Waarover collega's bij Turien & Co. en Ansvar spreken

Cyberrisicoverzekeringen

Ansvar idéa
VERZEKERINGEN

TURIEN&CO
ASSURADEUREN

Inleiding

In korte tijd is digitalisering tot in alle haarvaten van onze samenleving doorgedrongen. De afhankelijkheid van een goed werkende en betrouwbare digitale infrastructuur is groot. Misschien te groot. Die afhankelijkheid leidt ertoe dat wanneer er storingen optreden niet alleen het ongemak, maar ook de concrete financiële schade steeds vaker groot is.

De basis van de maatschappelijke waarde van het verzekeringsbedrijf is dat het de financiële gevolgen van incidenten en calamiteiten beheersbaar kan maken. Misschien heeft de sector daarnaast een nog belangrijkere meerwaarde doordat met zijn kennis van oorzaken van calamiteiten de samenleving geholpen kan worden maatregelen te nemen om die calamiteiten te voorkomen. Geld in de vorm van schadevergoeding is zelden compensatie voor al het leed en alle emoties die door cyberincidenten ontstaan. Cyberrisicoverzekeringen kunnen sturend en stimulerend inwerken op het aanbrengen van minimale veiligheidsmaatregelen die het risico van cyberincidenten niet wegnemen maar wel verkleinen.

Voor de verzekerbaarheid van risico's is echter nodig dat er sprake is van een onvoorzienbaar voorval, er voldoende ervaring is opgebouwd om goede inschattingen te maken van de kans dat het onvoorzienbare voorval intreedt en de schadeclaims voor de verzekeraars te dragen zijn, ook wanneer door een incident veel verzekerden tegelijkertijd worden geraakt. Deze kernelementen van verzekeren in het algemeen zijn bij het risico van schade door calamiteiten binnen de digitale infrastructuur nog niet uitgekristalliseerd.

Wij weten zeker dat de cyberrisicoverzekering in de komende jaren net zo belangrijk gaat worden als bijvoorbeeld de bedrijfsaansprakelijkheidsverzekering. Wij staan echter aan de start van een leerproces dat nog ruime tijd in beslag zal nemen, voordat wij over cyberrisico kunnen spreken als zijnde een stabiel onderdeel van de verzekeringsmarkt.

Financieel advieskantoren doen er verstandig aan deze ontwikkeling vanaf de start mee te maken en ook zelf geleidelijk kennis en ervaring op te bouwen.

Turien & Co. en Ansvar hebben in het kader van het AdviesSupport[1] met financieel adviseurs gesproken over hun ervaringen met cyberrisicoverzekeringen. Wij hebben de wens dat de ervaringen en tips die deze kantoren geven andere ondernemers helpen aandacht te schenken aan het groeiende risico van storingen in de digitale infrastructuur voor zowel bedrijven als particulieren.

Alkmaar/Amsterdam, april 2023

[1] AdviesSupport is een initiatief van Turien & Co., Ansvar en Bureau DFO met het doel financieel advieskantoren praktische informatie te verschaffen die deze kantoren versterkt in hun bedrijfsvoering. Voor meer informatie zie www.adviessupport.nl

AdviesSupport

Inhoudsopgave

1 Cyberrisicoverzekeringen: wat is hierbij de positie van de adviseur?

1.1 Inleiding

Waarom zou je als financieel advieskantoor aandacht besteden aan de cyberrisicoverzekering? Klanten vragen er zelden om. Elk kantoor heeft het druk met de advisering en begeleiding van haar relaties op andere gebieden. Waarom dan tijd besteden aan “weer” een nieuw aandachtsgebied. Het vak is al moeilijk genoeg!

1.2 Overeenkomst van opdracht

Wanneer een relatie aan een financieel adviseur vraagt “iets” te doen en het kantoor zegt toe dit te gaan doen, dan ontstaat er een overeenkomst. Namelijk een overeenkomst van opdracht als bedoeld in artikel 7:400 van het Burgerlijk Wetboek. Deze overeenkomst ontstaat ook wanneer de relatie en de adviseur niets op papier zetten en de relatie geen kostenvergoeding voor het werk van de adviseur betaalt.

Kan worden vastgesteld dat de adviseur de relatie zou “adviseren” op het gebied van verzekeringen dan ontstaat daarmee een overeenkomst van opdracht. Dit leidt dan direct tot de vraag hoever dit advies moet gaan? Is het bijvoorbeeld verplicht om in een gesprek met de ondernemer ook aandacht te geven aan het onderwerp cyberrisico en de financiële gevolgen die cyberincidenten voor de onderneming kunnen hebben?

1.3 Keuze bij de overeenkomst van opdracht

Wanneer adviseur en klant met elkaar in contact komen over de verzekeringen van de onderneming dan hebben partijen de keuze:

Of men kiest ervoor om heel precies te bepalen wat de werkzaamheden van de adviseur/bemiddelaar zullen inhouden. Bijvoorbeeld een risico- inventarisatie voor het vervoer van de producten die de relatie in Nederland maakt en die vervolgens naar de afnemers van deze onderneming in Zwitserland worden vervoerd. Onderneming en adviseur kunnen hierbij duidelijk afspreken dat de taak van de adviseur “beperkt” blijft tot het adviseren op welke wijze de specifieke risico’s van vervoer van de producten naar Zwitserland verzekerd kunnen worden. Tot meer is de adviseur dan niet gehouden.

Adviseur en onderneming kunnen ook een “ open relatie” met elkaar aangaan waarbij de ondernemer ervan uitgaat dat de adviseur in algemene zin met de ondernemer in gesprek zal gaan over de risico’s die het bedrijf in de volle breedte van haar bedrijfsactiviteiten loopt en op welke wijze via verzekeringen de financiële gevolgen van het intreden van bepaalde risico’s beheersbaar gemaakt kunnen worden.

1.4 Rechters en KiFiD geven aan wat de klant mag verwachten

Indien partijen ervoor kiezen om niet in detail af te spreken welke werkzaamheden de adviseur voor de relatie gaat verrichten, dan mag de relatie een prestatie verwachten zoals een redelijk handelend en redelijk bekwaam adviseur die in de gelijke situatie zou hebben geleverd.

Rechters en de geschillencommissie KiFiD hebben dit in vele uitspraken “ingevuld”. Hieronder een passage hoe de geschillencommissie KiFiD dit omschrijft. Deze omschrijving geldt zowel voor advisering aan particulieren als aan ondernemers.

Bij deze beoordeling moet vooropgesteld worden dat een tussenpersoon op grond van artikel 7:401 BW tegenover zijn opdrachtgever verplicht is om bij zijn werkzaamheden de zorg te betrachten die van een redelijk bekwaam en redelijk
handelend beroepsgenoot verwacht mag worden. Van de assurantietussenpersoon mag worden verwacht dat hij beschikt over de nodige deskundigheid en vakkennis, dat hij de financiële belangen van zijn cliënten naar bewust weten en kunnen behartigt en dat hij zorgvuldigheid betracht in de advisering.

De algemene zorgplicht uit het arrest van de Hoge Raad is ingevuld in de jurisprudentie. In dat kader is onder meer bepaald dat de assurantietussenpersoon moet waken voor de belangen van de verzekeringnemers bij de tot zijn portefeuille behorende verzekeringen. Daarbij hoort ook dat de assurantietussenpersoon de verzekeringnemer tijdig opmerkzaam maakt op de gevolgen die hem bekend geworden feiten voor de tot zijn portefeuille behorende verzekeringen kunnen hebben. Het gaat dan om feiten die aan de assurantietussenpersoon bekend zijn of hem redelijkerwijs bekend behoorden te zijn.3 De zorgplicht van de assurantietussenpersoon geldt niet alleen ten tijde van het sluiten van de overeenkomst maar vergt een voortdurende bemoeienis door de assurantietussenpersoon met de tot zijn portefeuille behorende verzekeringen. Een assurantietussenpersoon mag dus in beginsel niet stil blijven zitten wanneer hij tijdens de looptijd van de tot zijn portefeuille behorende verzekeringen kennisneemt van feiten of omstandigheden die meebrengen dat de door hem beheerde verzekeringen mogelijk aanpassing behoeven.

3 Zie Hoge Raad 10 januari 2003, ECLI:NL:HR:2003:AF0122, NJ 2003/375, overweging 3.4.1.

1.5 Alle feiten en omstandigheden

Bij het zoeken naar wat de relatie van de financieel adviseur had mogen verwachten in het geval dat partijen hierover geen gedetailleerde afspraken hebben gemaakt, zullen alle feiten en omstandigheden een rol kunnen spelen.

Belang kan bijvoorbeeld worden gehecht aan de vraag hoe het advieskantoor zich in haar algemene uitingen presenteert. Vermeldingen als “specialist zakelijke schadeverzekeringen” of “wij streven met u een totaalrelatie na” of “wij doen een integrale risicoanalyse” zijn vanuit juridisch oogpunt uitspraken op grond waarvan een relatie bepaalde verwachtingen mag baseren.

1.6 Attenderen op cyberrisico is niet vrijblijvend

Financiële schade als gevolg van cyberincidenten is een algemeen en inmiddels veel voorkomend risico voor vrijwel elke onderneming en organisatie. Van een redelijk handelend en redelijk bekwaam adviseur mag de relatie verwachten dat deze het cyberrisico bij zijn risico-inventarisatie signaleert en hierover met de relatie in gesprek gaat. Het is vervolgens aan de relatie om te beslissen wat hij met deze signalering en advisering doet.

Wil een adviseur niets met cyberverzekeringen te maken hebben, dan zal de adviseur dit onmiskenbaar duidelijk moeten maken aan de relatie en de relatie adviseren voor dit onderwerp zich te wenden tot een andere adviseur. Het “wegkijken” van het risico en hierover op geen enkele wijze met de relatie in gesprek gaan is vanuit juridisch oogpunt voor de financieel adviseur geen optie. Niet vanuit de professionaliteit van waaruit het kantoor wil functioneren. Ook niet vanuit het voorkomen van claims in het kader van gemaakte beroepsfouten die in dit geval dan bestaan uit het niet bespreekbaar maken van risico’s die de ondernemer wel overduidelijk loopt.

1.7 Legitimatie belang advies

Handhaving van het systeem van is voor de samenleving belangrijk. Onder meer omdat deze adviseurs het initiatief nemen om hun relaties te attenderen op risico’s waaraan mensen liever niet willen denken, zoals bij de overlijdensrisicoverzekering, of waarvan relaties zich onvoldoende van het risico bewust zijn.

In de loop der tijd is te zien dat het belang van de aanwezigheid van onafhankelijke adviseurs per product kan veranderen. Aan de onderkant van de verzekeringsproducten is te zien dat klanten meer en meer zich bewust zijn van het risico dat zij lopen en eventueel zelf in staat zijn deze verzekeringen rechtstreeks af te sluiten.

Tegelijkertijd ontstaan aan de bovenkant van de markt nieuwe gebieden waar de relatie zich niet bewust is van de keuzen die hij moet maken. Voorbeelden zijn de Wet Toekomst Pensioen waar weinig werknemers zich nog bewust zijn van de gevolgen van de veranderingen van deze wijzigingen. Maar dat geldt dus ook voor ontwikkelingen in het zakelijke verkeer. Wie weet welke risico’s bijvoorbeeld de ontwikkeling van artificial intelligence te brengen?

Wat wij wel weten is dat de aandachtsgebieden die er voor de financieel adviseur “bij” komen bijna altijd een stuk ingewikkelder zijn dan de gebieden die al geruime tijd bestaan. Dat vraagt van de adviseur elke keer weer inspanningen om zich te verdiepen in die nieuwe gebieden.

De bereidheid om die inspanning telkens weer te verrichten vormt het bestaansrecht van het systeem van het systeem van onafhankelijk financieel advies.

2 Cyberrisicoverzekeringen: wat zijn de bijzondere kenmerken?

2.1 Inleiding

Cyberrisicoverzekeringen zijn relatief nieuwe producten. De markt hiervan staat nog in haar kinderschoenen. Op een aantal gebieden heeft dit deel van de markt kenmerken die zich niet of in minder mate voordoen bij andere branches.

2.2 Premievolume

De bij het Verbond van Verzekeraars aangesloten verzekeringsmaatschappijen boekten in 2022 samen ongeveer 40 miljoen euro premie uit cyberrisicoverzekeringen. Van deze premie heeft ongeveer 95% betrekking op verzekeringen ten behoeve van grote ondernemingen. Het totale premievolume zal groter zijn wanneer ook gekeken wordt naar verzekeringen die bedrijven rechtstreeks, al dan niet via de holdingstructuur waartoe zij behoren, buiten Nederland worden afgesloten.

2.3 Weinig data

Hoewel cyberincidenten zich veelvuldig voordoen, beschikken verzekeringsmaatschappijen nog maar beperkt over data op grond waarvan de ontwikkeling van het risico over een langere tijd kan worden geanalyseerd. Een beperkte set aan data leidt ertoe dat het voor verzekeraars lastig is om voor een langere termijn een stabiel premieniveau aan te bieden.

De combinatie van een beperkte set aan data over *oorzaken* van schades en de *financiële gevolgen* per type incident leidt tot een sector waarin premies frequent worden aangepast. Zeker omdat de oorzaken van incidenten zich ook nog ontwikkelen. Een voorbeeld van zo een ontwikkeling is bijvoorbeeld het fenomeen RaaS (*Ransomware as a Service*) waarbij organisaties onderling complete dienstverleningspakketten aan andere criminele organisaties aanbieden om ransomware aanvallen uit te voeren. Zo een ontwikkeling komt op enig moment op en beïnvloedt op dat moment de risico-statistiek omdat het uitvoeren van randsomaanvallen gemakkelijker en effectiever wordt gemaakt.

2.4 Sterk verschillende voorwaarden

De markt van cyberverzekeringen kenmerkt zich ook door verzekeringsvoorwaarden die per aanbieder sterk verschillen. Dit geldt zowel voor de risico's waarvan wordt aangegeven dat deze verzekerd worden als voor de duidelijkheid waarmee risico's worden uitgesloten. Het aantal aanbieders dat in haar polisvoorwaarden uitdrukkelijk aangeeft dat schade als gevolg van een cyberincident bestaande uit *bederf* van voedsel (dat bijvoorbeeld in koelcellen was opgeslagen) uitdrukkelijk is meeverzekerd is zeer beperkt.

Maar dit betekent niet dat de andere verzekeraars dit type schade automatisch niet onder de dekking van de verzekering laten vallen. Eerst bij een schade kan dan duidelijk worden welke interpretatie de betreffende verzekeraar hanteert ten aanzien van dekkingen en uitsluitingen.

Een ander voorbeeld is dat tussen aanbieders verschil in dekkingsvoorwaarden geldt met betrekking tot de vraag of schade aan lokale opslag van data wel of niet onder de dekking van de verzekering valt.

De wachttijden die gelden voordat schade als gevolg van een cyberincident wordt vergoed, kunnen ook per aanbieder sterk verschillen.

Het zijn voorbeelden van verschillen in dekkingsvoorwaarden zoals die vandaag de dag aanwezig zijn in de verzekeringsvoorwaarden op de Nederlandse verzekeringsmarkt. Verschillen die na een calamiteit voor de ondernemer grote gevolgen kunnen hebben voor de vraag of de verzekering een deel van de schade die hij als gevolg van het incident leidt wel of niet vergoedt.

2.5 Termen zijn veelal technisch van aard

De verzekeringsvoorwaarden bevatten over het algemeen een fors aantal termen die bekend zijn bij mensen die in de ICT-branche werken maar niet of minder bekend zijn bij bijvoorbeeld financieel adviseurs en hun zakelijke klanten.

2.6 Risico van cumulatie is groot

Een verzekeringsmaatschappij die door heel Nederland bijvoorbeeld 1.000 woningen verzekert tegen het financiële risico als gevolg van brand zal er niet zo snel mee worden geconfronteerd dat in een korte tijdspanne de helft van deze woningen in vlammen opgaat. Elk jaar zal er wel aan enkele woningen schade plaatsvinden. Maar niet in één jaar aan alle woningen tegelijkertijd. Daar waar zoiets wel denkbaar zou zijn, bijvoorbeeld als gevolg van een oorlog of natuurramp, is deze risico-oorzaak van de dekking door de verzekering uitgesloten.

Bij cyberrisicoverzekering is het risico dat gelijktijdig bij een groot aantal verzekerden schade optreedt wel aanwezig. Sterker nog: dat kan van externe partijen die deze schade veroorzaken juist de opzet zijn. Dit cumulatierisico stelt grenzen aan de marktpositie die aanbieders in specifiek dit marktsegment kunnen en willen innemen.

2.7 Beperkt aanbod aan voorwaardenvergelijking

Een relatief kleine markt, polisvoorwaarden die in een hoge frequentie veranderen, termen en begrippen die nog weinig uniform zijn: dit zijn geen eigenschappen die het voor software ondernemers aantrekkelijk maken software te ontwikkelen en te onderhouden waarmee adviseurs geholpen worden bij het maken van vergelijkingen van verzekeringsvoorwaarden op het gebied van het cyberrisico.

2.8 Oproep AFM

In februari 2023 heeft de AFM aandacht gevraagd voor de resultaten uit twee onderzoeken die de toezichthouder kort daarvoor had gedaan naar cyberrisicoverzekeringen. De AFM signaleert dat de hoeveelheid cyberrisico's, zoals bijvoorbeeld ransomware-aanvallen, is de afgelopen jaren sterk zijn toegenomen.

In reactie hierop spreekt de AFM de verwachting uit dat de markt voor zakelijke en particuliere cyberverzekeringen gaat groeien.

Uit de onderzoeken die de AFM heeft gedaan constateert de AFM dat cyberverzekeringen onderling moeilijk te vergelijken zijn. Dit komt door de complexiteit van de voorwaarden, het gebrek aan eenduidige definities van kernbegrippen en dekkingen die (nog) niet volledig expliciet zijn gemaakt door verzekeraars.

Het volgende citaat van de AFM uit deze verkenning is een oproep waaraan adviseur en aanbieders gehoor zouden moeten geven:
"Een betere onderlinge vergelijkbaarheid van de dekking van het product kan hieraan bijdragen. Zo worden klanten en adviseurs in staat gesteld om nu en in de toekomst de juiste risico's af te dekken en worden voorzienbare teleurstellingen voorkomen."

2.9 Sterk verschillende dekkingsonderdelen

Een ander kenmerk van de cyberrisicoverzekering is dat de dekkingsonderdelen van de meeste cyberrisicoverzekeringen onderling sterk verschillen en in de beleving van de ondernemer niet automatisch geassocieerd worden met het risico van cyberincidenten.

In basis dekken cyberrisicoverzekeringen veelal de risico's van:

- Kosten van hulp en ondersteuning om de beschadigde data te herstellen.
- De kosten van de schade die het bedrijf oploopt als gevolg van het cyber-incident.
- De kosten van het oplossen van ransomware en eventuele vergoeding van het losgeld bij cyberafpersing.
- De kosten die het gevolg zijn om bij een datalek de regels van de AVG in acht te nemen, alsmede de boetes die de Autoriteit Persoonsgegevens bij een datalek eventueel oplegt.

Dit zijn onderling sterk verschillende risico's met als gemeenschappelijk kenmerk dat deze het gevolg kunnen zijn van cyberincidenten. In de beeldvorming van de doelgroep kan echter gemakkelijk één specifiek risico in beeld zijn dat door de gesprekspartner voor de onderneming niet als relevant wordt ervaren. Denk bijvoorbeeld aan de ondernemer van de kleine timmerfabriek die houtskeletbouw uitvoert die ervan uitgaat dat bij hem "niets te halen is en hij "dus" niet snel slachtoffer zal worden van ransomware". Misschien is die veronderstelling juist, maar deze ondernemer vergeet dat het verlies van data van de specificaties van de eerdere opdrachten en de blokkades van digitaal aangestuurde machines in zijn bedrijf, de continuïteit van zijn onderneming in korte tijd onder druk kan zetten.

3 Cyberrisicoverzekeringen: hoe bouw je als kantoor hierover kennis op?

3.1 Inleiding

Financieel advieskantoren die het als hun verantwoordelijkheid zien om in contacten met relaties ook het onderwerp cyberrisico bespreekbaar te maken, zullen hiervoor kennis moeten opbouwen. Hieronder geven wij een aantal tips van collega's die al enige tijd geleden zijn begonnen dit risico vast onderdeel van hun analyses te maken.

3.2 Medewerker die voorloopt met digitale gadgets

Misschien heb je ook zo een collega. Altijd vol enthousiasme over de nieuwste, digitale gadgets. Maar ook iemand die je als eerste vraagt even met jou mee te kijken op het moment dat jouw computer niet doet wat jij graag zou willen. Die collega's kunnen de ideale personen zijn om het kantoor te helpen kennis op het gebied van cyberrisicoverzekeringen op te bouwen. Wanneer zo een collega de vraag krijgt om per week een of twee uur te besteden aan het verzamelen van informatie over cyberrisicoverzekeringen, dan zullen elke week mini-stapjes worden gezet. Maar na een jaar blijken al die kleine stapjes samen toch een heel grote stap te zijn en bij te dragen aan een belangrijk onderscheid ten opzichte van veel andere kantoren.

3.3 Polis vergelijking

Anders dan bijvoorbeeld hypothecair krediet zijn er nog maar een beperkt aantal partijen die de voorwaarden van cyberrisicoverzekeringen kunnen vergelijken. In de markt zijn er wel een aantal partijen die op onderdelen deze dienst wel aanbieden. Onder meer Turien &Co., SUREbusiness en Polisvergelijker zijn partijen die op dit gebied diensten leveren. In een aantal situaties gaat het hierbij om een vergelijking van een deel van de markt en niet de hele markt. Kennis verwerft een kantoor door ook zelf een aantal voorwaarden te vergelijken. Hiervoor werd de suggestie gedaan om één specifieke medewerker te vragen per week een of meer uren aan het onderwerp cyberrisicoverzekering te besteden. Voorstelbaar is dat een polis vergelijking van de voorwaarden van een aantal aanbieders met wie het kantoor een relatie onderhoudt een waardevol onderdeel van deze tijdsinvestering kan uitmaken.

3.4 Workshops

Niet alleen opleidingsorganisaties maar ook aanbieders, serviceproviders en Turien & Co. bieden regelmatig workshops aan ten behoeve van financieel adviseurs. Veelal ontvangen deelnemers daarbij aanvullend materiaal dat gebruikt kan worden voor de verdere opbouw van de kennis over dit risico binnen het kantoor.

3.5 Cyberlunches

Ondernemers leren het meeste van andere ondernemers. Door het land zijn er meerdere collega's die cyberrisicoverzekeringen nadrukkelijker onderdeel willen laten zijn van hun adviespraktijk. Het kan zeer vruchtbaar zijn om bijvoorbeeld eens per kwartaal in een vaste samenstelling met een aantal collega's bij elkaar te komen om met elkaar ervaringen en tips uit te wisselen. Naast het feit dat praten met collega's over "het vak" vaak gewoon leuk is, is het voor het verwerven van inspiratie en concrete tips ook zeer effectief.

Mocht je dergelijke bijeenkomsten zinvol vinden, maar zelf niet over het netwerk beschikken dan kun je hiervoor altijd een oproep laten uitgaan via Advies Support.

3.6 Exposure calculator

Op het internet zijn diverse cyber risico calculators te vinden. Dit zijn programma's die aan de hand van een aantal in te voeren gegevens een indicatie geven van het financiële risico dat een specifieke onderneming loopt als gevolg van cyberincidenten.

Hoewel de adviseur voorzichtig moet zijn om de uitkomsten van deze programma's te gebruiken als basis van zijn advies aan een ondernemer is het wel leerzaam om in het kader van het verwerven van kennis en vaardigheid op dit terrein eens een aantal ondernemingen waarvoor het kantoor als adviseur op het gebied van verzekeringen optreedt door deze programma's te halen.

Een voorbeeld van een dergelijk programma is te vinden via de volgende link:
https://www.hiscox.nl/nl-nl/cyber-exposure-calculator/#results

4 Cyberrisicoverzekeringen: hoe zet je als kantoor deze nieuwe activiteit neer?

4.1 Inleiding

Wanneer je als financieel advieskantoor actief wilt worden op het gebied van cyberrisicoverzekeringen, wat zijn dan de tips die kantoren met iets meer ervaring geven? Een aantal van deze suggesties tref je hieronder aan.

4.2 Accountant

Naast het financieel advieskantoor is de accountant voor veel ondernemers een van de andere belangrijke adviseurs. Veel accountantskantoren beschikken zelf over een cyberrisicoverzekering en zijn zich bewust van de mogelijke, financiële gevolgen van een cyberincident voor hun relaties. Over het algemeen zal een accountant het advies aan de ondernemer om aandacht te schenken aan het cyberrisico dus ondersteunen. Voor het advieskantoor kan het waardevol zijn om een communicatiestructuur te onderhouden met de accountants van de zakelijke klanten van het kantoor.

4.3 ICT bedrijven in het eigen netwerk

Veel assurantiekantoren werken in hun eigen netwerk al samen met ICT-bedrijven. Bijvoorbeeld omdat het kantoor de verzekeringen van die bedrijven verzorgt. Of omdat het ICT-bedrijf diensten levert aan het advieskantoor. De tip voor het kantoor is om een lijst aan te leggen van ICT-bedrijven die het kantoor op deze wijze al binnen zijn netwerk heeft. Vervolgens kunnen met deze ICT-bedrijven gezamenlijke activiteiten worden opgezet die de digitale vaardigheid stimuleren en de digitale veiligheid verhogen.

4.4 Specialiseren

Een medische adviespraktijk kent op het gebied van cyberrisico's heel andere eigenschappen dan bijvoorbeeld een supermarkt. Een financieel advieskantoor kan ervoor kiezen zich te specialiseren in het cyberrisico binnen bepaalde branches. In het stadium waarin de markt thans verkeert, kan vrij snel een relevant onderscheidende positie worden opgebouwd voor wat betreft kennis van de betreffende branche in relatie tot cyberrisicoverzekeringen, kennis van de processen om voor het risico een passende offerte te krijgen en kennis van de aanbieders die bereid zijn voor deze branches offertes af te geven. Focus op een beperkt aantal branches zal over het algemeen leiden tot hogere conversies en kortere doorlooptijden.

5 Cyberrisicoverzekeringen: welke tips zijn er voor het adviesgesprek?

5.1 Inleiding

Het moment is daar. Je gaat in gesprek met jouw klant over het onderwerp cyberrisicoverzekeringen. Kunnen collega's "met ervaring" jou daarvoor tips geven? Jazeker.

5.2 Standaard in onderhoudsgesprekken

Het cyberrisico is een reëel risico. Zoals wij in het eerste hoofdstuk beschreven mag de klant van een redelijk handelend en redelijk bekwaam adviseur verwachten dat deze tijdens de risico-inventarisatie aandacht geeft aan dit risico.

Het is uiteraard aan de klant wat hij met de constateringen en de adviezen van jou als adviseur doet. Maar in het geheel het cyberrisico niet benoemen is juridisch onjuist en niet in het belang van de klant.

Bij nieuwe relaties en tijdens de periodieke onderhoudsgesprekken dient dit onderwerp daarom standaard te worden opgenomen, tenzij jij als adviseur uitdrukkelijk en aantoonbaar hebt aangegeven het onderwerp cyberrisicoverzekering niet tot jouw aandachtsgebied te rekenen. Indien de adviseur voorafgaand aan het bezoek al een agenda stuurt van de onderwerpen die besproken gaan worden kan op deze agenda het onderwerp "cyberrisico" worden vermeld.

5.3 Jouw gesprekspartner heeft geen antwoord op al jouw vragen

Stel je hebt een gesprek met een partner van een architectenbureau. Deze gesprekspartner zal je alles kunnen en willen vertellen over bijvoorbeeld bouwmaterialen, hoe sterk de prijzen zijn gestegen en hoe moeilijk het is noodzakelijke materialen op tijd geleverd te krijgen. Maar vraag jij vervolgens hoe exact de back-up-procedure van het ICT-systeem binnen het kantoor is geregeld en hoe vaak deze ook daadwerkelijk wordt getest dan is de kans groot dat het wat stiller wordt.

Veel van de informatie die jij voor een goed advies nodig hebt, zal menig ondernemer niet weten en moeten vragen aan de ICT-dienstverlener van wie de onderneming gebruik maakt. Natuurlijk kun je de lijst met vragen achterlaten. Maar dan weet je hoe dat gaat. Iedereen heeft het druk. Die vragen blijven dan liggen. Een (beter) alternatief is om een aantal vragen ruim van tevoren te sturen en aan jouw gesprekspartner te vragen de antwoorden hierop al voor het fysieke gesprek aan jou te sturen.

5.4 Jong of oud. Het maakt echt een verschil

Is jouw gesprekspartner jong of oud? Maakt dat wat uit? Jouw collega's ervaren regelmatig dat dit toch wel iets uitmaakt.

Voor jongeren is het risico van cyberincidenten iets dat ze kennen en als realiteit ervaren. Je hoeft hen dus veel minder te overtuigen dat dit een reëel risico is. Maar juist binnen de groep jongeren leeft vaak de idee dat "ze" zelf ook verstand hebben van cyberbeveiliging en in staat zijn om incidenten buiten de deur te houden.

Ouderen daarentegen zijn minder bekend met het risico en vinden veel "rust" in de wetenschap dat in de jaren van hun ondernemerschap "er nog nooit iets is gebeurd"; dus op grond daarvan nemen zij aan dat gedurende de paar resterende jaren van hun ondernemerschap ook wel niets meer zal gebeuren. De wetenschap dat door de ICT-onderneming waarvan de ondernemer gebruik maakt, is verteld dat er een "firewall" is, geeft dan vaak een onterecht gevoel van onkwetsbaarheid voor cyberincidenten. Waarbij cyberincidenten nog te veel worden verengd tot ransom aanvallen.

Als adviseur zal je beide invalshoeken moeten herkennen en de uitleg paraat moeten hebben om aan te tonen dat beide redeneringen begrijpelijk zijn, maar daarom nog niet juist zijn.

5.5 Stel W & H-vragen

Ga ervanuit uit dat jouw gesprekspartner zich niet bewust is van het financiële risico dat zijn onderneming loopt. Was dat wel het geval geweest, dan had de ondernemer waarschijnlijk zelf wel het initiatief genomen om contact met jou te zoeken.

In het gesprek zal je de klant dus versneld zich ervan bewust moeten laten worden dat zijn onderneming significante risico's loopt. In plaats van een stroom informatie op jouw gesprekspartner af te vuren, kun je dit inzicht bij jouw gesprekspartner misschien met meer resultaat laten ontstaan door W & H-vragen te stellen. In W & H-vragen staat de W voor "Wie en Wanneer" en de H voor "Hoe". Vragen dus die zich niet met een "ja" of "nee" laten beantwoorden.

Voorbeelden van vragen die ertoe kunnen leiden dat het onderwerp cyberrisico gaat leven, zijn bijvoorbeeld

- Hebben jullie een wachtwoordmanager?
- Hoe lang is de continuïteit van de onderneming geborgd indien jullie tijdelijk niet meer de mogelijkheid hebben om facturen uit te sturen?
- Hoe groot is het risico dat afnemers van jullie bedrijf alternatieve leveranciers vinden indien jullie als gevolg van een cyberincident tijdelijk niet kunnen leveren?
- Hoe regelen jullie de back-ups en worden deze wel eens in het kader van testen teruggezet?
- Hoe is jullie beleid ten aanzien van afvoer van printers en de daarin soms aanwezige harde schijf?
- Welk protocol hebben jullie voor digitale veiligheid bij thuiswerken?
- Wat betekent het voor jouw bedrijf indien de systemen een week niet bereikbaar zijn?
- Wie bel je bij een cyberaanval?

Via deze en andere vragen zullen de meeste ondernemers de mogelijke consequenties van het onderwerp cyberrisicoverzekeringen beter gaan begrijpen.

5.6 Argumenten ter onderbouwing van het advies

In het gesprek dat de adviseur met de ondernemer heeft is het verstandig dat de adviseur achtergrond informatie heeft bij argumenten waarom een ondernemer besluit een cyberrisicoverzekering af te sluiten. Een aantal belangrijke kernelementen zijn onder meer;

- Vindt er incident plaats dan is het belangrijk dat je direct kunt terugvallen op **specialisten** die ook binnen enkele uren aan de slag gaan. Voorkom dat je moet gaan zoeken wie je kan helpen, offertes moet aanvragen etc. Daar is bij een calamiteit allemaal geen tijd voor.

- De kans op een cyberincident is op dit moment 1:9. Cyberincidenten komen daarmee **vaker voor dan brand**. Waar het afsluiten van een brandverzekering een punt van afweging is, is dit ten onrechte nu nog wel voor het cyberrisico.

- Ook kleinere bedrijven lopen het risico van cyberincidenten. Incidenten met als achtergrond het verkrijgen van losgeld vindt misschien meer plaats bij grote bedrijven, maar cyberaanvallen en storingen zonder opzet vinden ook massaal plaats bij **kleinere bedrijven**.

- Raakt een onderneming als gevolg van een cyberincident in staat van faillissement dan kan onder omstandigheden de bestuurder van de onderneming door de crediteuren **aansprakelijk** worden gesteld indien de bestuurder aantoonbaar onvoldoende maatregelen heeft genomen om de risico's van cyberincidenten tegen te gaan.

Cyberincidenten kunnen zich herhalen. Ongeveer 1/3 van de bedrijven die losgeld betaalden werden nadien een 2e keer doelwit van cybercriminelen.

5.7 De klant volgt jouw adviezen niet op

De klant mag weigeren met jou in gesprek te gaan over het onderwerp cyberrisicoverzekering (geen tijd) of jouw adviezen om dit risico te verzekeren (te duur) niet opvolgen.

Wanneer er zich nadien dan een cyberincident voordoet, is het maar de vraag of de klant zich deze voorgeschiedenis op dezelfde manier herinnert als jij. De rechtspraak staat bol van procedures waarin mensen na geruime tijd bepaalde gesprekken zich volstrekt verschillend herinneren.

Ben jij overtuigd van het belang een bepaald onderwerp te bespreken of geef jij een advies dat de klant niet wil opvolgen, zorg dan dat in de toekomst aantoonbaar is, dat:

- Jij het aanbod voor het gesprek hebt gedaan of het advies hebt gegeven.
- De klant het aanbod of het advies heeft afgewezen.
- Jij de klant hebt geïnformeerd over de mogelijke consequenties van zijn besluit bij een calamiteit.
- Jij de klant de ruimte hebt gegeven dat de klant altijd op jouw aanbod kan terugkomen als de klant dat wenst.

AdviesSupport

Checklist

Cyberrisicoverzekeringen

AdviesSupport

Veel tips: maar welke zijn voor jouw kantoor interessant?

Nr.		Actie	Misschien actie	Geen actie
1.	Voert het advieskantoor een beleid waarin duidelijk met de klant wordt overeengekomen op welke gebieden wel en op welke gebieden het advieskantoor niet adviseert en is de uitvoering van dit beleid per klant reproduceerbaar?			
2.	Heeft het kantoor een keuze gemaakt of het wel of niet actief wil worden op het gebied van cyberrisicoverzekeringen?			
3.	Is er binnen het kantoor minimaal een specifieke collega die tot taak heeft kennis over cyberrisicoverzekeringen voor het kantoor op te bouwen en de ontwikkelingen op dit gebied te volgen?			
4.	Heeft het kantoor bepaald op welke wijze de polisvoorwaarden van de aanbieders met wie op het gebied van cyberrisicoverzekeringen wordt samengewerkt efficiënt en kwalitatief goed kunnen worden vergeleken?			
5.	Inventariseert het kantoor welke workshops/webinars op het gebied van cyberrisicoverzekeringen partners, met wie het kantoor samenwerkt, aanbieden?			
6.	Is er interesse periodiek met collega's ervaringen en tips uit te wisselen op het gebied van cyberrisicoverzekeringen?			
7.	Voert het kantoor een actief communicatiebeleid met de accountants van de zakelijke klanten die het advieskantoor adviseert?			
8.	Heeft het kantoor in beeld welke ICT-gerelateerde klanten tot de relatiekring gerekend kunnen worden?			
9.	Wordt er met lokale ICT bedrijven samenwerking gezocht om de digitale veiligheid bij de lokale ondernemers te verbeteren?			
10.	Is het voor het kantoor mogelijk op het gebied van cyberrisicoverzekeringen de focus op specifieke branches te richten om daarmee snel een onderscheidende dienstverlening te kunnen aanbieden?			
11.	Is het onderwerp cyberrisicoverzekeringen vast onderdeel bij de risico-inventarisatie bij nieuwe relaties?			
12.	Is het onderwerp cyberrisicoverzekeringen vast onderdeel in de checklist onderhoud en nazorg?			
13.	Beschikt jouw kantoor over een checklist die voorafgaand aan het gesprek aan de onderneming wordt gezonden met het verzoek dit samen met de ICT dienstverlener van de onderneming in te vullen?			
14.	Beschikt jouw kantoor over modellen waarin op reproduceerbare wijze wordt vastgelegd wanneer een relatie om hem moverende redenen gegeven adviezen niet wenst op te volgen?			