



Het risicolandschap voor de komende vijf jaar

Het risicolandschap verandert voortdurend en vereist van organisaties om snel te reageren, wendbaar te zijn en zich aan te passen aan die veranderende omgeving, inclusief eventueel de bijbehorende nieuwe spelregels (*Survival of the fittest; the most adaptable organisms - Darwin*). Een representatief aantal risicoprofessionals is recentelijk ondervraagd om de mate van voorbereiding op zowel traditionele als opkomende risico's te beoordelen en om de risico's te identificeren die hen voor de komende vijf jaar het meest zorgen baren.

Door Gert Kogenhop, Operationeel Manager BCM Kader Group

Wat is de belangrijkste drijfveer voor compliance in dit kader, het managen van risico's? Het lijkt erop dat het om meer gaat dan alleen de verwachtingen en eisen van belanghebbers. Ruim twee op de vijf ondervraagden gelooft dat compliance en het optimaal managen van dit onderwerp positieve voorwaarden kan scheppen voor organisaties en dat het voor commerciële bedrijven zelf kan leiden tot concurrentievoordeel. Zij zien dit dan ook simpelweg als 'zoals het hoort', good practice. Ongeveer één op de drie ziet het als een voorwaarde voor zakendoen en het voldoen aan wettelijke vereisten. Helaas, zou je kunnen zeggen, ziet één op de vijf professionals risicomanagement vooral als het vermijden van claims en rechtszaken.

Wat zijn de belangrijkste risico's voor de komende vijf jaren?

Cybercriminaliteit en de hieraan gekoppelde ICT-beveiliging springt eruit als de belangrijkste zorg. Bijna twee derde ziet het risico op een cyberaanval als een substantiële zorg. Slechts enkelen zien de kwestie als een klein probleem, wat de vraag oproept wat hun organisaties hebben gedaan om een duidelijk wijdverbreid risico aan te pakken; het risico erkennen is één ding, het mitigeren ervan is iets anders. Dit kan te maken hebben met het vertrouwen in hun aanpak, maar evengoed met zelfgenoegzaamheid. Het is ook de moeite

waard om er rekening mee te houden dat de recente golf van cyberaanvallen in de nasleep van de invasie van Oekraïne de zorgen op dit gebied kan hebben doen escaleren. Wat de reden ook is, de cijfers vertellen ons dat cybercriminaliteit het probleem is dat de meeste risicoprofessionals 's nachts wakker houdt.

Verstoring van de toeleveringsketen (Supply Chain) is een duidelijke nummer twee. Gezien de gevolgen van de pandemie, tot op zekere hoogte de Brexit en de gespannen relaties met China en Rusland plus de oorlogen en onrusten op diverse cruciale plekken in de wereld, is het niet verwonderlijk dat verstoring van de toeleveringsketen hoog op de lijst van erkende risico's staat. De versturende effecten van de pandemie lijken in de toeleveringsketen nog steeds niet helemaal verdwenen: op diverse gebieden is het nog geen 'business as usual'. Opvallend genoeg lijken de gevolgen van de pandemie in dit geval verontrustender dan de pandemie zelf. Desalniettemin hebben tekorten aan onderdelen en apparatuur door de diverse oorzaken een aanzienlijke invloed gehad op het risicodenken. Maatregelen die zijn genomen en overwogen worden zijn onder andere:

- meerdere leveranciers - 69%;
- near- en On-shoring (lokale/Nederlandse leveranciers) - 37%;
- in huis (terug)halen van uitbestede producten en diensten - 29%; en

- verplaatsing van sommige activiteiten naar stabielere landen/locaties - 22%.

Talentacquisitie, het beschikken over voldoende gekwalificeerd personeel, is de volgende meest geïdentificeerde uitdaging, zeg maar gewoon risico. De helft van de professionals geeft dit aan en zegt er last van te hebben. Dit kan te wijten zijn aan het geslonken personeelsbestand na de pandemie, maar dat is slechts een deel van het probleem. Realistischer is het dit te wijten aan een veelheid van zaken. Een opvallende reden lijkt de 'Great Resignation' te zijn, waarbij werknemers hun functie hebben verlaten nadat ze een andere levensstijl hebben ontdekt. Forbes Magazine heeft de oorlog om talent zelfs gemarkeerd als het nieuwe normaal, en McKinsey merkt op dat eerdere pieken in vrijwillig verloop vaak duiden op een concurrentie om talent, waarbij mensen veel makkelijker dan vroeger (verminderde loyaliteit) overstappen naar een andere organisatie. Men is nu toch van mening dat de nieuwe golf van verloop anders is, waarbij werknemers die gedurende langere tijd onder extreme omstandigheden werken 'privé boven werk' verkiezen. Om het nog ingewikkelder te maken, is er op veel gebieden een schaarste aan talent; mensen zijn in beweging. Veel van de vaardigheden die tegenwoordig worden gevraagd, werden tien jaar geleden nog niet onderwezen en de



pandemie heeft daarbovenop nog een deuk geslagen in mogelijke omscholing. Gezien de markt is het dan ook niet verwonderlijk dat hiervoor genoemde problemen vervolgens worden verergerd, doordat werknemers kieskeuriger zijn als het gaat om organisaties waarvoor ze willen werken.

Klimaatverandering staat op de radar van elke organisatie, en hier toonde de helft een hogere mate van bezorgdheid. Gezien de media-aandacht en potentiële risico's, ook vanuit actiegroepen trouwens, is het toch enigszins verrassend dat het voor de andere helft geen groot aandachtspunt is.

Pandemie is de verrassende hekkensluiter in dit rijtje. Terugdenkend aan de aanzienlijke en wijdverbreide gevolgen van de pandemie, die we allemaal nog op ons netvlies hebben, wordt het risico toch als laag beschouwd. Slechts één op de zes risicoprofessionals waardeert het als een substantieel risico. Mogelijk omdat het wordt gezien als een gebeurtenis die zich maar eens in je leven voordoet en zich in de

komende vijf jaren niet zal herhalen; mogelijk omdat een organisatie er niet veel aan kan doen; mogelijk omdat thuiswerken goed heeft gewerkt voor die organisaties waar dat mogelijk was.

Vanzelfsprekend zijn er nog meer risico's, zeker in specifieke sectoren. Het belang van gedegen risicomanagement – inclusief het mitigeren van die risico's die hoog scoren – lijkt belangrijker dan ooit. Dit mede als gevolg van de soms angstaanjagende afhankelijkheid van zaken, zoals de hier niet specifiek

benoemde IT en telecommunicatie. Uitval hiervan legt het merendeel van de organisaties compleet plat. Wordt dit niet benoemd omdat we dat al niet meer als een risico zien, maar iets wat gewoon 'a fact of life' is? Ik hoop het niet. Belangrijk is tevens, ook weer gelinkt aan het woord afhankelijkheid, dat als er iets gebeurt, je nooit verrast wordt en de controle verliest over het handelen van de organisatie en de levering van de belangrijkste producten en diensten. Zorg voor een gedegen, goed voorbereide reactie, een Plan B, het bedrijfscontinuïteitsplan – Business Continuity Plan (BCP).

Dit artikel is mede gebaseerd op onderzoek door Riskconnect in samenwerking met CIR Magazine (Continuity Insurance Risk). Riskconnect is een toonaangevende leverancier van geïntegreerde softwareoplossingen voor risicobeheer, bedrijfscontinuïteit en resilience.

Heb je een mening over risicomanagement in dit kader of heb je andere ervaringen als het gaat om Business Continuity Management gerelateerde risico's, laat me dat dan weten. Jullie reacties verwerk ik in een redactioneel stuk in een komend nummer. Een boeiende discussie is altijd goed! Mail me via: g.kogehop@kader.nl