Q&A: de meest gestelde vragen over de CyberClear by Hiscox verzekering

Vraagt u zich af waarom u een cybercrimeverzekering nodig heeft? Hieronder geeft HBR Branche Verzekeringen antwoord op de meest gestelde vragen.

- Mijn andere polis biedt al dekking hiervoor. Is dat niet voldoende?
  Mogelijk, maar meestal niet. In de meeste gevallen is de dekking zeer beperkt en wordt slechts een gering bedrag in euro's toegekend. Het kan bijvoorbeeld zijn dat alleen de Third Party-kosten worden vergoed, of dat de maximumdekking voor First Party-kosten beperkt is tot slechts € 50.000. Een complete verzekeringspolis bij inbreuken op privacy en het verlies van data is profijtelijk voor elk bedrijf en biedt de geruststelling dat de kosten van een potentiële inbreuk geen ontwrichtende werking zullen hebben op de bedrijfsvoering.

- Als mijn werkelijke risico alleen First Party-gegevens betreft (zoals gegevens van werknemers), heb ik dan zo'n polis wel nodig?
  Elk bedrijf heeft de taak en verplichting om namens werknemers beheerde gegevens te beschermen. Hetzelfde geldt voor vertrouwelijke gegevens van het bedrijf zelf. Geen enkel bedrijf is immuun tegen cyberaanvallen. Een polis van Hiscox biedt dekking voor het verlies van werknemersgegevens en andere bedrijfsgerelateerde data en persoonsgegevens.

- Ik ben geen doelwit zoals Sony, KPN of ASML. Waarom zou ik me zorgen maken?
  Grote bedrijven halen het nieuws. Kleine niet. Als het gaat om inbreuken op gegevens is het niet de vraag of het gebeurt, maar wanneer het gebeurt. Er bestaat een zwarte markt waar gestolen gegevens worden gekocht en verkocht, en hackers worden steeds slimmer. KPN, Sony, ASML en andere grote organisaties hebben complete ICT- en Risk afdelingen die zich bezighouden met het analyseren van de risico's waaraan het bedrijf wordt blootgesteld en die meewerken aan het opzetten van beleid en procedures waarmee ze zichzelf kunnen beschermen, maar hackers weten nog steeds gaten in de verdediging te slaan. Kleinere bedrijven die geen netwerkbeveiligers in dienst hebben en niet de middelen hebben om hun gegevens te beschermen, zijn voor hackers een gemakkelijke prooi.

- Wie sluit tegen cyberrisico's een dekking af?
  Bedrijven die zich bewust zijn van de risico's die er zijn en uit voorzorg maatregelen treffen om dit risico te beperken. Het wordt al een 'must have'-dekking genoemd vanwege de toegenomen cybercriminaliteit.

- Waarom zou ik twijfelen aan mijn IT-afdeling als ze zeggen dat ze al hun zaakjes op orde hebben?
  Veel grote of kleine bedrijven hebben complete afdelingen, of huren ICT-expertise in, die zich bezighouden met IT-beveiliging, maar ze bleken kwetsbaarder dan ze dachten. Eén simpele fout of vergissing, zoals het niet updaten van software, het niet instellen van de juiste procedures voor authenticatie van leveranciers, het kwijtraken van een niet-versleutelde laptop waarop gevoelige gegevens zijn opgeslagen, of een medewerker met kwaad in de zin, kan leiden tot een inbreuk. De risico's groeien mee met de technologische ontwikkelingen en hackers gaat steeds slimmer en geraffineerder te werk. Bedrijven kunnen nooit 100% hack-proof zijn. Daarnaast zijn de eigen medewerkers nog wel eens de oorzaak van het binnenhalen van een computervirus.

- Heb ik deze dekking wel nodig als ik gegevens van klanten niet opsla op mijn netwerk?
  Ja, u slaat klantgegevens weliswaar niet op, maar u hebt er wel toegang tot. U kunt zelf de oorzaak zijn van een inbreuk op gegevens van uw klanten en zo contractbreuk veroorzaken. Bedrijfsinformatie valt eveneens onder de dekking van een polis tegen inbreuk op gegevens en privacy. Aansprakelijkheid bestaat ook voor gegevens van werknemers.

- Ik heb maar een heel klein bedrijf. Loop ik dan nog steeds enig risico van inbreuk op gegevens?
  Elk bedrijf is blootgesteld aan privacyrisico's, hetzij via gevoelige gegevens van werknemers, hetzij via betalingen die van derden worden geïnd, geleverde diensten enz. Sommige risico's zijn groter dan andere maar het is belangrijk om te benadrukken dat elk bedrijf met werknemers in dienst aansprakelijk is voor verlies van Third Party-gegevens (met inbegrip van gegevens van werknemers). Een inbreuk kost het kleinste bedrijf met de geringste risico's gemiddeld € 188.000. De kosten stapelen zich razendsnel op.

- De verwerking van betaalkaarttransacties besteed ik uit aan een derde. Op dat gebied loop ik dus geen risico, klopt dat?
  Volgens de PCI Compliance Guide, geldt de PCI-standaard voor ALLE organisaties of handelaren, ongeacht de omvang van of het aantal transacties, die gegevens van kaarthouders accepteren, doorgeven of opslaan. En het simpele feit van uitbesteding aan een derde partij ontslaat u niet van de plicht te voldoen aan de PCI-voorschriften. Misschien kunt u zo het risico verminderen en daarmee de PCI-compliance wat vergemakkelijken, maar dat betekent nog niet dat er volledig aan PCI voorbij kan worden gegaan.

- Als mijn klantgegevens zijn opgeslagen in de cloud berust de aansprakelijkheid toch bij de cloudaanbieder?
  Dat is niet zeker. Het is in het belang van de verzekerde om contracten op dit gebied zorgvuldig door te spreken met een juridisch adviseur. Zelfs als het risico beperkt is, kan het nog steeds dat de aansprakelijkheid bij de verzekerde wordt gelegd.

- Welke soorten data vormen een risico?
  De risico's betreffen in het algemeen de persoonsgegevens die bedrijven onder beheer hebben, zoals BSN-nummers, rijbewijsnummers, gegevens van betaalkaarten waarmee goederen, diensten en rekeningen worden betaald, gevoelige gegevens van klanten, verzamelde medische gegevens, enzovoort.

- Wat is een record precies?
  Niet-openbare persoonsgegevens zoals bepaald in nationale, regionale, plaatselijke of buitenlandse wet- of regelgeving kunnen bestaan uit, maar zijn niet beperkt tot, onbeveiligde vertrouwelijke gezondheidsinformatie, BSN-nummers, persoonsgebonden belastingidentificatienummers, rijbewijsnummers, nummers van een identiteitskaart of paspoort, bankrekeningnummers en nummers van betaalpassen of creditcards. Wat wij willen weten is het aantal afzonderlijke gegevenselementen (records) die een verzekerde in totaal bezit. Indien meerdere gegevenselementen van dezelfde persoon zijn opgeslagen in het netwerk van de verzekerde of op locatie bij de verzekerde, willen wij informatie hebben over de ter plekke gehanteerde bewaar- en duplicatieprocedures.

- Heeft de privacyverklaring gevolgen voor websites?
  Ja, want de privacyverklaring is in veel opzichten te beschouwen als een overeenkomst met uw klanten. Belangrijker nog, als u uw gegevensbeschermingsprocedures geheim wilt houden en niet wilt vertellen met wie u gegevens van anderen deelt, kan dat in strijd zijn met privacyregelgeving.

- Aan welke wet- en regelgeving zijn bedrijven in het algemeen onderworpen?
  Voor gegevens van betaalkaarten de PCI/ DSS-regels. Deze gegevens zijn samen met BSN-nummers, financiële en medische gegevens enz. ook onderworpen aan nationale, regionale en lokale wet- en regelgeving. Bijvoorbeeld de AVG (Algemene Verordening Gegevensbescherming)

- Wat gebeurt er als ik de PCI-regels niet naleef?
  Iemand die zich niet houdt aan de PCI-regels kan een boete krijgen van kaartuitgevers en voor de rechter worden gedaagd door diverse partijen die opkomen voor boze consumenten die slachtoffer zijn van inbreuken op hun gegevens.

- Mijn Point-of-Sale-leverancier zegt dat hij PCI-compliant is. Dat betekent dat ik ook compliant ben, klopt dat?
  Niet per se, de meeste handelaren zijn blootgesteld aan enig risico. De enige manier om volledig te ontkomen aan de noodzaak om PCI-compliant te worden, is door uitbesteding van het gehele betalingsverwerkingsproces. In de meeste gevallen wordt bij de verwerking een beroep gedaan op in ieder geval een deel van uw netwerkinfrastructuur. Dit betekent dat ook handelaren onderworpen zijn aan de PCI-standaard.

- Wat is het verschil tussen een boete en een assessment van de PCI?
  Uitgevers van betaalkaarten (Visa, Mastercard enz.) kunnen naar eigen goeddunken boetes opleggen die variëren van € 5.000 tot € 100.000 per maand voor overtreding van de PCI-voorschriften. De boetes hebben een punitief doel en hebben geen betrekking op schadevergoeding aan banken door fraude met betaalkaarten. PCI-assessments gaan gepaard met aansprakelijkheden en kosten die zijn uitgewerkt in een overeenkomst inzake diensten van handelaren of inzake betalingsverwerking. Dergelijke overeenkomsten kunnen bepalingen bevatten inzake kosten voor uitgifte van nieuwe passen en van frauduleuze debiteringen na een inbreuk.

- Wat zijn de gemiddelde kosten van een gegevensinbreuk?
  Het gemiddelde schadebedrag van een cybercrime situatie in Nederland is € 340.500. Hoe groter het bedrijf, des te hoger de kosten. Maar ongeacht de grootte van het bedrijf geldt wederom: hoe meer gevoelige gegevens het bedrijf verzamelt, des te hoger de kosten.

- Wat is het verschil tussen First Party- en Third Partydekking?
  Met een First Party-verzekering dekt de verzekerde zijn eigen schade als gevolg van kennisgeving aan gedupeerden, digitaal forensisch onderzoek om na te gaan hoe de inbreuk heeft kunnen plaatsvinden, herstel en bedrijfsstagnatie. Met een Third Party-verzekering dekt de verzekerde de kosten als gevolg van aansprakelijkheid collectieve rechtszaken en andere aanspraken die door externe partijen worden ingesteld.

- Wat zijn vertrouwelijke bedrijfsgegevens als handelsgeheimen buiten beschouwing worden gelaten?
  In dat geval hebben vertrouwelijke bedrijfsgegevens betrekking op informatie waarvan openbaarmaking schade zou toebrengen aan het bedrijf. De informatie kan bestaan uit verkoop- en marketingplannen, productplannen, documenten over ontwerpen en uitvindingen, gegevens over klanten en toeleveranciers, financiële gegevens enz. die naar hun aard niet openbaar zijn.

- Aan welke limieten moet ik denken?
  Dat hangt af van de grootte van het bedrijf en van het risico. De limieten stijgen navenant mee met de grootte van het bedrijf en de gevoeligheid van de gegevens.

- Wat houdt 'dekking per persoon' in?
  In plaats van een waarde in euro's te bepalen voor meldings- en fraudecontrolekosten stelt de verzekeraar het maximumaantal personen vast die tegen deze schade zijn gedekt (geen vastgesteld eurobedrag).

- Dekt een cyberverzekeringspolis het rechtstreeks verlies van gelden?
  De meeste cyberverzekeringspolissen zijn bedoeld om de schade door verlies van data, niet van gelden (rechtstreeks) te dekken. Bij Hiscox kunnen we voor bepaalde risico's de dekking uitbreiden. Onze polis tegen cybercriminaliteit biedt dekking tegen inbreuken op gegevens, bijvoorbeeld bankgegevens die worden gestolen om rekeningen van bedrijven of instellingen te plunderen.

- Biedt de polis dekking tegen 'social engineering'?
  Social engineering is een methode om personen door misleiding beveiligde gegevens afhandig te maken. Slachtoffers van social engineering zijn kwetsbaar door hun ingeboren aard om anderen te vertrouwen en te willen helpen. De meeste verzekeringspolissen dekken verlies van gegevens ongeacht hoe het verlies tot stand is gekomen, al moet wel goed worden gekeken wat hier precies over in de polis staat.

- Dekt de polis ook gegevensverlies veroorzaakt door malafide medewerkers?
  De meeste verzekeringspolissen dekken de kosten van gegevensverlies ongeacht de wijze waarop het verlies zijn beslag heeft gekregen. Er zijn echter ook polissen die gegevensinbreuken veroorzaakt door malafide medewerkers uitsluiten. De dekking van de verzekeringspolissen van Hiscox tegen standaardinbreuken op gegevens door malafide medewerkers is overeenkomstig de voorwaarden van de polis, maar bepaalde situaties waarbij leidinggevend personeel van de organisatie betrokken is, kunnen in de polis zijn uitgesloten.

- Zijn ook gegevens op papier gedekt?
  In bijna alle polissen op dit gebied zijn papieren gegevens meeverzekerd, maar het is zaak de polis hier altijd even op na te slaan. De polis van Hiscox voor privacybescherming definieert persoonsgegevens als gegevens in welke vorm dan ook die onder uw zorg, beheer en toezicht staan, of die onder zorg, beheer en toezicht staan van derden voor wie u volgens de wet aansprakelijk bent. Een inbreuk op papieren gegevens zou vallen onder de standaardbepalingen van de Hiscox-polis.

- Is er wereldwijde dekking?
  Wij bieden wereldwijde dekking maar onze jurisdictie bij claims afhandeling beperkt zich tot het juridisch rechtsgebied zoals vermeld op de polis.

- Wat zijn uw diensten met toegevoegde waarde?
  Wij hebben directe toegang tot vooraanstaande partners en de eRisk Hub. Hun diensten zijn voor onze verzekerden gratis beschikbaar. Onze partners leveren op het gebied van risicobeheersing uitgebreide maatregelen, procedures, instructies en andere tools voor verzekerden om inbreuken te voorkomen. Daarnaast wordt voorzien in onlinemateriaal op het gebied van compliance, e-mailupdates, procedures en voorbeeldformulieren, training van medewerkers, responsplannen in geval van gegevensinbreuken en volledige telefonische ondersteuning. eRisk Hub®, mede mogelijk gemaakt door NetDiligence®, stelt tools en middelen beschikbaar om onze verzekerden te helpen inzicht te krijgen in de risico's, een responsplan op te stellen en de organisatorische gevolgen van een gegevensinbreuk op de organisatie zoveel mogelijk te beperken. In dat kader wordt ook een inbreukadviseur en een responsteam beschikbaar gesteld.