De impact van cybercrime op een **Legal Counsel**

Hoe maakt u als Legal Counsel het verschil bij de bescherming tegen cyber?

- Cyber vormt grootste bedreiging voor bedrijven
- Wat gebeurt er als uw organisatie zelf getroffen wordt?
- Organisaties erkennen het probleem, maar ondernemen te weinig actie
- Cyber raakt iedereen, niet alleen IT
- De rol van een Legal Counsel bij de beheersing van cyberrisico's
- Aanpak van cyberrisico's is geen eenmalige exercitie

Leestijd 6 -10 MIN

AON
Empower Results®

Top 10 belangrijkste risico's

volgens Nederlandse bedrijven en organisaties

Aon's 2019 Global Risk Management Survey geeft inzicht in de belangrijkste risico's voor organisaties en bedrijven in Nederland. De top 10 risico's die genoemd werden, zijn:

1. **Bedrijfsonderbreking**
2. **Reputatieschade (merk)**
3. **Cyberaanvallen / dataverlies**
4. **Economische teruggang / langzaam herstel**
5. **Niet kunnen aantrekken of behouden van toptalent**
6. **Commodityprijzen**
7. **Cash flow / Liquiditeit**
8. **Niet kunnen leveren of voldoen aan de behoefte van de klant**
9. **Snel veranderende marktfactoren**
10. **Problemen met distributie / supply chain**

AON
Empower Results®

Cyber vormt **grootste bedreiging** voor bedrijven

Uit de resultaten van het Global Risk Management Survey blijkt dat **bedrijfsonderbreking**, **reputatieschade** en **cyberaanvallen/ datalekken** als de grootste risico's worden beschouwd.
Deze top 3 bestaat uit risico's die sterk verbonden zijn met de dynamische en turbulente wereld waarin we tegenwoordig leven. Het zijn risico's die lastig te beheersen en te verzekeren zijn.
Ze zijn bovendien allemaal gerelateerd aan cyber.

De totale financiële schade van een cyberincident of datalek bedroeg gemiddeld **€5 miljoen**.

Kijk bijvoorbeeld naar de actuele ontwikkelingen: door de uitbraak van het coronavirus gaan medewerkers massaal thuiswerken. Omdat bij veel bedrijven de thuiswerkvoorzieningen niet optimaal zijn, schakelen zij snel over op (nieuwe) third party suppliers. Maar wat betekent dit voor de veiligheid van uw data en voor die van klanten of andere partijen? Zeker wanneer in crisissituaties snelle beslissingen moeten worden genomen, is het belangrijk dat u als Legal Counsel scherp naar de gemaakte afspraken kijkt om verstrekkende gevolgen te voorkomen.

Cyberrisico's hebben een grote impact op bedrijven door het verstorende effect op de essentiële bedrijfsprocessen. Daarnaast kunnen de financiële gevolgen groot zijn. In 2019 deed het Ponemon Institute in opdracht van Aon onderzoek, waaruit bleek dat 41 procent van de ondervraagde organisaties in de laatste 24 maanden een cyberincident of datalek had meegemaakt. De totale financiële schade van dergelijke incidenten bedroeg gemiddeld €5 miljoen. Met schades van die omvang komt voor veel bedrijven zelfs het voortbestaan in gevaar.

AON
Empower Results®

Wat gebeurt er als **uw organisatie** zelf **getroffen** wordt?

Bij een ingrijpend cyberincident is het meteen alle hens aan dek. De vragen “Wie doet wat?” en vooral “Wie neemt de beslissingen?” zouden al beantwoord moeten zijn voordat het incident plaatsvindt. Je stelt immers ook niet het basiselftal samen op de dag dat Nederland de eerste voetbalwedstrijd in het EK speelt.

Voorbereiding en voorzorgsmaatregelen zijn van groot belang. Denk bijvoorbeeld aan wat er gebeurde bij de Universiteit Maastricht. Hackers blokkeerden met ransomware de toegang tot bepaalde servers. Alle activiteiten binnen de universiteit kwamen vanaf dat moment twee weken stil te liggen. Bedrijven en organisaties moeten zich dus afvragen wat de consequenties zijn indien hun dagelijkse processen geen doorgang kunnen vinden door een dergelijk incident.

“Naast de acute vragen over de rolverdeling en de eventuele hulptroepen van het crisisteam, dient een bedrijf vooraf na te denken over het antwoord op de vragen: **“Wat kunnen we nog wel doen? Hoeveel kost dit per dag? Hoe lang houdt het bedrijf dit vol? Is er een back-upplan?”**

Bij financiële schade door cyberincidenten denken we in eerste instantie aan de kosten van het herstellen van de systemen, het betalen van ransomware of administratieve boetes, bijvoorbeeld van de Autoriteit Persoonsgegevens in verband met een datalek. Maar de **schade door bedrijfsstilstand vanwege een cyberincident** kan nog vele malen hoger uitvallen.

AON
Empower Results®

Organisaties **erkennen het probleem,** maar **ondernemen te weinig actie**

In de praktijk merken we dat veel mensen de mogelijke impact van een cyberincident wel erkennen, maar dat zij toch lang niet altijd de urgentie voelen om direct passende maatregelen te nemen. Marie-Louise: "Veel bedrijven en organisaties denken dat het zo'n vaart niet zal lopen, terwijl de kans op een cyberincident minstens even groot is als de kans op brand. Bedrijven investeren veel meer in preventie en verzekering van het brandrisico dan van het cyberrisico."

Volgens het Ponemon rapport wordt **59 procent van alle materiële activa** (zoals gebouwen, apparatuur en voertuigen) verzekerd, terwijl **slechts 18 procent van alle immateriële activa** (zoals data, strategische bedrijfsinformatie, merk) verzekerd is. Dit is vooral opvallend omdat er een duidelijke trend zichtbaar is waarin de totale waarde van onze immateriële activa die van de materiële activa overstijgt.

Marie-Louise de Smit

Marie-Louise de Smit is Cyber Deals Director bij Aon Risk Solutions. Zij was eerder zelf Legal Counsel binnen de IT-sector en daarvóór als advocaat gespecialiseerd in commerciële contracten. In haar huidige rol adviseert zij organisaties over de impact van cyberrisico's en hoe die beperkt kan worden. In dit document geeft zij haar visie op de steeds belangrijkere rol van de Legal Counsel bij de beheersing van cyberrisico's.

AON
Empower Results®

Cyber raakt iedereen, niet alleen IT

Het is tegenwoordig niet meer de vraag of u te maken krijgt met een cyberincident, maar wanneer. En op het moment dat het gebeurt is de impact op uw organisatie mogelijk zeer groot. Het is daarom opmerkelijk dat niet meer organisaties passende maatregelen nemen om dit risico te voorkomen, beperken of verzekeren.

Hoe komt dit?

Marie-Louise: ''Cybersecurity wordt vaak gezien als een zaak voor de afdeling IT. Wanneer we bedrijven vragen naar hun cyberrisicomanagement, krijgen we soms het antwoord: 'Onze IT-leverancier heeft dat goed op orde'. Helaas kan ook de IT-afdeling niet garanderen dat de organisatie niet geraakt wordt door een cyberincident. Daar komt bij dat cyber verder gaat dan de technische kant. Iedereen zou doordrongen moeten zijn van de impact van een datalek of cyberincident. Verantwoord omgaan met cyberrisico's heeft te maken met allerlei disciplines binnen de organisatie, zoals cultuur, gedrag en ook met juridische aspecten.''

De **rol van een Legal Counsel** bij de beheersing van cyberrisico's

Hoe gaat u om met privacygevoelige gegevens, verwerkersovereenkomsten, autorisaties en het wachtwoordbeleid?

Helder beleid

Door een helder beleid op te stellen zorgt u ervoor dat u risico's en aansprakelijkheden zoveel mogelijk beperkt en dat relevante wetgeving, zoals de Algemene Verordening Gegevensbescherming (AVG) en de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni), door iedereen binnen het bedrijf wordt nageleefd. Daarnaast worden deze risico's gemitigeerd door het hanteren van algemene voorwaarden en door uw contractbeleid. Klanten en leveranciers eisen ook steeds vaker dat bedrijven en organisaties verzekerd zijn tegen cyberrisico's, zoals verlies van gegevens en eventuele boetes die voortvloeien uit de AVG. Als Legal Counsel ziet u dit soort bepalingen vaak als eerst. Het is belangrijk om te kunnen beoordelen of deze eisen terecht zijn en of uw bedrijf eraan kan voldoen.

Voorkomen en beperken

Bij 50% van de ondervraagde Nederlandse bedrijven is de afdeling Legal betrokken bij besluitvorming over risicomanagement, zo blijkt uit het Global Risk Management Survey. Maar het cyberrisico is voor veel Legal Counsels nog onbekend terrein. De kans is echter zeer reëel dat u er in de toekomst steeds meer mee te maken krijgt. Hoe zorgt u ervoor dat de kans op schade door cyber zo laag mogelijk blijft? Het is essentieel dat u als Legal Counsel betrokken blijft bij wat er speelt binnen uw organisatie. Uw toegevoegde waarde op het gebied van cybersecurity ligt vooral in het voorkomen en beperken van mogelijke schade en claims.

AON
Empower Results®

Aanpak van cyberrisico's is **geen eenmalige exercitie**

We zullen de komende decennia moeten leren leven met het feit dat cyberrisico's altijd en overal om ons heen aanwezig zijn en impact hebben op ons leven. Het is de vraag hoe bedrijven en organisaties hiermee omgaan. Omdat cyberrisico's zich blijven ontwikkelen, kan de aanpak ervan in de visie van Aon geen eenmalige exercitie zijn. Het is nooit af, maar een continu proces.

Wanneer een bedrijf zich goed wil voorbereiden op cyberrisico's is het belangrijk om volgens een cyclisch stappenplan te werk te gaan.
Vaste onderdelen van de werkwijze zouden moeten zijn:

- **Assessment**; inventariseren van de cyberrisico's, zoals het checken van contracten op cyberbepalingen.
- **Kwantificeren**; in kaart brengen van de (financiële) impact van eventuele incidenten.
- **Verzekeren**; bepalen welke risico's u wilt afdekken met een specifieke cyberverzekering.
- **Incident Response Readiness**; voorbereiden op incidenten door het vastleggen van de verantwoordelijkheden bij een cybercrisis, het oefenen met scenario's, etc.

Zelf aan de slag met Cyber?

Heeft u vragen over cyberrisico's en hoe u hier als Legal Counsel mee aan de slag kunt? Laat het ons weten. De cyberspecialisten van Aon helpen u graag verder met advies op maat in elke fase van de aanpak van cyberrisico's.

Marie-Louise de Smit

+31 629167547

marie-louise.de.smit@aon.nl

Wat zijn de stappen om inzicht te krijgen in uw cyberrsisico's?

Dit stappenplen helpt bedrijven cyberrisico's structureel aan te pakken en te beheersen.

Aon

Empower Results®