Verschillende expertisegebieden optimaal laten samensmelten

Hoe veerkrachtig wilt u zijn?

Veel organisaties die een risico-, crisis-, IT- of Business Continuity Management Systeem hebben geïmplementeerd, doen dit door een enorme hoeveelheid Word- en Excel-bestanden te creëren, veelal ondersteund door databases, echter los van elkaar, zo leert de ervaring. Ze gebruiken daarbij nagenoeg altijd PowerPoint of andere office-software om de informatiestroom te ondersteunen. In sommige gevallen wordt SharePoint gebruikt om het systeem robuuster te maken en om een veilige omgeving te creëren voor het opslaan van documenten, berekeningen en andere gegevenscomponenten. Enkele grotere organisaties hebben eigen systemen of instrumenten gebouwd voor deze disciplines en hoewel deze in de meeste gevallen aan hun specifieke behoeften voldoen, zijn ze moeilijk te onderhouden, laat staan verder te ontwikkelen in een constant veranderende omgeving met nieuwe wet- en regelgeving, plus (klant) eisen. Een link tussen de verschillende disciplines is in slechts enkele gevallen voorzien. Creëren ze op deze wijze een veerkrachtig, flexibel overall beheersysteem dat op elk moment klaar is om te worden gebruikt wanneer dat nodig? Of is dit slechts de eenvoudigste en 'slimste' manier om te voldoen aan de vereisten met betrekking tot een documentmanagementsysteem?

Door Gert Kogenhop

Elke organisatie wordt blootgesteld aan risico's, zoals ICT-uitval, een bedrijfsbrand, problemen met energievoorziening of extreem weer. Andere risico's zijn meer branchespecifiek: van de chemische industrie tot softwareontwikkelaar, van bouwbedrijf tot datacenter, van gemeente tot bakkerij. Ook waar organisaties gevestigd zijn maakt een verschil; in de buurt van een luchthaven of naast een rivier, dijk of dam of bijvoorbeeld naast een chemische fabriek of een olie-opslag of een distributiecentrum. Risk Management, organisational en operational, is een must voor de organisatie en over het algemeen wordt dit redelijk goed beheerst en beheerd (gemanaged): vooral in grotere organisaties waar het gebruik van bijvoorbeeld Integrated Risk Management (IRM) software gebruikelijk is. Deze aanpak bestaat uit een reeks processen en procedures die de besluitvorming en prestaties ondersteunen en verbeteren. Het geeft een geïntegreerd beeld van hoe goed een organisatie haar specifieke risico-set managet. De wereld – en specifiek onze (zakelijke) omgeving – verandert in een steeds hoger tempo, dus we moeten allemaal voortdurend onze ogen op de bal houden. Voorbeelden zijn de gevolgen van klimaatverandering, de brexit, de handelsoorlog VS versus China, het coronavirus en de ontwikkelingen op cyber security gebied. Denk bij dat laatste maar eens aan de gebeurtenissen bij de Universiteit van Maastricht en vele andere recente situaties.

Onvoorbereid zijn is niet acceptabel

Tegenwoordig is iedereen afhankelijk van informatietechnologie. Als gevolg daarvan zijn informatiebeveiliging en gegevensbescherming belangrijke elementen waar aandacht aan moet worden besteed. De EU-richtlijn 'Concerning measures for a high common level of security of network and information systems across the Union' en de 'General Data Protection Regulation' (GDPR) zijn belangrijke drijfveren voor alle IT-gerelateerde disciplines. IT-afhankelijkheid maakt organisaties kwetsbaar en daarom moet dit worden aangepakt en gemanaged. IT-uitval, niet alleen technisch falen, maar ook het niet beschikbaar zijn van applicaties, netwerken en 'het internet' als gevolg van cybercriminaliteit veroorzaakt een enorme verstoring en kan voor veel organisaties zelfs fataal zijn.
Organisaties kunnen dus steeds vaker worden geconfronteerd met een crisissituatie als gevolg van een ernstige verstoring. Crisismanagement en Business Continuity Management zijn voorwaarden voor een goed gemanagede organisatie en in sommige landen zelfs verplicht. Onvoorbereid zijn is niet acceptabel en 'we zullen handelen wanneer het gebeurt'

is onverantwoordelijk en wordt zeker niet beschouwd als een 'good business practice'.

Weerbaarheid en veerkracht

Organisaties moeten stabiel, robuust en tegelijkertijd veerkrachtig (resilient) en wendbaar (agile) zijn. Enige tijd geleden is de term Organisational Resilience geïntroduceerd, hoewel er nog geen overeenstemming is over hoe deze te definiëren. Gezien de complexiteit van het verband tussen onder meer resilience, risico en business continuity management is het verstandig om met resilience te beginnen, omdat dit een overkoepelend karakter heeft. Als het gaat over resilience – weerstandsvermogen (weerbaarheid) en veerkracht – dan moet deze wel in de juiste context geplaatst worden. Hierna een aantal definities die voor het behoud van originaliteit in het Engels zijn.

Psychological resilience is the ability to mentally or emotionally cope with a crisis or to return to pre-crisis status quickly.

Computer networking resilience is the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.

Material science resilience is the ability of a material to absorb energy when it is deformed elastically, and release that energy upon unloading.

Organizational resilience (ISO 22316:2017) is the ability of an organization to absorb and adapt in a changing environment.

Organisational resilience (BS 65000:2014) is the ability of an organisation to anticipate, prepare for, respond and adapt to incremental change and sudden disruptions in order to survive and prosper.

Als we vertrekken vanuit de laatste definitie, die iets specifieker is dan de ISO 22316, dan is nog niet geheel duidelijk waar risico en business continuity management passen. Het Security and Continuity (SECO) Institute heeft hieraan een vervolg gegeven en een aantal disciplines samengebracht in wat zij noemen Business Resilience. De definitie daarvan, voortbordurend op de British Standard luidt:

Business Resilience is the ability of an organisation to anticipate, prepare for, detect, respond and adapt to substantial change and sudden disruptions in order to survive and prosper by integrating management systems that build resilience, and develop capabilities for an effective risk response that safeguards

the interests of key interested parties and restores the organization's capabilities.

Business Resilience is de integratie van een aantal disciplines of expertisegebieden, gecombineerd in een gezamenlijke inspanning om de toekomst van een organisatie veilig te stellen in de continu veranderende omgeving waarin deze opereert: de veerkracht van uw organisatie op het moment van een ernstige verstoring. Het gaat hier over het combineren van Risk Management (RM), Information Security en Data Protection (IS & DP), Business Continuity Management (BCM) en Crisis Management (CM) op het juiste niveau, met als doel een optimale uitvoering van de elementen te garanderen. Het is absoluut een uitdaging om de verschillende expertisegebieden optimaal te laten samensmelten, terwijl elk nog steeds in staat moet zijn onafhankelijk te werken. Wie is vervolgens de eigenaar van dit proces? Voor veel organisaties is dit onbekend terrein. Er moet aandacht worden besteed aan samenwerking, informatie-uitwisseling en het juiste niveau van (systeem)integratie.

Deze definitie van Business Resilience is essentieel voor het opbouwen van een veerkrachtige organisatie, want wat de doelen en doelstellingen ook zijn, dit is de kern van elk bedrijf. 'Hoe' en 'Waarom' elementen werden toegevoegd aan de British Standard definitie en de belangrijke term 'detect' werd toegevoegd, daar dit een 'must have' is voor mensen die werkzaam zijn in Information Security. Bij SECO Institute werd het woord 'substantial' in dit geval als een betere match ervaren dan 'incremental'.

De belangrijkste redenen voor het combineren van deze vijf expertisegebieden zijn:

- Deze gecombineerde gebieden hebben al een gemeenschappelijke doelstelling: het beschermen van de activa van de organisatie en het veiligstellen van de toekomst.
- Het koppelen van de inspanningen is een kwestie van consistentie en coördinatie door afstemming, met tal van synergiemogelijkheden.
- De professionals die werkzaam zijn in deze vijf expertisegebieden zullen veel effectiever en efficiënter kunnen functioneren, terwijl zij nog steeds in staat zijn om onafhankelijk te werken en hun onpartijdigheid kunnen behouden voor die zaken waarvoor dit vereist is.

Een veerkrachtige organisatie

Uiteraard kunnen er andere elementen aan Business Resilience worden toegevoegd, bijvoorbeeld op basis van het feit dat organisaties zich in een specifieke branche bevinden. Zo moeten bijvoorbeeld banken rekening houden met specifieke wet- en regelgeving en eisen vanuit De Nederlandsche Bank en andere toezichthouders (bijvoorbeeld EU-regelgeving en Bazel-akkoorden). Twee belangrijke elementen die 'naar voren zijn gekomen' (als gevolg van de Sarbanes-Oxley Act van 2002) naast het reeds behandelde element van Risicomanagement zijn Governance and Compliance. Deze twee moeten ook worden opgenomen, wanneer ze van toepassing zijn. In de voedselindustrie zijn er specifieke kwaliteit en 'food safety manufacturing' regelingen (bijvoorbeeld BRC, IFS en ISO 22000) en 'product fraud' elementen die kunnen worden toegevoegd voor een optimale invulling. In de chemiesector zijn er veel lokale eisen en bijvoorbeeld OSHA-eisen.

Vanuit dit perspectief kan Business Resilience gezien worden als een soort 'Joint Crisis Fighter', zoals de JSF, de nieuwe 'Joint Strike Fighter' (de F-35), die informatie sneller kan verzamelen én delen dan welk ander vliegtuig dan ook. Vanzelfsprekend dien je voorzichtig om te gaan met vergelijkingen, maar het verzamelen en delen van informatie is wel de kern van een veerkrachtige organisatie.

Samenwerken, informatie delen en integratie

Het verzamelen en delen van informatie tijdens bijvoorbeeld een cyberincident, de samenwerking van inspanningen tussen het Crisis Management Team (CMT), het Cyber Security Incident Response Team (CSIRT) en het Business Continuity Management Team (BCMT), is cruciaal en van het grootste belang, net als tijdens elke andere vorm van verstoring die van invloed is op de levering van geprioriteerde producten en diensten. In de ISO 22301:2019 Business Continuity Management Systems – Requirements (hoofdstuk 8.3.4) standaard is een lijst opgenomen van soorten benodigde middelen, die ten minste moeten worden bepaald om geselecteerde strategieën te kunnen implementeren. Dit zijn in ieder geval:

a. mensen;
b. informatie en gegevens;
c. fysieke infrastructuur zoals gebouwen, werkplekken of andere faciliteiten en bijbehorende voorzieningen;
d. uitrusting en verbruiksmaterialen;
e. systemen voor informatie en communicatietechnologie (ICT);
f. transport en logistiek;
g. financiën;
h. partners en leveranciers.

In het geval van een cyberincident zijn er nog een aantal specifieke elementen die op z'n minst ook aandacht verdienen. Dit zijn:

a. beveiliging van (persoonlijke) informatie/gegevens;
b. wet- en regelgeving;
c. merk en reputatie; en
d. communicatie met belanghebbenden en de media.

Bij het over elkaar leggen van deze elementen en daaraan gerelateerde activiteiten over de drie teams die betrokken zijn bij een cyberincident – CMT, CSIRT en BCMT – is het duidelijk dat er elementen en middelen zijn die teamspecifiek zijn. Zo worden merk en reputatie en communicatie met belanghebbenden en media beheerd door de CMT en beveiliging van (persoonlijke) informatie/gegevens door de CSIRT. Aan middelen gerelateerde activiteiten met betrekking tot de fysieke infrastructuur, zoals gebouwen, werkplekken of andere faciliteiten en bijbehorende voorzieningen, uitrusting en verbruiksmaterialen plus transport en logistiek worden beheerd door de BCMT. Alles in overeenstemming met hetgeen hiervoor vermeld aangaande de behoefte – en vaak een vereiste – om zelfstandig, onafhankelijk

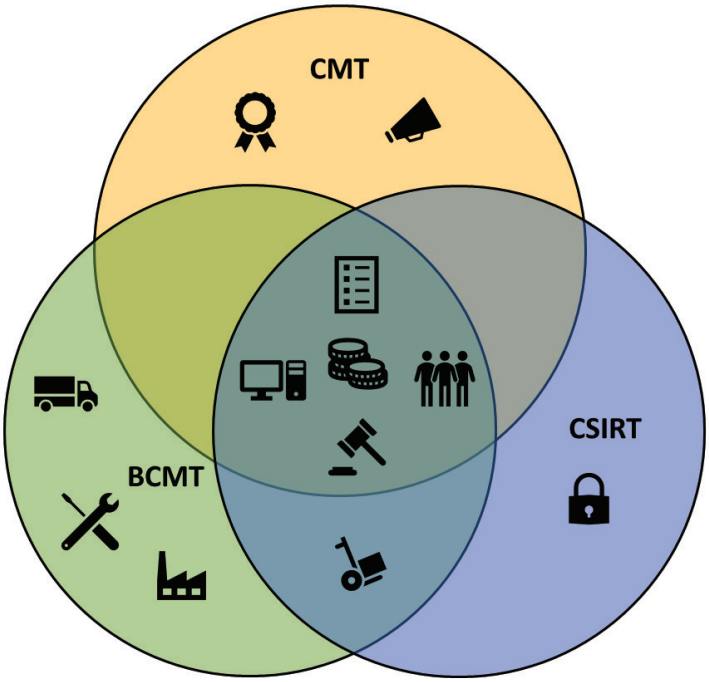
CYBER INCIDENT – SAMENWERKEN, INFORMATIE DELEN EN INTEGRATIE

Elke organisatie kent de volgende typen middelen benodigd voor het leveren van producten en diensten:

- **a) mensen;**
- **b) informatie en gegevens;**
- **c) fysieke infrastructuur zoals gebouwen, werkplekken of andere faciliteiten en bijbehorende voorzieningen;**
- **d) uitrusting en verbruiksmaterialen;**
- **e) systemen voor informatie en communicatietechnologie (ICT);**
- **f) transport en logistiek;**
- **g) financiën;**
- **h) partners en leveranciers.**

In geval van een Cyber Incident is er tevens aandacht voor de volgende zaken vereist:

- **a) Vertrouwelijkheid van (persoons)gegevens;**
- **b) wet en regelgeving (incl. juridisch);**
- **c) merk en reputatie;**
- **d) communicatie met stakeholders en media.**



Figuur 1.

en onpartijdig zaken uit te kunnen voeren. Het is echter compleet duidelijk dat alle andere middelen – en met name zaken als het voldoen aan wet- en regelgeving – betrokkenheid van alle teams vereisen, maar in de meeste gevallen met een ander doel. Dit wordt duidelijk wanneer het gaat om de informatiebehoefte. Zo is informatie over het cyberincident voor het CMT van het grootste belang om het ernstniveau te bepalen en onder meer nodig voor het vaststellen van wat te communiceren aan wie, rekening houdend met wederom fungerende wet- en regelgeving en mogelijke specifieke voorschriften die van toepassing zijn.
Voor het CSIRT is informatie een vereiste voor het proces van detecteren en adequaat reageren, omdat hier hun specifieke verantwoordelijkheid tijdens een cyberincident ligt. Het BCMT heeft informatie nodig om de situatie te beoordelen en het juiste scenario uit te voeren om de levering van producten en/of diensten op aanvaardbare vooraf gedefinieerde niveaus voort te zetten. Het is duidelijk dat het interpreteren en gebruiken van alle gedeelde middelen en elementen nog steeds een specifieke teaminspanning is op basis van hun specifieke vereisten, maar de beschikbaarheid van één unieke set van elk op één plaats is een voorwaarde voor een succesvolle reactie in het geval van, in dit voorbeeld, een cyberincident. Samenwerken, informatie delen en integratie zijn de sleutelwoorden en tegelijkertijd de uitdagingen (zie figuur 1).

Business Resilience Management Systeem

Op basis van de 'wens' om een gedegen bedrijfsbeleid te voeren en onder alle omstandigheden de controle te kunnen behouden, dus inclusief adequaat reageren tijdens een incident, dienen de genoemde vakgebieden te worden samengebracht in één managementsysteem, het Business Resilience Management Systeem, voor een optimalisering van weerstandsvermogen en veerkracht van de organisatie: een 'Resilient Organisation'.

Elke organisatie dient een verantwoordelijke functionaris aan te stellen, waarbij de titel niet van het grootste belang is (Manager, Officer, Hoofd of Coördinator bijvoorbeeld) voor het beheer van de Business Resilience inspanning. Deze functionaris is automatisch de eigenaar van het Business Resilience proces en eventuele tooling die de uitdagingen genoemd in de inleiding grotendeels elimineert. Optimaal is het wanneer deze functionaris rechtstreeks rapporteert aan het juiste C-level. Dit is eigenlijk een voorwaarde voor een succesvolle implementatie en uitvoering, maar wellicht voor menig organisatie nog niet duidelijk. Op deze manier kunnen de belangrijkste redenen voor het combineren van de vijf expertisegebieden, zoals hiervoor vermeld, worden ingevuld en zullen de resultaten snel zichtbaar worden.

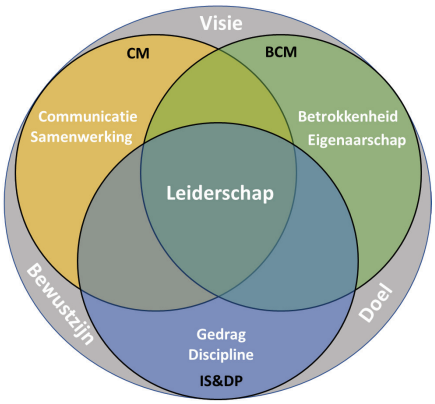
Veel organisaties bevinden zich nog in de ontwikkelingsfase als het gaat om het implementeren van een Business Resilience Management aanpak: slechts een enkeling heeft een managementsysteem ingericht. Het volwassenheidsniveau is dientengevolge nog steeds laag en een uitspraak als 'Business Resilience is ingebed in de manier waarop we hier werken' lijkt vaak nog een brug te ver. Business Resilience is nog steeds een relatief jong vakgebied en organisaties zijn dan ook

op zoek naar richting, ondersteuning en 'best practices' om hun inspanningen te verbeteren en de organisatie verder te brengen. Het implementeren van Business Resilience Management en het creëren van een managementsysteem in elke organisatie met silo's, eilandjes en koninkrijkjes, waarin de vijf expertisegebieden zijn gevestigd, is voor alle betrokkenen een uitdaging. Om in dit geval gebruik te maken van de kracht van herhaling hier nogmaals één van de redenen om dit te doen is: De professionals die werkzaam zijn in deze vijf gebieden van expertise zullen veel effectiever en efficiënter kunnen functioneren, terwijl zij nog steeds in staat zijn om onafhankelijk te werken en hun onpartijdigheid kunnen behouden voor die zaken waarvoor dit vereist is.

Er zijn ongetwijfeld binnen de verschillende vakgebieden in de organisaties verschillende niveaus van bijvoorbeeld automatisering aanwezig. Veel van de huidige informatie is waarschijnlijk opgenomen in Word, Excel, SharePoint en misschien zelfs wel meerdere tools, waarvan sommige ook nog 'zelfgemaakt'. De meeste processen zullen inefficiënt, veel tijd en energie vergen om te implementeren, te onderhouden en te verbeteren. De totale inspanning holt achter de organisatieontwikkelingen en omgevingsverandering aan en rapportages zijn vaak beperkt, onvolledig, inconsistent, soms dubbel en niet tijdig, laat staan op elkaar afgestemd en multifunctioneel inzetbaar en bruikbaar. Voor sommigen een overdreven beeldvorming, maar voor velen helaas herkenbaar. Een fantastische uitdaging voor de Business Resilience functionaris.

De culturele kant van Business Resilience

Een van de grootste uitdagingen waar de Business Resilience functionaris voor staat, houdt echter verband met het op elkaar afstemmen van de culturele kant van Business Resilience. Alle verschillende expertisegebieden zijn gewend om zelfstandig te werken, los van elkaar, zij het in lijn met de missie, visie en doelstellingen van de



Figuur 2.

organisatie – mag men hopen. Risicomanagement is het gemeenschappelijke vakgebied dat alle andere vakgebieden kennen, maar allemaal met een ander doel. Het is ook duidelijk dat Crisis Management een 'apart' gespecialiseerd, meestal gecentraliseerd proces is dat alleen wordt gebruikt wanneer zich een incident voordoet en wanneer men een beroep moet doen op het crisismanagementplan en de installatie van het Crisis Management Team.

Het niveau van 'inbedding' in de organisatie verschilt van zowel Business Continuity Management als Information Security & Data Protection. Business Continuity Management is gedeeltelijk ingebed; het is de combinatie van optimale voorbereiding en handelen en vooral reageren wanneer zich een incident voordoet, leidend tot het activeren en uitvoeren van het Business Continuity Plan. Information Security & Data Protection maakt volledig deel uit van 'Hoe wij hier werken' en is volledig ingebed in de organisatie en het dagelijks handelen. Dit kan van invloed zijn op de governance-aanpak, terwijl dit binnen Business Resilience Management allemaal op elkaar moet worden afgestemd en er geen ruimte meer is voor organisatorische eilandjes of koninkrijkjes. Allen hebben gemeen dat er behoefte is aan focus op visie, doel en bewustzijn, terwijl sterk leiderschap een voorwaarde is voor succes als onderdeel van de rol van de Business Resilience functionaris.

Vanuit cultureel perspectief gaat Crisis Management over communicatie en samenwerking. Het is volledig afhankelijk van het delen van informatie uit alle andere delen van de organisatie in geval van een crisis, daar dit team nagenoeg altijd 'opgesloten' zit in de crisisruimte. Een specifieke Business Continuity Management focus ligt rond betrokkenheid en eigenaarschap. Proceseigenaren moeten de uitvoering van hun herstelactiviteiten aansturen en ze hebben volledige betrokkenheid nodig van alle betrokkenen in de organisatie en veelal ook daarbuiten, te beginnen met het topmanagement. Ook hier zijn het delen van informatie en samenwerking belangrijke succesfactoren. De volledige inspanningen op het gebied cultuur rond de onderwerpen die na aan het hart liggen van de verantwoordelijken binnen Information Security & Data Protection, zijn gericht op het zorgdragen voor het juiste gedrag en de juiste discipline van alle systeemgebruikers. Het delen van (relevante) informatie en samenwerking met alle betrokkenen is ook hier van essentieel belang. (Zie figuur 2).

Optimale integratie

Uit onderzoek onder deelnemers aan een internationaal webinar over dit onderwerp in januari, komt naar voren dat ongeveer veertig procent al op de één of andere manier bezig is om deze vijf vakgebieden met elkaar te verbinden of zelfs 'volledige' integratie nastreeft, zoals in dit artikel bedoeld. Op de vraag of men dit een goede ontwikkeling vindt reageert nagenoeg iedereen positief. Toch is er helaas nog steeds een kleine twintig procent die denkt dat dit niet succesvol gaat zijn, vooral door de culturele hordes die genomen moeten worden, het omhalen van de opgetrokken muurtjes en het uit ivoren torens slepen van betrokkenen. Vandaar de eis dat elke discipline nog steeds in staat moet zijn om onafhankelijk te kunnen blijven werken en de onpartijdigheid moet kunnen behouden voor die zaken waarvoor dit vereist is. Deze eis blijft overeind en is een essentieel onderdeel van de optimale integratie. Dit is de toekomst. Q