De rol van de **risicomanager** bij een **circulaire aanpak** van cyberrisico's

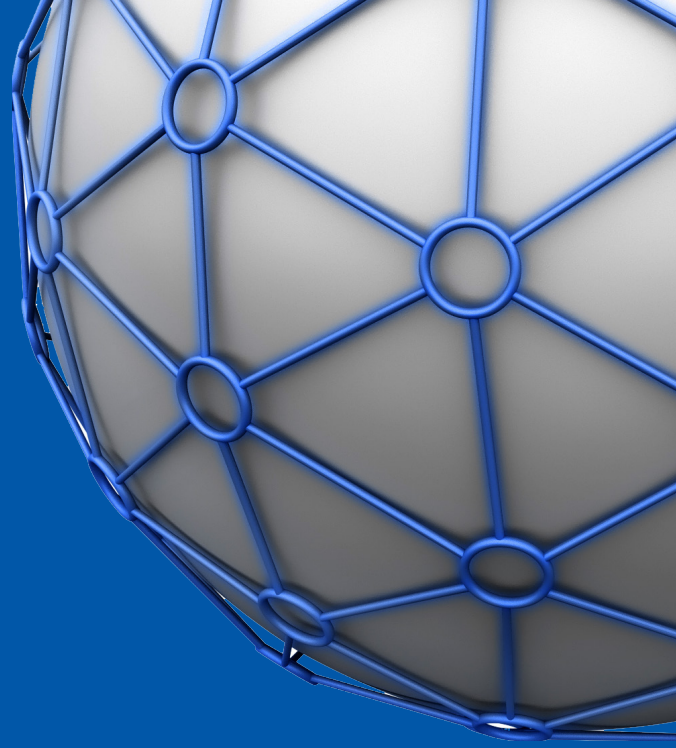
Onze experts over:

- Waar start en eindigt goed cyberrisicomanagement?
- De kwetsbaarheden en grootste cyberrisico's voor uw organisatie
- De vier entry points van de cyberloop

Leestijd 6 -10 MIN

AON
Empower Results®

De **cruciale rol** van **goed cyberrisicomanagement**



Cyberweerbaarheid staat bij Nederlandse directies hoog op de agenda. Ze zien de noodzaak van goed cyberrisicomanagement en zijn bereid tijd en geld te investeren om hun organisatie weerbaar te maken. Dit wordt versterkt door het toenemende aantal cyberincidenten in het eerste kwartaal van 2020.

Non-stop op de hoogte zijn en blijven

Organisaties hebben hun processen gedigitaliseerd, werknemers werken op afstand, er wordt een Bring Your Own Device-beleid gehanteerd en de wetgeving is uitgebreid. In reactie hierop stroomt de markt over van technologieën en operationele checklists die organisaties moeten helpen bij het beveiligen tegen cyberincidenten en hen begeleiden door het cyberrisico-landschap. Maar cyberweerbaarheid wordt niet alleen bereikt met technologie, governance of compliance.

Het bereiken van cyberweerbaarheid start bij het non-stop op de hoogte zijn en leren van de ontwikkelingen in het continu evoluerende cyberrisico-landschap en binnen de organisatie. En hier ook steeds op kunnen anticiperen. Waarom? Omdat er niet één universele of lineaire benadering is van cyberweerbaarheid in deze sterk veranderende wereld.

Leer continue

Organisaties moeten voortdurend data verzamelen en analyseren die een rol kunnen spelen bij cyberbedreigingen. En juist ook op directieniveau moet de kennis aanwezig zijn van de processen rond activa, kwetsbaarheden, balance sheet exposure en de mogelijkheden om cyberrisico's te verzekeren of beheersen. Het belangrijkste is dat organisaties snel kunnen reageren en leren wanneer een aanval plaatsvindt.

Waar start en eindigt goed cyberrisicomanagement?

We zien dat, mede gezien het groeiend besef en inzicht bij organisaties, de vraag naar goed (cyber)risicomanagement en verzekeringsoplossingen flink toeneemt. Zeker als organisaties zelf voor het eerst geconfronteerd worden met de diverse impact van een cyberincident. Denk dan niet alleen aan bedrijfsonderbreking en IT-kosten, maar ook juridische consequenties, claims van klanten en reputatieschade. Maar waar start en eindigt goed cyberrisicomanagement en waar 'stapt een organisatie in'? En waar en hoe levert de risicomanager zijn of haar meerwaarde?

AON
Empower Results®

Cyber is een **miljoenenindustrie** voor **criminelen**

Op 19 maart van vorig jaar werd de Noorse aluminiumproducent Hydro getroffen door ransomware. De schade bedroeg tussen EUR 57 en 67 miljoen en dat betrof 'slechts' de (direct meetbare) schade in de eerste helft van dit jaar. Alleen al in de eerste week na de 'besmetting' bedroeg de schade meer dan EUR 40 miljoen.

Deze ransomware is vermoedelijk via de mail gedistribueerd naar diverse werkplekken en locaties in de vijftig landen waarin het bedrijf is gevestigd. De ransomware kon zoveel schade aanrichten omdat het Noorse bedrijf moeite had om de bedrijfsvoering in Europa en Noord-Amerika te herstellen. Ook locaties van de Franse technologieconsultant Altran en zinkbedrijf Nyrstar werden dat jaar getroffen door een cyberaanval waardoor de organisaties zich genoodzaakt zagen om systemen uit te schakelen.

Hoewel Hydro aangaf een cyberverzekering te hebben die bedrijfsonderbrekingen dekt, blijft de impact gigantisch. Effectief te kunnen reageren om de impact te minimaliseren is noodzakelijk. Cyberincidenten veroorzaken niet alleen financieële schade.

AON
Empower Results®

Grote organisaties een geliefd doelwit

Alle organisaties waar direct of indirect geld te halen is, zijn een potentieel doelwit van cybercriminelen. Grote organisaties zijn sterk afhankelijkheid van informatietechnologie, internationale connectiviteit en geautomatiseerde processen. Omdat zij hiervoor specialisten in dienst hebben, is het beveiligingsniveau over het algemeen hoog. Toch zijn deze organisaties voor criminelen zeer interessant, omdat hier voor hen veel geld te verdienen is. Dit kan door diefstal van vertrouwelijke informatie, die criminelen doorverkopen aan derden of aan de getroffen organisatie aanbieden voor een 'ransom', maar ook door het op slot zetten van systemen. Een grote organisatie kan ook interessant zijn vanuit het perspectief van concurrentie, internationale strategische positie of politiek activisme.

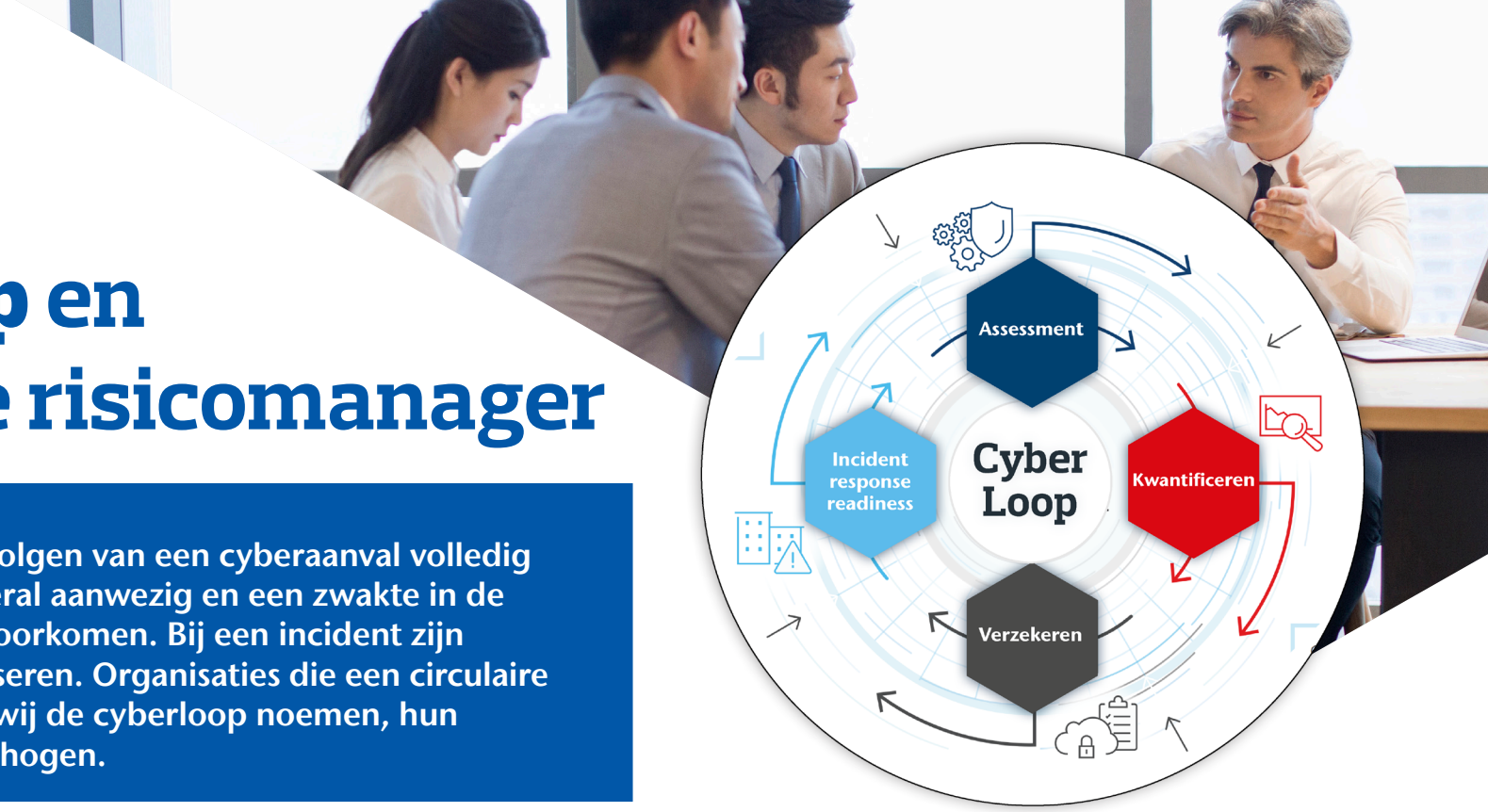
Wat bepaalt het cyberrisicoprofiel van uw organisatie?

Een cyberincident valt nooit 100% te voorkomen, maar waarom zou u het cybercriminelen makkelijker maken dan nodig? Zodra u weet via welke deuren een 'inbreker' binnen kan komen, heeft u de eerste stap naar een goede beveiliging gezet. De volgende stap is zorgen dat deze deuren zo goed mogelijk gesloten zijn.

Talrijke factoren dragen bij aan het cyberrisicoprofiel van een organisatie, waaronder:

- **handelen van werknemers;**
- **systeem- en programmafouten;**
- **beveiligingsmaatregelen;**
- **de aard van en hoeveelheid data;**
- **politieke of strategische waarde;**
- **afhankelijkheid van technologie.**

AON
Empower Results®



De cyberloop en de rol van de risicomanager

Het is onmogelijk om de gevolgen van een cyberaanval volledig uit te roeien. Het risico is overal aanwezig en een zwakte in de beveiliging is niet 100% te voorkomen. Bij een incident zijn de gevolgen wel te minimaliseren. Organisaties die een circulaire benadering overwegen, die wij de cyberloop noemen, hun weerbaarheid aanzienlijk verhogen.

Een ecosysteem voor cyberweerbaarheid

De cyberloop stelt dat elke organisatie haar reis steeds op een van de vier entry points start: assessment, kwantificering, verzekering of incident response readiness. Eenmaal in de cyberloop worden de betrokken collega's van de verschillende disciplines actieve deelnemers aan het risicomanagement. Zo wordt de cyberloop een ecosysteem voor cyberweerbaarheid, continu bezig met evaluatie, verbeteringen en investeringen in cyberrisicobeheer.

Schat aan data in één ecosysteem

In de cyberloop wordt een schat aan data verzameld: assessmentresultaten, kwantificeringstudies, schade , statistieken, peer-benchmarking, claims, threat intelligence en ervaring verkregen door incidentrespons uit de praktijk. Alles wordt samengebracht in één data-ecosysteem. Met elke omloop van deze cyberloop worden meer data verzameld en vervolgens opnieuw in de loop gebruikt. Dit resulteert in inzichten die gebruikt worden om richting te geven aan het verbeteren van de weerbaarheid van de organisatie.

Sneller detecteren, reageren en herstellen

Terwijl een organisatie de cyberloop doorloopt, versterkt het haar vermogen om een cyberaanval snel te detecteren, erop te reageren en ervan te herstellen. De mogelijkheid om geïnformeerde beslissingen te nemen, wordt scherper en efficiënter en de weerbaarheid verbetert. Een organisatie die gebruik maakt van de cyberloop is niet langer passief maar heeft een denkvermogen dat continu wordt 'gevoed' door data en ervaringen. Zo kan zij actief reageren op (mogelijke) dreigingen.

AON
Empower Results®

Assessment

Om cyberrisico's te kunnen managen, is een goed assessmenttraject van belang. Een organisatie die het belang ziet van goed cyberrisicomanagement, is bereid om te beginnen met enkele moeilijke vragen te beantwoorden:

- Wat zijn de belangrijkste activa die we moeten beschermen en de meest waarschijnlijke bedreigingen waarmee we worden geconfronteerd?
- Hoe brengen we organisatiedoelen in evenwicht met cyberrisico's?
- Hoe staat het met onze beveiliging en controles?
- Hoe gebruiken onze mensen onze technologie en data?
- Hoe goed begrijpen onze mensen bestaand beleid en procedures, leven ze deze na en zijn deze bruikbaar in de dagelijkse praktijk?
- Kunnen we aan aandeelhouders, toezichthouders en rechtspersonen laten zien dat we due diligence hebben uitgevoerd om onze cyberweerbaarheid veilig te stellen?
- Hoe goed communiceren we intern met betrekking tot cyberrisico's, mitigatieactiviteiten en cyberincidenten en respons?
- Heeft het management eenzelfde beeld van wat cyber is en wat cyberweerbaarheid is?
- Waar moet ons budget aan worden besteed?

AON
Empower Results®

Maarten de Jonge:
"Een goed cyber assessment geeft de risicomanager, behalve inzicht, de handvatten om onderbouwd maatregelen af te kunnen stemmen met andere disciplines."

Assessment

Inzichten en data verzamelen

Tijdens een assessment worden inzichten en data verzameld en geanalyseerd binnen het ecosysteem van de cyberloop. Kritieke activa, systemen en operaties worden geïdentificeerd. Beleid en procedures worden geëvalueerd. Gebruikersgedrag bevestigd. Kwetsbaarheden worden gediagnosticeerd en prioriteit gegeven, cyberbeveiligingscontroles worden vergeleken met specifieke bedreigingen en governance en responsbereidheid worden beoordeeld. Na een goed assessment weet u wat u al geregeld heeft en welk onderdeel nog aandacht behoeft.

Gewapend met dit inzicht, kunnen de juiste beslissingen worden genomen en het cyberrisico van de organisatie strategisch worden beheerd via een combinatie van vier paden: risico vermijden, risico beperken, risico accepteren en het risico overdragen.

Bedreigingen, organisatiedoelen en risicobereidheid

De resultaten van het assessment maken het mogelijk om strategische beslissingen te nemen in de context van de cultuur van de organisatie en haar risicotolerantie. Maatregelen worden zo goed afgestemd op bedreigingen, organisatiedoelen en de risicobereidheid van een organisatie wordt beter begrepen.

Een assessment geeft de risicomanager de informatie en het overzicht om andere disciplines, zoals IT, beveiliging, de directie, audit, juridisch zaken en HR te informeren en maatregelen voor te stellen. Deze nieuwe samenwerking, gebaseerd op inzicht en feiten, zorgt voor een organisatiebrede benadering om beslissingen te nemen en zo de cyberweerbaarheid te maximaliseren.

De strategische roadmap

Deze gezamenlijke aanpak, de strategische roadmap, is voor elke organisatie uniek. Het stelt een organisatie in staat om onmiddellijk te handelen binnen een kader en hier tegelijkertijd van te leren om daarmee weer beter voorbereid te zijn op de volgende aanval.

Kwantificatie

Als er iets misgaat en uw organisatie wordt slachtoffer van een cyberincident, kan dit leiden tot zulke grote operationele, financiële en reputatieschade dat deze het voortbestaan van de organisatie kunnen bedreigen. De rol van de risicomanager is om een duidelijk inzicht te geven in deze grote potentiële verliezen. Zonder dit inzicht, onderbouwd met harde financiële cijfers, tast men voor de keuze van cyberrisico-investeringen vaak in het donker.

Maarten de Jonge:
"Juist omdat we soms nog onvoldoende historische data hebben, is het uitvoeren van een impactanalyse voorafgaand aan het afsluiten van een cyberverzekering zo belangrijk."

Cyber heeft een beperkt data-verleden

Het vaststellen van dekkingslimieten voor de al honderden jaren bestaande brandverzekering, gebeurt met risicotechnieken die gebruik maken van tientallen jaren van ervaring en data. Deze vanzelfsprekendheid geldt (nog) niet voor het bepalen van de juiste cyberbescherming en -verzekering. Toch moet de risicomanager een zo goed mogelijk inzicht geven in de financiële blootstelling bij een cyberdreiging. Alleen dan kan een organisatie de juiste keuze maken voor het managen van dit risico.

Bedrijfsspecifieke scenario's voor commerciële impact

Kwantificering van het cyberrisico is van cruciaal belang. Bij een kwantificatiestudie worden bedrijfsspecifieke scenario's gebruikt om de impact van verschillende cyberincidenten te begrijpen. Deze scenario's vormen de input voor de financiële modellen die gebruikt worden om de financiële impact te bepalen. Deze impact is de basis voor de roadmap voor investeringen in de cyberweerbaarheid, welke financiële gevolgen de organisatie zelf wil en kan dragen én welke zij wil en kan verzekeren.

Kwantificatie stelt de risicomanager in staat om de effectiviteit te meten van het huidige risicobeheer en verzekeringsregelingen, in termen van de totale kosten van het managen van het risico. Dit helpt de besluitvorming te verbeteren zodat het budget efficiënter wordt ingezet om de cyberweerbaarheid te vergroten.

Stakeholdermanagement

Door het cyberrisico te kwantificeren, is de impact op de balans duidelijk en kunnen organisaties doelbewuster investeren in informatiebeveiliging, bedrijfscontinuïteitsprogramma's, risico-overdrachtsstrategieën en een cyberverzekering. Wanneer er een cyberincident plaatsvindt, laat het kwantificatiemodel aan toezichthouders en stakeholders zien dat er doordacht actie is ondernomen en de juiste inspanningen zijn geleverd om stakeholders (financieel, klanten, gemeenschap en leveranciers) te beschermen.

Verzekeren

Het kan ook voorkomen dat organisaties de cyberloop betreden vanuit verzekeren. De risicomanager heeft een belangrijke rol als verbinder tussen de verschillende disciplines. Het managen van cyber als een bedrijfsrisico vereist dat de risicomanager nauw samenwerkt met onder ander de CIO, CISO, de insurance manager, HR en Legal. Hij brengt de belangrijkste stakeholders bij elkaar. Zo bespreekt hij met de insurance manager of en hoe de cyberrisico-overdracht te verzekeren. De cyberverzekering dekt daarnaast ook de geleden financiële schade en schade aan derden.

Tegelijk met het afdekken van de financiële risico's biedt elke cyberverzekering incident response-dienstverlening. Zo kunnen zij direct over hulp van cyberspecialisten beschikken op het moment dat er een cyberincident plaatsvindt. Zij helpen om de gehackte organisatie zo snel mogelijk weer operationeel te krijgen en om de juiste beslissingen (bijvoorbeeld over communicatie en juridische stappen) te nemen.

Kennis van impact bepaalt keuze bescherming

Om de juiste keuzes te maken voor het verzekeren van cyberrisico's, is het van belang deze te kwantificeren. Organisaties die weten welke risico's zij lopen en welke financiële impact dit kan hebben, kunnen vervolgens bepalen welke beschermingsmaatregelen daarbij passen. Misschien is het zinvol om een deel te transfereren naar de cyberverzekeringsmarkt, maar ook het behoud van het risico of self-insuring zijn alternatieven.

Eisen van klant en leveranciers

Er is nog een andere reden om aandacht te schenken aan een cyberverzekering: klanten en leveranciers eisen in toenemende mate dat een organisatie een goede cyberverzekering heeft, kan aantonen dat het door hele organisatie maatregelen neemt tegen cyberrisico's én dat zij heeft geïnvesteerd in balansbescherming.

AON
Empower Results®

Incident response en crisismanagement

De kans op een cyberincident is altijd aanwezig en zoals we hebben laten zien, is beveiliging maar één onderdeel van alle maatregelen om de cyberweerbaarheid te vergroten. Ook als een cyberincident leidt tot een cybercrisis zijn de gevolgen nog sterk te beperken door vooraf, maar juist ook tijdens deze crisis de juiste beslissingen te nemen.

Incident response

Een daadwerkelijke cyberaanval staat centraal bij het betreden van de cyberloop vanuit Incident Response Readiness (IR). Hierbij is het mogelijk dat een organisatie de cyberloop op reactieve wijze betreedt, een cyberincident heeft dan plaatsgevonden, maar ook op proactieve wijze. Het grote voordeel voor organisaties die op proactieve wijze de cyberloop betreden vanuit IR, is dat er een vracht aan kennis aanwezig is om juist en adequaat te reageren op een cybercrisis.

Het beleid, de procedures en de verschillende rollen van de mensen zijn helder. Hierdoor is het voor incident-responders mogelijk om sneller een beeld te ontwikkelen van wat er exact aan de hand is binnen de organisatie, en hoe de dreiging zo snel mogelijk beperkt kan worden.

Veelvoorkomende cyberscenario's oefenen

Goed crisismanagement vraagt altijd goede voorbereiding en oefening. Oefenen kan het verschil maken tussen een organisatie die wordt geteisterd door een aanval, en een organisatie die het slechts als disruptief ervaart. Een organisatie met een interdisciplinair leiderschapsteam dat op veel voorkomende scenario's heeft geoefend, zal betere beslissingen nemen tijdens een cybercrisis en vermindert het risico voor de balans en stakeholders.

Maarten de Jonge:

"Direct na de start van een crisis komt er enorm veel op de getroffen organisatie af: leiding en coördinatie, continuïteit, mogelijke effecten bij leveranciers en/of klanten, interne en externe communicatie, vertrouwen/reputatie, onderzoek, juridische aspecten, verzekeringen en de mogelijke impact op veiligheid, beveiliging en HR. Al deze zaken moeten op hetzelfde moment worden gemanaged. Een managementteam met ervaring, bijvoorbeeld door gezamenlijk te oefenen, heeft een enorme voorsprong"

AON
Empower Results®

Maak uw organisatie voor eens en voor altijd cyberweerbaar

De risico's, impact en urgentie van het cybervraagstuk zullen u inmiddels duidelijk zijn. Juist voor de risicomanager is er een cruciale rol weggelegd in het traject van coördinatie en besluitvorming.

Heeft u vragen over cyberrisico's en hoe u hier als riskmanager 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.

Maarten de Jonge

Managing Consultant

Cyber & Privacy

maarten.de.jonge@aon.nl

Aon

Empower Results®