Auteur: Gert Kogenhop is directeur van bcm+, een bedrijf dat is gespecialiseerd in training, consultancy en implementatie van business continuity-managementsystemen conform de norm ISO 22301. Hij is voorzitter van Business Continuity Management en Crisismanagement normcommissie bij NEN. Gert is bereikbaar via gk@bcmplus.nl.

CMT, CSIRT, BCMT, de rollen en verantwoordelijkheden

Het aantal cyber security incidenten neemt eerder toe dan af. Kleine, maar ook grote, gerenommeerde organisaties worden getroffen. In eigen land staat ons het ransomware incident bij de Universiteit Maastricht nog helder voor de geest en in de zomer was Garmin volop in het nieuws en zij zijn zeker niet de enigen die dit hebben ervaren. De afhankelijkheid van IT of ICT is enorm, eigenlijk onaanvaardbaar groot.

De harde realiteit is dat bijna niemand alternatieven heeft, bijvoorbeeld een handmatige wijze van werken, in situaties waarbij applicaties, het netwerk of internet niet beschikbaar of bereikbaar zijn, bestanden 'verdwenen' zijn of gecompromitteerd. In ernstige gevallen leidt dit tot een crisissituatie waarbij de samenwerking tussen verschillende disciplines in de (tijdelijke crisis) organisatie van doorslaggevend belang is bij het oplossen van het probleem, adequate reactie en schadebeperking, zowel organisatorisch, financieel alsook met betrekking tot de reputatie.

Elke organisatie wordt blootgesteld aan risico's. Velen zijn vergelijkbaar, zoals ICT-uitval, een bedrijfsbrand, problemen met gas, water en elektra of extreem weer. Anderen zijn specifiek, bijvoorbeeld als gevolg van wat bedrijven of organisaties doen: zoals de chemische industrie, softwareontwikkeling, een bouwbedrijf, datacenter, gemeente of bakkerij. Ook waar organisaties gevestigd zijn maakt een verschil: in de buurt van een luchthaven of naast een rivier, dijk of dam. Of de buurman is bijvoorbeeld een chemische fabriek of een olie-, opslag- of distributielocatie. Risk Management, organisational en operational, is een must en over het algemeen wordt dit redelijk goed beheerst en beheerd (gemanaged). 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 heel specifiek onze (zakelijke) omgeving, verandert in een snel tempo, dus we moeten allemaal voortdurend onze ogen op de bal houden. Voorbeelden zijn de gevolgen van klimaatverandering, Brexit, de handelsoorlog VS versus China, COVID-19 en de niet echt gunstige ontwikkelingen op cybersecuritygebied.

Iedereen afhankelijk van ICT

Tegenwoordig is iedereen afhankelijk van informatietechnologie, of we het nu leuk vinden of niet, en we hebben deze situatie zelf gecreëerd. 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 ICT-gerelateerde disciplines. ICT-afhankelijkheid maakt organisaties kwetsbaar en we kunnen niet wegkijken en doen of het ons niet zal raken. ICT-uitval, niet alleen technisch falen, maar ook niet beschikbaar zijn van applicaties, gegevensbestanden, netwerken en toegang tot internet als gevolg van cybercriminaliteit, veroorzaakt een enorme verstoring en kan voor veel organisaties zelfs fataal zijn. Een kwestie die 25 jaar geleden nauwelijks bestond.

Organisaties kunnen worden geconfronteerd met een crisissituatie als gevolg van een ernstige verstoring, dus Crisis Management en Business Continuity Management zijn voorwaarden voor een goed gemanagede organisatie en in sommige landen zijn deze zelfs verplicht. Onvoorbereid zijn is niet acceptabel en 'We kijken wel als er wat gebeurt' is onmogelijk, onverantwoordelijk en wordt zeker niet beschouwd als een 'good business practice'.

Wat is Business Resilience?

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 soort overkoepelend karakter heeft. Als het gaat over resilience, of vertaald weerstandsvermogen (weerbaarheid) en veerkracht, dan moet deze wel in de juiste context geplaatst worden. Hieronder 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.
- **Organisational resilience (ISO 22316:2017)** is the ability of an organization to absorb and adapt in a changing environment.
- **Organisational resilience (BS65000:2014)** 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 & 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 zo goed mogelijk te laten samensmelten, terwijl iedereen nog steeds in staat moet zijn onafhankelijk te werken. En 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:

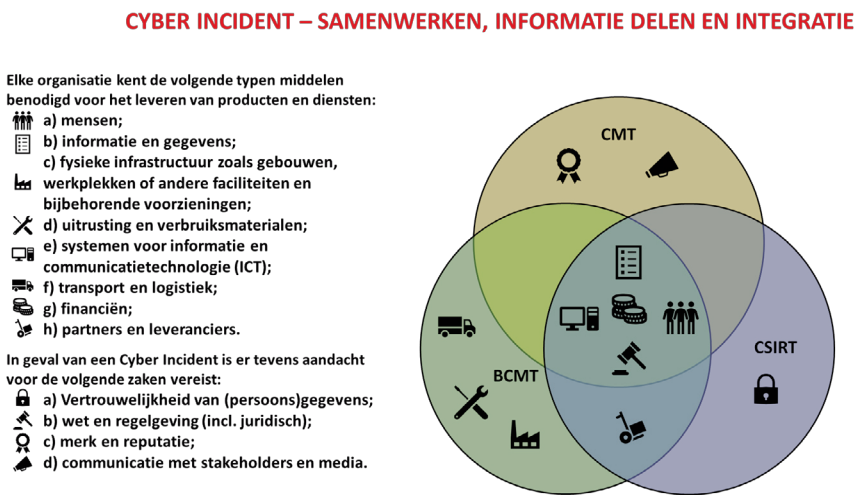
- Deze gecombineerde gebieden hebben al een gemeenschappelijk doelstelling: het beschermen van de kroonjuwelen van de organisatie en het veiligstellen van de toekomst;
- Het koppelen van de inspanningen is een kwestie van consistentie en coördinatie door afstemming, met tal van synergiemogelijkheden;
- 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 zij hun onpartijdigheid kunnen behouden voor die zaken waarvoor dit vereist is.

De kern van een resilient 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). 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, bijvoorbeeld vanuit OSHA.
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 zowel informatie sneller kan verzamelen als 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 in de kern van een resilient organisatie.

Samenwerken, informatie delen en integratie

Het verzamelen en delen van informatie tijdens bijvoorbeeld een cyberincident, de inspanningen tijdens de samenwerking tussen het Crisis Management Team (CMT), het Cyber Security Incident Response Team (CSIRT) en het Business Continuity Management Team (BCMT), zijn 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 implementeren. Zie figuur 1.



Figuur 1 – Samenwerken, informatie delen en integratie.

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 team-specifiek zijn. Zoals merk, reputatie en communicatie met belanghebbenden en media, die worden beheerd door de CMT. Beveiliging van (persoonlijke) informatie/gegevens worden beheerd door de CSIRT en 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 over de behoefte, en vaak zelfs een vereiste, om zelfstandig, onafhankelijk 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 om onder meer vast te stellen 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, daar hier hun specifieke verantwoordelijkheid ligt tijdens een cyberincident. 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 kunnen 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 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 (blijven) behouden, dus inclusief adequaat reageren tijdens een incident, dienen de genoemde vakgebieden te worden samengebracht in één managementsysteem, het Business Resilience Management Systeem.

Veel organisaties bevinden zich nog in de ontwikkelingsfase als het gaat om het implementeren van een Business Resilience Management aanpak

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. Optimaal is het wanneer deze functionaris rechtstreeks rapporteert aan het juiste C-level in de organisatie. Dit is eigenlijk een voorwaarde voor een succesvolle implementatie en uitvoering, maar wellicht voor menig organisatie nog niet volledig duidelijk. Een sponsor op C-level is wel het minste en wie dat dan moet zijn hangt af van het soort bedrijf. Voor een bank of verzekeraar ligt dit vaak op het bordje van de Chief Information Officer of Chief Risk Officer, terwijl dit in de maak- of bijvoorbeeld voedingsindustrie, waar dit soort functies op een ander niveau opereren, de Chief Financial Officer of Chief Operating Officer blijkt te zijn.

Uitdaging

Veel organisaties bevinden zich nog in de ontwikkelingsfase als het gaat om het implementeren van een Business Resilience Management aanpak en slechts een enkeling heeft een managementsysteem ingericht. Het volwassenheidsniveau is daardoor nog steeds laag en een uitspraak als "Business Resilience is ingebed in de manier waarop we hier werken" lijkt een brug te ver voor velen. Business Resilience is nog steeds een relatief jong vakgebied en organisaties zijn 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: 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 fantastische uitdaging voor de Business Resilience functionaris.

Uit een recent onderzoek onder deelnemers aan een webinar over dit onderwerp komt naar voren dat ongeveer 40% al op de één of andere manier bezig is om deze vijf vakgebieden met elkaar te verbinden of zelfs 'volledige' integratie nastreeft zoals hier bedoeld. Op de vraag of men dit een goede ontwikkeling vindt, reageert nagenoeg iedereen: "Dit is de toekomst, daar is geen twijfel over mogelijk". Waarvan akte.