BCM: Bezint eer ge begint!

Risicomanagement is een begrip geworden en is zeker binnen de grotere mkb-bedrijven een discipline die redelijk goed tot goed geborgd is. Bij multinationals maakt dit als vanzelfsprekend onderdeel uit van de organisatie. Er worden risicoprofielen gemaakt, analyses met verschillende invalshoeken op zowel 'Enterprise' (ERM) als 'Operational' (ORM) niveau uitgevoerd, er wordt met risicoregisters gewerkt en er is in vele gevallen een goede samenwerking met de (ad hoc) crisisorganisatie, het Crisis Management Team (CMT), als het gaat om de uitwerking van de verschillende scenario's. Als het gaat om het inrichten van Business Continuity Management (BCM) ofwel bedrijfscontinuïteitsbeheer, dan is dat bij de écht grote jongens wel goed geregeld, maar tegelijkertijd bij velen helemaal niet. Een duidelijke omissie; in mijn woordenboek is dit een foutieve weglating. *'Het ontbreken van een handeling, aldus een nalatigheid of verzuim'.*

Door Gert Kogenhop, bcm+

Recent zijn er weer voldoende voorbeelden van ernstige verstoringen van de bedrijfsvoering geweest die iedereen kent, maar dat wil niet zeggen dat betrokkenen ook allemaal adequaat en optimaal hebben kunnen reageren in de betreffende situatie. Enkele voorbeelden in ons eigen land zijn de (niet onverwachte) OV-stakingen en de (onverwachte) PIN-storingen en niet werkende kassa's bij Albert Heijn, Etos en Gall & Gall. Verder waren de gevolgen van een storing in het brandstoftoevoersysteem op Schiphol enorm te noemen. Inmiddels zijn we allemaal wel een beetje klaar met, maar velen nog steeds onvoldoende voorbereid op, de impact van wel/geen Brexit … *'In any shape or form'*. Wereldwijd zijn er vele voorbeelden van incidenten als gevolg van extreem weer te noemen en kort geleden nog de massale stroomuitval in Zuid-Amerika en op een avond in Manhattan, New York, het hart van het uitgaansleven. De gevolgen van cybercrime in al z'n vormen en facetten zijn nog niet tot iedereen doorgedrongen, maar in dit specifieke geval gaat het er hier niet meer om óf het gebeurt, maar alleen nog maar wanneer en wellicht hoe erg het wordt. Personeelstekort is één van de grootste knelpunten in de sectoren zorg, onderwijs, land- en tuinbouw en automatisering. Ook dit is een sluipend, groeiend continuïteitsrisico en er zullen andere sectoren volgen.

Nogmaals, de risico's zijn wellicht onderkend en staan in het risicoregister en op uw radar, u heeft binnen het crisisteam de taken wellicht ook al verdeeld en de woordvoerder heeft ook al zijn of haar woordje gereed. Als het bijvoorbeeld om cyberdreigingen gaat is binnen de discipline Informatiebeveiliging ook al ontzettend veel geregeld om te voorkomen dat hét gebeurt en er zijn processen toegevoegd om te kunnen detecteren en monitoren. Optimaal voorbereid zo lijkt het. Maar hoe staat het met uw reactie als het dan tóch gebeurt? Hoe zorgt u ervoor dat u uw producten en diensten kunt blijven leveren? Dát is benodigd voor de continuïteit van uw organisatie.

Ga eens bij uzelf en uw organisatie te rade en zeg eens eerlijk: 'Hoe goed bent ú voorbereid?'

Wat is Business Continuity Management?

Dit is het holistisch managementproces dat potentiële bedreigingen voor een organisatie identificeert en tot welke gevolgen deze bedreigingen mogelijk kunnen leiden met betrekking tot de operationele activiteiten. Het schept een kader voor het opbouwen van organisatorisch weerstandsvermogen en veerkracht (resilience), leidend tot een effectieve reactie die de belangen van alle betrokkenen (stakeholders), reputatie, merk en waarde creërende activiteiten

veiligstelt. Simpel gesteld gaat het om het zo optimaal mogelijk voorbereid zijn op het (on)verwachte. De strategische, tactische en operationele vaardigheden van een organisatie om te plannen voor en te reageren op ernstige incidenten, met als direct gevolg een ontwrichting van de organisatie. Dit om te kunnen waarborgen dat de organisatie zo snel mogelijk, met zo min mogelijk schade operationeel op minimaal een van tevoren vastgelegd niveau functioneert. Voorkomen is beter dan genezen (proactief), maar als hét dan tóch gebeurt, juist weten te reageren (reactief).

Wat levert Business Continuity Management op?

Naast dat het geen toelichting behoeft waarom aandacht voor het optimaliseren van de bedrijfscontinuïteit zo belangrijk is – wie wil er niet morgen nog zijn bedrijf c.q. baan hebben – is het wel zinnig om te kijken naar de extra waarde van een gedegen Business Continuity Management Systeem. We hebben het dan over een breder inzicht in uw activiteiten vanuit een continuïteitsperspectief, met kennis van zaken aangaande bijvoorbeeld Single Point of Failure (We hebben slechts één machine die dit kan), Single Point of Knowledge or Authority (Slechts één persoon – of enkelen – die iets van groot belang voor de organisatie kunnen of mogen) of Single Sourcing (We hebben maar één leverancier voor deze belangrijke grondstof).

Maar we hebben het ook over het toegenomen weerstandsvermogen en veerkracht van de organisatie, door aandacht voor dit onderwerp in al haar facetten. Het versterkt uw merk en reputatie en eventueel concurrentievoordeel, wat te halen valt uit het delen hiervan met (potentiële) klanten onder het mom van: 'Wij kunnen u te allen tijde en onder alle omstandigheden van dienst zijn en blijven.' Voorts leidt een implementatie ontegenzeggelijk tot organisatieverbeteringen en mogelijk zelfs kostenbesparingen als gevolg hiervan, bijvoorbeeld ook bij verzekeringen en financieringen (vanwege lagere risico's door beheersmaatregelen). Verder is er een duidelijke bijdrage aan de inspanningen van de organisatie op het gebied van maatschappelijk verantwoord ondernemen (MVO) en compliance (Corporate Governance).

Ontwikkeling van BCM

Tot voor kort was dit onderwerp bij vele organisaties volledig onbekend, laat staan als BCMS, als managementsysteem. Wel werd in sectoren als de voedings- en chemische industrie (als gevolg van wet- en regelgeving) en in de ICT-, telecom- en energiesector als gevolg van eisen vanuit de markt of van toezichthouders, aandacht besteed aan het waarborgen van de continuïteit van specifieke activiteiten bij bepaalde risico's. Ook De Nederlandsche Bank stelt in dit kader eisen aan banken en verzekeraars. Een financieel debacle als rond 2008 willen we liefst nooit meer meemaken.

Er bestaat sinds 2012 een ISO-standaard aangaande dit onderwerp, ISO 22301. Naar verwachting zal eind dit jaar een herziene versie worden gepubliceerd. Steeds meer bedrijven herkennen en erkennen hun afhankelijkheid van specifieke partners of leveranciers en deze afhankelijkheid leidt tot het vriendelijke, maar dringende verzoek om met BCM aan de slag te gaan. In vele gevallen wordt zelfs tijdens nieuwe contractonderhandelingen gesproken over de eis tot het inrichten van een BCMS of zelfs certificering conform de ISO 22301-standaard. Op deze wijze verschijnt het

op de agenda van steeds meer organisaties en velen nemen dit (soms verplicht dus) serieus ter hand. Men wil voorbereid zijn.

Hoe pakt u dit aan?

Ondernemen is risico nemen, maar tegelijkertijd is een van de belangrijkste doelstellingen er voor een heel lange tijd te zijn en te blijven. Risicomanagement, crisismanagement en business continuity management maken aldus een wezenlijk onderdeel uit van het vergroten van de kans op een succesvolle duurzame inspanning van alle betrokkenen. Het hoort bij 'Hoe wij hier werken'. Neem als organisatie eens de tijd om een workshop te organiseren met het managementteam en doorloop het stappenplan hieronder met als vraagstelling: 'Wat is er minimaal nodig om onze doelstellingen te halen?'

Kunt u (high level):

a) activiteiten, processen en middelen identificeren die nodig zijn om uw doelstellingen te bereiken; en

b) de minimale operationele niveaus voor elk van deze bepalen?

Voor activiteiten en processen lukt dit waarschijnlijk wel, maar vervolgens bepalen welke middelen daarvoor minimaal nodig zijn, is vaak al een stuk lastiger. Denk hierbij bijvoorbeeld aan:

- mensen (aantal, rollen, autorisatieniveau, vaardigheden);
- informatie en gegevens (formulieren, handleidingen, werkvoorschriften);
- gebouwen, werkomgeving en bijbehorende voorzieningen (speciale vereisten, zoals hoogte, temperatuur, locatie, bronwater of hoogspanning);
- faciliteiten, uitrusting en verbruiksartikelen (machines en gereedschappen);
- informatie- en communicatietechnologie (ICT) en -systemen (type systeem, applicaties, toegang tot specifieke harde schijven of smartphones);
- transport (aantal vrachtwagens, vereisten zoals de grootte van de vrachtwagen of gekoeld);
- financiën (minimale omzetgrootte, hoeveel geld moet beschikbaar zijn); en
- partners en leveranciers (afhankelijkheid van of kan niet zonder ...).

Wilt u vervolgens:

c) evalueren wat er nodig is om te voorkomen dat u ooit onder deze niveaus komt; en

d) uitgaande van de huidige stand van zaken de hiaten identificeren.

Als gevolg hiervan dient u actie te ondernemen in overeenstemming met de doelstellingen van bedrijfscontinuïteit, zo u die reeds heeft, en de risicobereidheid van de organisatie. Uiteindelijk kunt u hier de vervolgvraag nog aan toevoegen: 'En wat hebben we nodig in geval van een ernstig incident om als organisatie te overleven?'

Van systeem naar gedrag

Een duidelijke trend in de laatste vijftien jaar – die is begonnen binnen risicomanagement en die doorgezet moet worden binnen bedrijfscontinuïteitsbeheer – is de verschuiving van het systeemdenken naar houding en gedrag. Waar voorheen alle risico's zoveel als mogelijk werden gekwantificeerd en de uitkomsten van bijvoorbeeld Monte Carlo-simulaties als waarheid golden, gaat het nu veel meer om houding en gedrag. Immers, het overgrote deel van de risico's – en de gevolgen – zijn gerelateerd aan menselijk (niet) handelen! Om te weten of er grote risico's worden gelopen is het derhalve veel bepalender welke risicocultuur er in een organisatie heerst dan de omvang van de investeringen.

> **Bent u voorbereid op een calamiteit en de gevolgen daarvan voor de continuïteit?**

Vertrekkend vanuit het principe dat het voor de belangrijkste producten en diensten van een bedrijf van het allergrootste belang is dat in ieder geval de hiermee samenhangende kritische activiteiten te allen tijde en onder alle omstandigheden moeten worden uitgevoerd, hoeft het verder geen betoog dat alle betrokkenen daarvoor dan ook een uiterste inspanning dienen te verrichten. Deze inspanning, simpelweg het 'Wie, Wat, Hoe, Waar en Wanneer' zal echter alleen succesvol worden verricht wanneer iedereen het 'Waarom' hiervan begrijpt en onderschrijft.

De conclusie is waarschijnlijk het antwoord op de vraag: 'Hoe belangrijk is het voor onze organisatie om onder alle omstandigheden, te allen tijde te blijven leveren?' Indien u tot de conclusie komt dat er werk gemaakt moet worden van BCM binnen uw organisatie heeft u de 'Waarom' vraag aldus beantwoord. Vervolgens zult u aan de gang moeten, echter 'Bezint eer ge begint!', want dit is geen eenmalig, vrijblijvend project. Het gaat blijvend onderdeel uitmaken van de organisatie. Vervolgens gaat het om het bepalen van de aanpak en dan voornamelijk om het *Wie* en het *Hoe*.

Wie

Deze voor velen nieuwe discipline dient ergens ondergebracht te worden. Daar bestaat geen eenduidig antwoord op, maar algemeen gesproken wordt bij informatie-intensieve organisaties – zoals overheidsorganisaties, banken, verzekeraars en ICT-gerelateerde bedrijven de combinatie gezocht met informatiebeveiliging, terwijl bij productiebedrijven vaak de link wordt gemaakt met de kwaliteitsmanager. Deze laatste bekijken we hier iets gedetailleerder. De rol van (over het algemeen) de kwaliteitsmanager (KAM, QHSE-QESH, QA/QC) is hierbij cruciaal. Deze heeft, naast vakspecifieke normen en certificeringen, vaak reeds ISO 9001 (kwaliteitssysteem) en ISO 14001 (milieuzorgsysteem) onder zijn of haar hoede. Beiden worden/zijn net als ISO 22301 (bedrijfscontinuïteit) conform de HLS ingericht.

Hoe waardevol is het wanneer de kwaliteitsmanager zich kan ontwikkelen tot de

organisatorische spil op het gebied van de operationele risico's en continuïteit? Dit betekent wel een meer faciliterende, stimulerende en coördinerende rol. Belangrijke vaardigheden van een 'goede' bcm-risicomanager zijn, naast kennis van zaken vanzelfsprekend, onder andere:

- sterk analytisch vermogen aangaande het procesverloop en incidenten;
- in staat te rapporteren over wat goed gaat en wat beter kan;
- daagt uit naar volledigheid;
- weet het nooit beter, maar stimuleert de dialoog en het beslissingstraject;
- rapporteert over de opvolging van afgesproken beheersingsprocessen;
- helpt het management met het stellen van de juiste vragen;
- geeft handvatten en bewaakt het continu verbeterproces en correctieve acties; en
- adviseert gevraagd en ongevraagd, maar neemt de problemen niet over.

Hoe

In eerdere artikelen in dit magazine is al uitgebreid ingegaan op het 'Hoe', dus hier ga ik niet verder dan een korte beschrijving.

In twee stappen analyseert u de organisatie. Uitgaande van een bedrijf, gaat u bijvoorbeeld uit van de belangrijkste producten en/of diensten. Nadat deze zijn vastgesteld worden alle activiteiten tegen het licht gehouden en die activiteiten geselecteerd, die een directe bijdrage leveren aan het tot stand komen van de belangrijkste producten en/of diensten middels een Business Impact Analyse (BIA). Deze activiteiten worden geanalyseerd en beoordeeld op gevoeligheid voor een aantal van tevoren vastgestelde impactgebieden, zoals financiële impact, klanttevredenheid, productkwaliteit, reputatie en het voldoen aan wettelijke verplichtingen of overeengekomen SLA's (service level agreements).

Op deze wijze prioriteren we alle activiteiten en komen de meest kritische activiteiten naar voren en tegelijkertijd welke activiteiten best wel even kunnen stilliggen in geval van een ernstig incident of een calamiteit. De risicobeoordeling (RB) geeft inzicht in welke risico's voor de onderneming reëel zijn: algemene risico's (brand, stroomstoring, pandemie of IT-uitval), risico's behorend bij de aard van de activiteiten (advocatenkantoor, bakkerij of chemieconcern) en de vestigingsplaats (nabij water, het spoor, een luchthaven, een tankstation aan de overkant, wie zijn de buren ...). Het gaat hier om de kans en de mogelijke impact van het feit dat een bedreiging een ernstige verstoring veroorzaakt. Niet alle risico's kunnen vanzelfsprekend worden uitgesloten: er zal altijd een restrisico blijven.

Na bepaling van de 'gevaarlijke' combinatie van risico's en de eerder vastgestelde activiteiten, die onze belangrijke producten en/of diensten ondersteunen geven we invulling aan de vraag 'Wat vervolgens te doen?' Er worden diverse scenario's uitgewerkt met de kritische activiteiten (uit de BIA) als eerste prioriteit, op basis van de grootste risico's (uit de RB). Simpelweg gesteld zijn dit scenario's met als uitgangspunt: 'Hoe leveren wij onze klanten zo snel mogelijk in de volgende situaties':

- uitval van IT of telecom;
- stroomuitval (of water/gas);
- de locatie is onbereikbaar (wegafsluiting, afgebrand, explosiegevaar bij de buren...);
- ... specifiek voor uw situatie

En niet direct productiegericht: 'Hoe overleven wij als onderneming in geval van':

- een grote terugroepactie van ons product;
- het verlies van een grote klant, order of tender;
- het verlies van een belangrijke (product) certificering; en
- ... specifiek voor uw situatie.

Om ervoor te zorgen dat iedereen de extra toegevoegde waarde van dit soort managementsystemen ziet, is het belangrijk dat de link naar de strategie wordt behouden. Een strategische afstemming tussen de organisatiedoelstellingen en de doelstellingen van zowel risicomanagement als business continuity management (en crisismanagement) is dan ook een voorwaarde voor succes. De prestaties van de organisatie gaan over het realiseren van de doelen en daar horen risico's bij. Risicomanagement gaat over het nemen van risico's in het licht van de doelstellingen. Business continuity zorgt ervoor dat het weerstandsvermogen en de veerkracht van de organisatie te allen tijde voldoende is. Voorwaarden zijn dan ook:

- onvoorwaardelijke ondersteuning van bestuurders en de juiste plaats op de agenda;
- het actief betrekken van alle betrokkenen bij implementatie en onderhoud;
- SMART doelstellingen, *liefst SMART**IE** (tevens **I**nspirerend, ik moet er **e**nergie van krijgen, en Educatief, ik wil er iets van leren);*
- duidelijke succesfactoren, zodat iedereen weet waarin we goed moeten zijn om de doelstellingen te realiseren;
- zicht op de risicofactoren die het succes in de weg kunnen staan;
- continu (bij)sturing op basis van de veranderende omgeving en blijven verbeteren;
- oefenen, oefenen en oefenen.

Hou in elk geval een aantal belangrijke zaken op het netvlies. Blijf weg van bangmakerij of 'vermeende' risico's (negatief), maar richt u op de bepaling van die activiteiten die essentieel zijn voor de organisatie (positief) om uw doelstellingen te bereiken, zoals uit de workshop naar voren is gekomen bijvoorbeeld. Zo optimaal mogelijk voorbereid, kan de organisatie zich aanpassen aan veranderingen met betrekking tot (on)verwachte invloeden op de mogelijkheid om te leveren (product en/of dienst). De toegevoegde waarde van het vermogen zich aan te passen aan het leveren van een minimumniveau aan producten en diensten – essentieel voor het voortbestaan – levert een aanpak op die direct gekoppeld is aan de doelstellingen van de organisatie voor zowel de normale bedrijfsvoering (Business as Usual) als welke nodig is om te overleven na een ernstige verstoring (Business as NOT Usual). Door het versterken van het weerstandsvermogen en de veerkracht van de organisatie, door flexibiliteit op deze wijze als dimensie toe te voegen, dient deze inspanning beschouwd te worden als 'cost of doing business'. Door het verbeteren van de leverbetrouwbaarheid, is het duidelijk dat BCM van toegevoegde waarde voor de organisatie is. Q