



De uitdagingen van de moderne risicomanager

Hoe om te gaan met verschuivende bedrijfsrisico's en het nieuwe takenpakket?

Toenemende digitalisering, een pandemie, geopolitieke verschuivingen, het klimaat en innovaties hebben een grote invloed op de markt en stellen hoge eisen aan organisaties. Alleen door wend- en weerbaar te zijn, kunnen organisaties succesvol blijven. Ondertussen vragen stakeholders steeds meer van organisaties als het gaat om het onder controle krijgen van de gevolgen van optredende risico's. Al deze ontwikkelingen vragen om een nieuwe invulling van het risicomanagement. Hoe zou het werk van de moderne risicomanager eruit 'moeten' zien?

Verschuiving naar centraal risicomanagement

Vaak worden risico's nog vanuit de desbetreffende deskundigheid benaderd; arborisico's door een hr-specialist, digitale risico's door de IT-specialist. Vervolgens kiest de insurancemanager (of iemand die de verzekeringen in zijn takenpakket heeft) ervoor om veel van deze risico's te verzekeren. Maar juist een organisatiebreed risico-overzicht in deze snel veranderende wereld blijkt nu essentieel. Vanuit die gedachte van 'total balance sheet protection' zien we de laatste jaren bij veel organisaties een verschuiving naar centraal risicomanagement.

Cruciale nieuwe taken bijgekomen

De traditionele risicomanager groeide vaak vanuit een rol controller of (bedrijfskundig) analist door. Hij of zij was cijfermatig onderlegd, ervaren, in staat om (met name) financiële en marktrisico's in kaart te brengen en dit ook helder te communiceren naar de stakeholders. In de loop der jaren kwamen er steeds meer taken bij, zoals het werken met risicoscenario's, bijbehorende risico-inschattingen uitgedrukt in harde euro's en ook de niet-financiële consequenties voor de organisatie. Deze taken vallen nog steeds onder het huidige risicomanagement, maar er zijn een aantal cruciale nieuwe taken bijgekomen.

Kijken naar de totale impact en daarop beleid maken

De risicomanager kijkt nu naar het totale plaatje van de organisatie. Hoe zit het met de (vaak niet tastbare) commerciële en operationele risico's? Wat kan de bedrijfsvoering overkomen en hoe leidt dat tot bedrijfsstilstand of imagooverlies? Het gaat dus niet alleen om de risico's in kaart brengen en deze een-voor-een managen.

Zo ziet het takenpakket van de risicomanager van nu eruit:

- risico's kwalificeren en kwantificeren, zelfs als er maar beperkt data beschikbaar zijn;
 - dit laatste geldt met name voor cyber, een nieuw dynamisch risico.
- impactanalyses maken, aangeven welk deel verzekerd kan en moet worden;
- de bestaande en toekomstige budgetten meenemen in het advies;
- communiceren richting de diverse stakeholders en directie, op een laagdrempelige manier;
- overtuigen met zachte hand, maar waar nodig ingrijpen met harde hand;
- continue leren van de huidige actuele risico aanpak van de organisatie;
- best practices in de markt.

Gezien dit takenpakket zal het niet verbazen dat de risicomanager van nu een steeds centralere rol speelt bij de beslissingen van het topmanagement en, al dan niet in de hoedanigheid als chief risk officer, aanschuift bij de bestuurstafel.

Wij helpen u graag succesvol te ondernemen

Neem contact op met:

Maarten de Jonge
Managing Consultant
Cyber & Privacy
06 129 618 07

AON
Empower Results®

Cyber risico's: meer tijd steken in mitigerende maatregelen

Nederlandse risicomangers zien reputatieschade, bedrijfsonderbreking en met name de oorzaak 'cyber' als de grootste risico's van nu, zo blijkt uit de Global Risk Management Survey 2019 van Aon. En hoewel het moment dat risico's een direct gevaar vormen onverwacht is, zien we dat de gevolgen van de risico's in deze veranderde wereld ook minder voorspelbaar worden. De recente coronapandemie is daar het ultieme bewijs van. Er moet dus niet alleen tijd worden gestoken in het in kaart brengen van de risico's, maar juist ook in het verdiepen in mitigerende maatregelen voor het onbekende.

Actief reageren op dreigingen, gebaseerd op feiten

Door de mogelijke gevolgen van externe bedreigingen, interne kwetsbaarheden en de bestaande beheersmaatregelen te inventariseren, kan de risicomanager bepalen welke stappen te nemen om de risico's beter beheersbaar te maken. Wat kan helpen is om een geïntegreerde aanpak vanuit een circulaire gedachte te hanteren. Elke organisatie kan op een andere manier beginnen met het versterken van haar cyberweerbaarheid: met assessment, kwantificering, verzekeren of incident response/crisismanagement. Een organisatie die gebruik maakt van zo'n circulaire aanpak is niet langer passief, maar heeft een denkvermogen dat continu wordt 'gevoed' door ervaringen en nieuwe inzichten. Zo kan zij, gebaseerd op feiten, actief reageren op (mogelijke) dreigingen.

Risicomanagement koppelen aan een circulaire gedachte

Het is onmogelijk om (cyber)risico's en hun impact, zoals financiële en reputatieschade als gevolg van een incident, volledig te beheersen. Het risico is overal aanwezig. Maar wanneer risicomangers vanuit de circulaire gedachte werken, versterkt dit de weerbaarheid van hun organisatie aanzienlijk. Het betekent dat de risicomanager van nu dagelijks met zijn collega's bezig is met de combinatie van beveiliging, monitoring, beleid, budget, incident response, crisismanagement en verzekeren. En, voor velen ook een grote uitdaging, het helder communiceren van al hun analyses, adviezen en bevindingen.