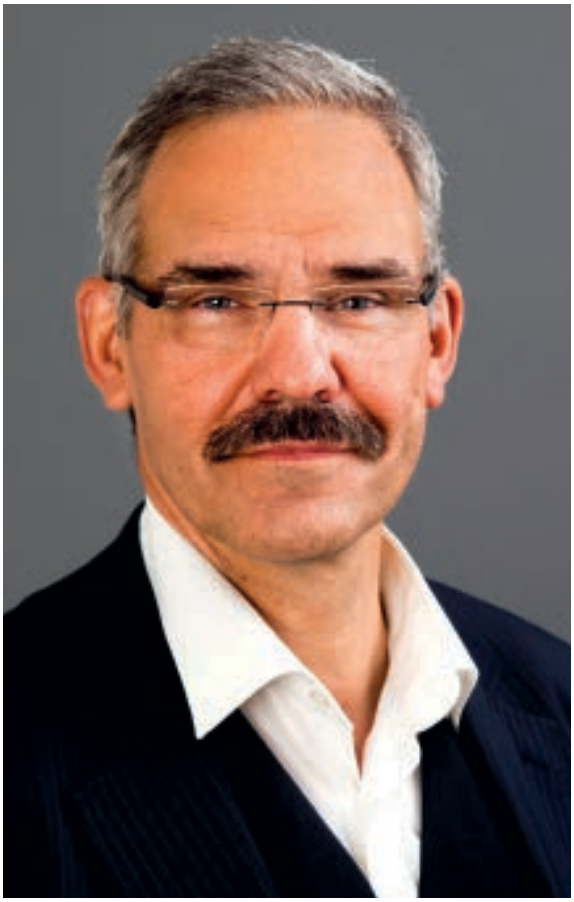
Risico's vermijden of verminderen zijn bekende strategieën om de veiligheid in een organisatie te managen. Hoge verzekeringspremies en hoge kosten voor beveiligingsmaatregelen zijn hiervan het gevolg. Maar bewust risico nemen en hierdoor nieuwe kansen voor de organisatie creëren, is een verfrissende andere kijk op de zaken. Een gesprek met Ron Massink, voorzitter van het Genootschap voor Risicomanagement.

tekst Frans Visser en Lies Thuring

Ron Massink, voorzitter Genootschap voor Risicomanagement:

'Risico's nemen biedt kansen'

Risicomanagement is vaak een containerbegrip. In de praktijk maken wij veelal mee dat het managen van (niet financiele) bedrijfsrisico's beperkt wordt tot het inhuren van beveiligers en het in stand houden van de aanwezige bouwkundige en elektronische beveiligingssystemen. Om de eventueel aanwezige mystiek rondom dit onderwerp te verminderen, geeft *Ron Massink*, manager integrale veiligheid van TU Delft en onder andere ook voorzitter van het Genootschap voor Risicomanagement, zijn visie op het onderwerp.



Ron Massink is manager integrale veiligheid van de TU Delft en onder andere ook voorzitter van het Genootschap voor Risicomanagement.

RISICOMANAGEMENT IN HISTORISCH PERSPECTIEF

Er zijn meerdere definities van risicomanagement in de vakliteratuur, maar in essentie is het niets meer of minder dan de verzameling van activiteiten die erop gericht zijn om de risico's van een organisatie op een aanvaardbaar niveau te houden. Naar aanleiding van bankschandalen, de economische recessie en zaken zoals reputatiebeschadiging en fraudezaken, kwam er begin deze eeuw aangescherpte regelgeving. De Amerikaanse senatoren Sarbanes en Oxley hebben in 69 artikelen getracht om met een naar hen genoemde wet (bekend als SOX) deugdelijk (internationaal) ondernemingsbestuur af te dwingen en nieuwe schandalen te voorkomen. Daarnaast zijn er Basel I-, Basel II- en Basel III-richtlijnen opgesteld. Deze zijn gericht op het versterken van de kwaliteit, de kapitaalsnormen en de liquiditeit van de banken.

VAN THEORIE NAAR PRAKTIJK

Ondanks deze (in ieder geval binnen de financiële sector) strenge regelgeving is risicomanagement geen doel op zich, of uitsluitend een middel om sancties van een toezichthouder te voorkomen, maar biedt risicomanagement ook kansen. Een goed risicobeleid brengt namelijk niet alleen risico's en bedreigingen aan het licht, maar maakt ook inzichtelijk waar mogelijk nieuwe kansen liggen. Belangrijk hierbij is dat de securitymanagementafdeling een zeer goede kennis heeft van de eigen organisatie, en daardoor de organisatiestrategie kan beïnvloeden.

Voorbeeld

Een transportbedrijf dat dagelijks vestigingen van McDonalds bevoorraadt, zal zich voornamelijk richten op de risico's rondom een strakke planning, een goed wagenpark en fitte chauffeurs. Maar een technologiebedrijf dat zaken doet met Rusland zal zich veel meer richten op risico's rondom (cyber)beveiliging en het trainen op mogelijke veiligheidsrisico's voor de eigen mensen.

Er zijn dus geen gelijke risico's en elke onderneming moet bewust eigen afwegingen maken. Dit noemen wij het opstellen van een risicoprofiel. Het woord 'risicoprofiel' schrikt mogelijk af, maar het is niets anders dan wat wij elke dag weer doen. Voorbeeld: als je objectief nadenkt welke risico's je loopt door in de auto te stappen en de snelweg op te rijden, zou je eigenlijk thuis moeten blijven. Toch doen wij het elke dag weer. Onbewust wegen wij de risico's (regen, drukte, gladheid, laaghangende zon, defect aan auto, andere weggebruikers enz.) af tegen de opbrengst (snelle verbinding, comfortabele wijze van reizen, enz.).

GRENZEN ZOEKEN IS ONDERNEMEN

Het is de kunst voor de security-afdeling om de onderneming optimaal te ondersteunen in haar strategie en kerndoelen, door te zoeken naar de grenzen van de acceptatie van het risicoprofiel van de onderneming. Je kunt dat zien als een dashboard of mengpaneel, waar je met schuifjes en knoppen kunt draaien om zo minder of meer risico te nemen, afhankelijk van het onderwerp en de actuele situatie.

Een mooi voorbeeld zijn de vele *start-ups*. Zij beginnen gewoon met hun activiteiten en dat biedt veel kansen. Uiteraard lopen zij tegen grenzen aan en dan is het zaak om de rafelrandjes eraf te knippen zodat het niet fout gaat. Hiermee kan een onderneming met een hogere snelheid haar doelstellingen bereiken. Denk ook eens aan de Japanse kogeltreinen die

Onderzoek de risicobereidheid van de onderneming

– uiterst veilig – al jarenlang zonder problemen en met zeer hoge snelheden (de nieuwe versie gaat tot circa 500 km per uur!) het land doorkruisen: hoge snelheid en toch de risico's onder controle!

RISICOMANAGEMENT-MODELLEN

Zoals gezegd gaat het erom dat de visie en kerndoelen van de onderneming bekend zijn. De CEO, de directie of het managementeam heeft deze vastgelegd en security kan toegevoegde waarde bieden door een risicomanagementstrategie te ontwikkelen. Vraag is welke systemen er zijn om dit proces te besturen?

INK-model

Een eerste stap kan het INK-model zijn waarmee een goed inzicht in de eigen onderneming verkregen wordt. 'Ken je bedrijf' is hiervan het resultaat. Een belangrijke start om daarna de verschillende risico's in beeld te krijgen.

COSO

COSO is een ander goed te hanteren model dat is ontwikkeld door The Committee of Sponsoring Organizations of the Treadway Commission. Dit comité geeft richtlijnen voor interne controle en interne beheersing. In 2004 werd het model geactualiseerd, werden elementen toegevoegd en aangepast. Dit geactualiseerde model richt zich niet meer alleen op interne →

Invoering risicomanagement in 6 stappen

1. Zorg voor goede kennis van de onderneming.
2. Onderzoek de risicobereidheid van de onderneming.
3. Adopteer de belangrijkste kortetermijndoelstellingen.
4. Maak een mix vanuit beproefde modellen.
5. Ontwikkel een eigen risicomanagement-dashboard.
6. Wees actief: bedenk zelf nieuwe projecten (ondernemer binnen de onderneming).

controle maar op het gehele interne beheersingssysteem en staat bekend als COSO II of Enterprise Risk Management Framework (ERMF). COSO is een van de standaard referentiemodellen die door auditors worden gebruikt bij een onderzoek.

ISO 31000

ISO 31000 beschrijft de principes en algemene richtlijnen voor de implementatie van risicomanagement. Deze richtlijnen zijn bedoeld voor alle typen organisaties, ongeacht grootte en aard van de activiteiten, en kunnen worden toegepast op een breed scala van activiteiten, projecten, producten, assets, maar zijn vooral gericht op organisatiebreed risicomanagement.
ISO 31000 laat nadrukkelijk ruimte voor maatwerk, omdat wordt onderkend dat risicomanagement maatwerk is. Een voordeel van het hanteren van het ISO 31000-model is dat het, naast het verminderen of overdragen van risico's, ook aandacht geeft aan het nemen of zelfs vermeerderen van risico's. Hiermee wordt de onderneming in staat gesteld om nieuwe kansen te benutten, omdat barrières en investeringen bewust wel of niet genomen worden en zo haar doelstelling behaald kan worden.
ISO 31000 is niet certificeerbaar, maar dat is eigenlijk wel fijn, omdat een vast format vaak beklemmend werkt en mogelijk alleen nog maar een afvinklijst van onderwerpen wordt. En zoals gezegd is iedere onderneming anders en kan je dus zelf de benodigde onderwerpen kiezen die passen bij de eigen onderneming.

DASHBOARD

Securitymanagement kan bijdragen aan het realiseren van de doelstellingen van de onderneming door het actief inzetten van risicomanagement.

Eerste stap

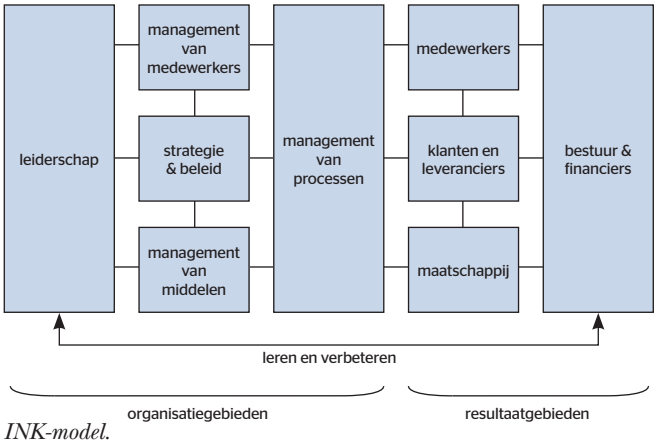
De eerste stap is het ontleden van de onderneming: wie zijn wij? Gebruik maken van het INK-model kan hierbij van waarde zijn.

Tweede stap

De tweede stap is achterhalen hoe de onderneming tegenover risico's en kansen staat: wat is de risico-attitude van de onderneming? Grofweg zijn er drie mogelijkheden:

1. een offensieve (risicozoekende) benadering
2. een neutrale (risiconeutrale) benadering
3. een defensieve (risico-aversie) benadering.

De benadering van risico's kan zeer verschillend zijn.



INK-model.

Politiemensen bijvoorbeeld voelen zich meestal wel veilig tijdens de uitvoering van hun werkzaamheden, terwijl zij relatief gezien veelvuldig aan onveilige situaties blootgesteld worden. Gewenning aan deze onveilige situaties geeft waarschijnlijk een gevoel van *control*, waardoor dit niet altijd meer gezien wordt als onveilig. Daarnaast moet je ook aandacht geven aan mogelijke cultuurverschillen. Een voorbeeld: vrouwelijke studenten midden in de nacht op de bus laten wachten is in bijvoorbeeld India volledig anders dan in ons land.

Derde stap

De derde stap is het centraal vastleggen van incidenten. Hiermee kunnen over de afgelopen periode analyses gemaakt worden die met meer of minder maatregelen weer op de toekomstige periode anticiperen. Indien security voor haar diensten en producten op deze wijze het risicomanagement inricht en laat aansluiten op de bedrijfsdoelen, zal zij zich vrijer voelen om een volgende stap te maken. Bij elk project of onderwerp wordt dan structureel afgewogen of er meer of minder risico gelopen kan worden en zij toch in control blijft. Daarmee ontstaat een dashboard voor risicomanagement.

SAMENVATTING

Risicomanagement is maatwerk en kan, indien er actief mee gewerkt wordt, een bijdrage leveren aan de doelstelling van een onderneming. Het geeft naast het afdekken en bewust nemen van risico's ook nieuwe kansen voor securitymanagement om haar toegevoegde waarde te laten zien. ■

Frans Visser en Lies Thuring zijn verbonden aan Visser & Van der Ven security management (www.visservdven.nl), samenwerkingspartner van VFM facility experts.