Regie nemen is de taak van de risicomanager

Met de in rap tempo toenemende digitalisering van onze maatschappij verandert ook het risicoprofiel van bedrijven in sneltreinvaart. Geen enkele zichzelf serieus nemende onderneming kan er omheen om met enige regelmaat uitvoerig stil te staan bij de cyberrisico's die de bedrijfsactiviteiten met zich meebrengen. Dat blijkt wel uit de praktijk: 60% van de bedrijven heeft te maken met cyberincidenten, 20% wordt slachtoffer van een cyberaanval. Voor de financieel adviseur die zich heeft bekwaamd op het gebied van risicomanagement is er dus een hoop werk aan de winkel.

door Maarten van Wieren, managing director Aon Cyber Solutions

Cyberrisico's zijn mondiaal gezien één van de grootste en snelst groeiende bedrijfsrisico's. Ze vormen nu nog het tweede belangrijkste bedrijfsrisico's, net achter business interruption (bedrijfsonderbreking). Maar hoe lang ze die tweede plek nog innemen, is maar de vraag: vijf jaar geleden stonden cyberrisico's nog op de vijftiende plek. Goedbeschouwd is het ook niet verwonderlijk dat cyberrisico's binnen het bedrijfsleven aan zo'n opmars bezig zijn: vrijwel alles (processen, middelen, apparaten) om ons heen is tegenwoordig cyber. Was een telefoon vroeger nog een apparaat waarmee je contact kon leggen met een ander; tegenwoordig is het een computer waarmee je ook nog eens kunt bellen. Diezelfde vergelijking kun je ook maken met bedrijven; dat zijn nu vaak computersystemen waarmee je ook zaken kunt doen. Dat gaat overigens met name op voor de industriesector.

Vormen van cybercrime

Dankzij cyber is dus heel veel mogelijk geworden. Maar als je een zakelijke klant hebt die er waarde aan ontleent, moet je je er ook bewust van zijn dat die klant door cyber extra risico's gaat lopen. Zeker in de industrie is het anno 2018 onmogelijk om een bedrijf te runnen zonder geconfronteerd te worden met cyberincidenten. Verschillende partijen gebruiken cyber namelijk om uiteenlopende doelen te bereiken. Ten eerste overheden. Landen als Rusland, China of het Verenigd Koninkrijk hebben ieder hun eigen belangen. En die hoeven niet per definitie te stroken met die van (een specifieke sector in) Nederland. Er kan ook dreiging uitgaan van criminelen: van heel sophisticated bedrijfsspionage tot het cyberequivalent van de aloude kruimeldief. Tot slot zijn er de ideologische partijen. Een organisatie, zoals bijvoorbeeld Greenpeace zal er waarschijnlijk niet snel toe overgaan om zelf op georganiseerde schaal te hacken, maar een samenwerkingsverband als Anonymus wel. Ook terroristen hebben vaak ideologische drijfveren en van hen is ook bekend dat ze cyber gebruiken om hun doelen te bereiken. Het probleem hierbij is dat al deze partijen van elkaar leren waardoor dreigingen steeds meer geavanceerd worden.

Overige vormen van cyberdreiging

Cyberdreiging kan ook uitgaan van zaken als IT-systemen die falen of van onzorgvuldigheid van mensen. Neem een willekeurig bedrijf in gedachten en ga eens na wat er gebeurt als door een cyberincident zoiets simpels als telefonie-, data- of elektra eruit ligt. Dat is voor een bedrijf dat dagelijks grote hoeveelheden data verwerkt, zoals een advocatenkantoor, over het algemeen erger dan voor, bijvoorbeeld, een ambachtelijke glazenblazer. Maar het bedrijf ligt hoe dan ook (deels) plat en dat kost geld. Ook het cybergedrag van medewerkers, leveranciers en klanten vormt een bedreiging voor de cyberveiligheid van een onderneming. Met de inwerkingtreding van de AVG afgelopen 25 mei is het alleen maar belangrijker geworden dat bedrijven hier extra aandacht aan besteden.

Scope van de risicomanager

Als risicomanager moet je je realiseren hoe groot en reeel cyberdreiging is, je moet weten welke sectoren extra risico lopen en je moet weten uit welke hoek de dreiging te verwachten valt. De scope is enorm en komt ook nog eens bovenop de traditionele, bekende risico's, zoals letsel, brand- en waterschade en aansprakelijkheid. Maar daar blijft het niet bij. Een goede risicomanager heeft ook (basale) kennis van de systemen die ervoor kunnen zorgen dat de kans dat het risico zich voordoet kleiner wordt, zoals cybersecuritytechnologieën. Hij heeft nagedacht over wat er gebeurt als een veiligheidssysteem niet werkt, bijvoorbeeld een sprinklerinstallatie. Ook heeft hij nagedacht over hoe ervoor wordt gezorgd dat het management van een bedrijf na een cyberincident toch de juiste beslissingen kan nemen, welke info daar nodig voor is en hoe die naar boven kan worden gehaald. Je moet je als het ware een holistisch beeld vormen van de risico's waarmee een bedrijf geconfronteerd kan worden. En voor het uitvoeren van de specifieke maatregelen die genomen moeten worden om de kans dat het risico zich voordoet te minimaliseren de juiste expertise inhuren.

Rol en taken van de risicomanager

Wat goed is om te beseffen, is de verantwoordelijkheid en druk die - als 'linking pin' - op de schouders van de risicomanager rust. Bij een brand bellen we de brandweer. Zij nemen de regie en weten exact wat er moet gebeuren. Zo'n instantie is er niet als zich een cyberincident voordoet. De regie moet dan genomen worden door de risicomanager. Daar moet de klant vanuit kunnen gaan. Als je met kennis van zaken je klant bewust hebt gemaakt van de vele cyberrisico's waar hij aan is blootgesteld en daarvoor met goede adviezen maatregelen hebt getroffen, moet je er ook voor zorgen dat je klaar staat als puntje bij paaltje komt. Dus zorg dat er een gedetailleerd draaiboek ligt. En in het geval van een groot of impactvol incident: weet wie je moet inschakelen als er een forensisch expert nodig is, via welk nummer bij de Autoriteit Persoonsgegevens je een datalek moet melden en wat daarvoor nodig is. Weet ook wie je kunt bellen om de crisiscommunicatie op zich te nemen. En ga zo maar door. Ook hiervoor geldt dat je dit niet allemaal zelf hoeft te regelen: een deel gebeurt vanuit de verzekering en voor een ander deel regel je dat experts zijn aangehaakt. Daarom is het ook belangrijk dat een goede risicomanager de taal spreekt van alle stakeholders waarmee hij aan tafel zit. <

Adfiz, partner van SCHADE magazine