CONCORDIA DE KEIZER
Riskmanagement & Benefits

FAQ – alles wat u wilt weten over de cyberverzekering

Onze cyberspecialisten merken dat er rondom cyberrisico's en cyberverzekeringen vaak dezelfde vragen leven. Daarom hebben we de meest gestelde vragen voor u op een rij gezet.

Is een cyberverzekering zinvol voor mijn organisatie?

Dekking tegen cyberrisico's is van meerwaarde voor elke onderneming die afhankelijk is van zijn digitale systemen en/of beschikt over vertrouwelijke informatie en/of klantgegevens. Per 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG, ook wel General Data Protection Regulation (GDPR)) van kracht. Deze Europese privacywetgeving stelt o.a. eisen aan het veilig bewaren van gegevens. Hierdoor lopen bedrijven een aanmerkelijk aansprakelijkheidsrisico. Naast het aansprakelijkheidsrisico voor schade aan derden, kan ook de schade die bedrijven zelf lijden door cybercriminaliteit, falen van systemen en menselijk handelen desastreus zijn. Diefstal of verlies van gevoelige informatie over klanten of werknemers kunnen iedere onderneming overkomen. Het verlies van één laptop kan al tot ernstige financiële gevolgen en reputatieschade leiden. Een cyberverzekering voorziet daarbij niet alleen in een financiële tegemoetkoming, ook de 'incident response'-diensten worden gedekt.

Is de aansprakelijkheid voor cyberincidenten (bijvoorbeeld datalekken) verzekerd onder algemene aansprakelijkheidsverzekeringen?

Traditionele aansprakelijkheidsverzekeringen bieden zelden dekking voor aansprakelijkheid naar aanleiding van cyberincidenten. In de regel bieden algemene aansprakelijkheidsverzekeringen alleen dekking in geval van letsel of fysieke schade. Daarnaast zien wij de ontwikkeling dat onder de aansprakelijkheids-verzekeringen, waaronder vermogensschade, steeds vaker cyberincidenten en/of datalekken worden uitgesloten. Een cyberverzekering biedt hiervoor wél dekking.

Hoe bepaal ik welk risico ik kan of wil dragen? En hoe bepaal ik de dekkingslimieten bij een cyberverzekering?

Het is van belang om uw cyber-gerelateerde scenario's na te lopen om inzicht te krijgen in de maximale schade die u als organisatie kunt of wenst te dragen. Die schade bestaat onder andere uit notificatiekosten, IT-kosten, dataherstel, juridische kosten, pr-kosten, datadiefstal, afpersing en netwerkinterruptie. Concordia de Keizer heeft expertise op dit gebied en kan u adviseren, zodat u tot een gepaste dekkingslimiet komt. Het eigen risico hangt af van de omvang van uw bedrijf, maar ook van een keuze die u als klant maakt en het risico dat u zelf kunt ofwel wenst te dragen.

Mijn bedrijf maakt gebruik van antivirussoftware en data-encryptie. Is een cyberverzekering dan wel nuttig?

Hoewel deze middelen zeker kunnen helpen schade te voorkomen of beperken, vormen ze geen gegarandeerde bescherming tegen datalekken of andere cyberincidenten. Cybersecurity en cyberverzekeringen zijn complementair aan elkaar. Er zijn tal van voorbeelden van grote multinationals die het slachtoffer werden van cybercrime. Zelfs de beste antivirussoftware en de meest ervaren in-house IT-experts konden dit niet verhinderen. Bovendien zijn meer dan 40 procent van de claims te herleiden naar menselijk of systeem-falen. Met andere woorden; 100 procent veiligheid bestaat niet.

Mijn IT-expert zegt dat onze maatregelen op het gebied van cybersecurity op orde zijn en wij geen risico lopen. Heb ik een cyberverzekering wel nodig?

Voor cyberrisico's geldt dat zelfs de beste cybersecuritymaatregelen niet kunnen garanderen dat hackers u niet raken. U kunt een cyberverzekering vergelijken met een brandverzekering. Ondanks blusinstallaties, sprinklers en brandwerend materiaal, blijft er altijd risico op een brand. Daarom hebben bedrijven met uitstekende brandpreventie alsnog een brandverzekering.

Ben ik als MKB-bedrijf een doelwit voor hackers?

Een hacker maakt geen onderscheid tussen grote en kleine bedrijven. Veel aanvallen, bijvoorbeeld de recente Petya-aanval, zijn geen doelgerichte aanvallen. Ze kunnen dus ieder bedrijf dat ermee in aanraking komt raken. Uiteraard is de premie wel afhankelijk van de omvang van uw bedrijf. Juist kleinere bedrijven worden vaak als target gezien door hackers, omdat hun veiligheidsmaatregelen over het algemeen minder uitgebreid zijn dan die van multinationals.

Is een cyberverzekering wel zinvol als gegevens niet op een eigen netwerk worden opgeslagen, maar op een externe server of in de cloud?

Ook wanneer u als onderneming gebruikmaakt van externe partijen, blijft u verantwoordelijk voor de data. Zelfs als een data-lek optreedt bij een externe server, rust er een aansprakelijkheidsrisico bij degene die de data bij de externe partij in beheer heeft gegeven. Een cyberverzekering blijft daarom aan te raden, ook als alle gegevens in de cloud staan opgeslagen.

Als zich een cyberincident heeft voorgedaan, voorziet de cyberverzekering dan alleen in een financiële tegemoetkoming?

Een cyberverzekering verzekert, naast de aansprakelijkheid van een onderneming voor door derden geleden schade plus de gevolgschade, ook de eigen kosten als gevolg van een cyberincident. Denk aan kosten voor herstel van het verloren gaan van gegevens door hacken of een systeeminbraak, diefstal van (privacygevoelige) gegevens, een menselijke fout of een technische misser. Kortom, er wordt meer gedekt dan alleen de kosten als gevolg van aanvallen van cybercriminelen. Ook bieden wij u met onze cyberverzekeringen een totaal 'ontzorg-concept'. Naast preventie helpt deze verzekering u om in geval van een incident snel en adequaat te reageren. U krijgt direct toegang tot een incident response team dat de technische, juridische en publicitaire gevolgen samen met u oppakt om de gevolgen voor uw bedrijf zoveel mogelijk te beperken. Vooral bij dit immateriële deel speelt de cyberverzekering een essentiële rol: wij zorgen voor verregaande 'ontzorging' van uw bedrijf door professionele begeleiding van experts.

Kan een bestuurder aansprakelijk worden gesteld wanneer het bedrijf geen cyberverzekering heeft?

Als bestuurder kunt u persoonlijk aansprakelijk worden gesteld als u uw cybersecurity niet op orde heeft, inclusief het verzekeren ervan.

Bedrijfsvoering is grotendeels digitaal en/of online, dus cyberproblemen bedreigen de continuïteit van een onderneming. Als bestuurder bent u wettelijk verplicht uw onderneming naar behoren te besturen. Behoorlijk bestuur geldt zeker ook voor cyber security.

Bestuurders moeten de volgende twee zaken kunnen aantonen:
- Is er voldoende geïnvesteerd in IT-veiligheid?
- Heeft er een verschuiving van de IT-afdeling naar bestuursniveau plaatsgevonden?

Ook is er van rechtswege bepaald dat er sprake kan zijn van bestuurdersaansprakelijkheid als - gezien aard van de bedrijfsvoering - de gebruikelijke en noodzakelijke verzekeringen niet zijn afgesloten. Het is meer dan logisch dat cyberverzekeringen vanaf nu (gaan) behoren tot die gebruikelijke en noodzakelijke verzekeringen. In de VS is de eerste bestuurder intussen al aansprakelijk gesteld voor het afsluiten van een te beperkte cyberverzekering.

Staat uw vraag er niet bij?

Vraagt u zich nog steeds af welke risico's uw organisatie loopt en wat er verzekerbaar is? Neem dan contact op met een van onze cyberspecialisten.

CONCORDIA DE KEIZER

Concordia de Keizer adviseert (middel) grote bedrijven, instellingen en (semi) overheden op het gebied van financiële dienstverlening en risicomanagement. Wij begeleiden onze opdrachtgevers bij het inschatten van potentiële risico's en adviseren optimale oplossingen om die risico's te beheersen. Dit doen wij met hoog gekwalificeerde, betrokken mensen, met hart voor uw zaak en passie voor het vak. Met maar één doel voor ogen: de continuïteit van uw business of dienstverlening waarborgen.
Wij ontzorgen onze opdrachtgevers op onder meer de volgende gebieden:
- Brand- en bedrijfsschade.
- Bedrijfs-, product-, beroeps- en bestuurders-aansprakelijkheid.
- Marine, logistiek en transport.
- Technische verzekeringen, CAR, machinebreuk- en bedrijfsschade.
- Employee benefits en collectieve pensioenen.
- Warranty indemnity, product tampering, product recall en extortion.
- Fraude, cybercrime, kidnap & ransom.
- Kredietverzekeringen.
- Captives en andere vormen van risk transfers.
- Europese aanbestedingen.

Annet Govaert-Proos
Sr. Product Specialist
Cyber & Aansprakelijkheid

› 010 – 251 12 46
› annet.govaert@concordiadekeizer.nl

CONCORDIA DE KEIZER
Lichtenauerlaan 202-220
3062 ME Rotterdam
Postbus 23403
3001 KK Rotterdam
010 251 12 51