleden waardoor verzekeraars geen accurate inschatting van de benodigde maatregelen kunnen maken. Toch zijn er wel degelijk 'best practices' in de markt, die nu niet via de verzekeraar gedeeld worden met de verzekerden. Dit impliceert niet dat verzekeraars in het geheel geen strategieën hanteren om moreel risico te beperken - we constateerden immers eerder dat er wel degelijk gebruik wordt gemaakt van een eigen risico en maximale uitkeringen.

Verzekeraars en hun strategieën

Bij het ontstaan en het ontwikkelen van een cyberverzekeringsmarkt speelt de volgende paradox: enerzijds hebben verzekeraars accurate en recente data nodig om hun producten te kunnen prijzen en risico te kunnen inschatten zodat zij een aantrekkelijk product in de markt kunnen zetten; anderzijds is een aantrekkelijk product nodig dat afgenomen wordt door bedrijven zodat er daadwerkelijk claimdata beschikbaar komen. Uit ons empirisch onderzoek blijkt dat verzekeraars wel degelijk mogelijkheden zien in de Nederlandse cyberverzekeringsmarkt voor het MKB. We observeren twee benaderingen die verzekeraars kunnen volgen.
Ten eerste zijn er de verzekeraars die de markt op vrij agressieve wijze benaderen met gemakkelijk af te sluiten polissen en een aantrekkelijke prijs-dekkingsratio. Ten tweede zijn er meer voorzichtige verzekeraars die eerst en vooral zijn gericht op het aanbieden van producten die hun eigen risico's beheerst houden, resulterend in verzekeringen met uitgebreide aanvraagprocedures en hogere prijzen.
Het overgrote deel van de aanvraagprocedures uit ons onderzoek was moeilijk en tijdrovend. Daarnaast zijn premies en dekkingen lastig te vergelijken, zowel voor experts als voor MKB'ers, omdat de duivel in de details zit. Het is ons niet duidelijk geworden of de verzekeraars hier bewust voor kiezen om gebruik te kunnen maken van hun informatievoorsprong, of dat onzekerheid hierin veeleer een bepalende rol speelt.
Het gebruik van standaardclausules zou naar onze mening de concurrentie kunnen vergroten, omdat afnemers polissen dan beter kunnen vergelijken en de benodigde data geaggregeerd kan worden. Anderzijds zijn verzekeraars dan niet meer in staat snel te reageren op ontwikkelingen in de markt, hetgeen de concurrentie beperkt. [21]

4. Conclusie

Dit artikel heeft de Nederlandse markt voor cyberverzekeringen onderzocht voor het MKB. Nederland is een voorbeeld van een Europees land met een ontwikkelde digitale infrastructuur en is middels de interne markt van de Europese Unie verbonden met andere Lidstaten. De gevonden resultaten verschillen kwantitatief mogelijkerwijs met de resultaten die in andere Lidstaten gevonden zouden worden, maar kwalitatief zijn de conclusies generaliseerbaar naar andere landen binnen de EU en/of met een ontwikkelde digitale economie, zoals de Verenigde Staten.

[21] Avraham (2012).

Alhoewel de resultaten een momentopname zijn van een zich snel ontwikkelende markt, kunnen we wel stellen dat verzekeraars tussen twee strategieën te lijken twijfelen. Gaan zij voor marktaandeel en het snel verkrijgen van claimdata, of betreden ze de markt voorzichtiger om geen slachtoffer te worden van de potentieel sterk correlerende schadeclaims? Het is in ieder geval duidelijk dat op dit moment een kernfunctie van de cyberverzekeringsmarkt nog onvoldoende functioneert: namelijk die van de informatie-overdracht van 'best practices' gerelateerd aan het rendement van cybersecurity investeringen teneinde meer weerbaar te zijn voor cyberaanvallen. Daarmee heeft de bijdrage van de cyberverzekeringsmarkt aan de maatschappelijke welvaart naar onze mening haar volledige potentieel nog niet bereikt.

De resultaten leiden tot het doen van een drietal aanbevelingen. Allereerst zou men kunnen overwegen de aanvraagprocedure te vereenvoudigen. Hierdoor is het voor MKB'ers meer kostenefficient om verschillende offertes aan te vragen. Ten tweede zou een basiscyberverzekering, die niet in allerlei details verschilt, kunnen helpen om de keuze tussen verzekeraars te vergemakkelijken. Ten derde zou kunnen worden overwogen om claimdata verplicht publiek te maken om de informatiecirculatie die onder andere nodig is voor premie-inschatting en moreel risico clausules op gang te brengen. Tot slot adviseren we een goede analyse te maken van andere methoden van cyberrisicoverschuiving. Een voorbeeld hiervan is het delen van het risico, ook wel 'pooling' genoemd. Pooling kan potentie hebben als de verzekeraar niet meer informatie over de markt heeft dan de verzekerde. In dat geval kunnen de verzekerden mogelijk efficiënter onderling informatie uitwisselen in een pool.

Literatuurlijst

R. Avraham, 'The Economics of Insurance Law: A Primer', 19 Connecticut Insurance Law Journal 29 112 (2012).

W. S. Baer en A. Parkinson, 'Cyberinsurance in IT Security Management' (2007) 5(3) IEEE Security & Privacy 50.

R. S. Betterley, 'Cyber/Privacy Insurance Market Survey 2013, The Betterley Report' (2013) <http://betterley.com/samples/cpims13_nt.pdf> bezocht op 21 maart 2016.

P. J. Beshar, 'Protecting America from Cyber-Attacks: The Importance of Information Sharing, US Senate Committee on Homeland Security & Governmental Affairs' (Hearing U.S. Senate Committee on Homeland Security, 2015) <http://www.hsgac.senate.gov/hearings/protecting-america-from-cyber-attacks-the-importance-of-information-sharing> bezocht op 21 maart 2016.

C. Biener, M. Eling and J.H. Wirfs, 'Insurability of Cyber Risk: An Empirical Analysis' (2015) 40(1) Geneva Papers on Risk and Insurance 131.

R. Böhme en G. Schwarz, 'Modelling cyber-insurance: Towards A Unifying Framework' (Ninth Annual Workshop on the Economics of Information, Boston, 2010)

<http://www.econinfosec.org/archive/weis2010/papers/session5/weis2010_boehme.pdf> bezocht op 30 augustus 2017.

M.G. Faure en D. Porrini, 'Göran Skogh on Risk Sharing and Environmental Policy' (2017) 42(2) The Geneva Papers on Risk and Insurance – Issues and Practice 177.

L.A. Gordon, M.P. Loeb en W. Lucyshyn, 'Sharing information on computer systems security: an economic analysis' (2003) 22(6) Journal of Accounting and Public Policy 461.

J.P. Kesan, M.P. Ruperto en W.J. Yurcik, 'The Economic Case for Cyberinsurance' (2004) Working paper, University of Illinois, IL.

G. Skogh, 'The Transactions Cost Theory of Insurance: Contracting Impediments and Costs' (1989) 56(4) The Journal of Risk and Insurance 726.

G. Skogh, 'Insurance and the Institutional Economics of Financial Intermediation' (1991) 16 The Geneva Papers on Risk and Insurance 360.

ENISA, 'Incentives and Barriers of the Cyber Insurance Market in Europe' (Report for the European Commission, 2012).

PGI Cyber, 'SMEs are Vulnerable to Cyber Attacks' (2015) <https://pgicyber.com/NewsandEvents/SMEs-are-vulnerable-to-Cyber-Attacks> bezocht op 20 september 2016.

Ph. Rawlings, 'Cyber Risk: Insuring the Digital Age' (2015) Queen Mary School of Law Legal Studies, Research Paper 189.

S. Shavell, *Foundations of Economic Analysis of Law* (Harvard University Press 2004).