In-Secure Secure – Onzekerheid, enige zekerheid (I)

Verontrusting en angst voor Cyber In-Security groeit toenemend sterker. Zoals meerdere (BCM Academy eigen) expertbronnen, maar ook het World Economic Forum (WEF) eerder dit jaar, maar nu actueel wederom het dreigings niveau heeft bijgesteld, wordt nadrukkelijk gewezen op de toenemende afhankelijkheid van organisaties, economieën binnen de digitale connectiviteit en digitale informatie, waaronder cyberaanvallen en gegevensfraude als de derde en vierde meest ernstige bronnen van mondiale risico's in 2018.

Terwijl systematische dimensies van Cyber risico's steeds duidelijker worden, is het begrip van hoe een grootschalige crisis eruit kan zien en hoe het moet worden behandeld toenemend onduidelijker aan het worden. Er kunnen echter belangrijke lessen worden getrokken uit eerdere manifeste disruptie systemen (Crisis Systems) en theoretische projecties en analyses van eerdere 'ontwrichtingen. Historische perspectieven dwingen om juist het goede te gebruiken om scenario's duidelijker te maken. Zoals de 'learnings' uit de financiële meltdowns uit het afgelopen decennium.

Er zijn opvallende analogieën tussen het internet, digitale veiligheid en het wereldwijde financiële systeem. Kortom, beide zijn nauw met elkaar verbonden netwerken die levensaders bieden aan de 'economie', via de overdracht van informatie, financiering en alle uitwisselingen van 'geld en goed'. Kortom; het is wijs om vanuit Business Continuity Management Perspectief de licence to operate op de horizon te blijven houden, daarom is het wijs juist nu binnen beleid nadrukkelijk die dimensies te plaatsen. De systeemtechnieken kennen we wel, nu de bestuurlijke technieken nog.

Cyber security, cyber risico's en gegevens(fraude) vormen een vaste set binnen de modulaire opbouw van BCM Academy. Een 'eigen future view' projecteren op de in-securities binnen eigen omgeving(en) om vervolgens begrip te verkrijgen is wijs. Bestuur binnen beleid, onze professie, schept de organisatorische uitdaging.

"BCM Academy kent het kennen en herkennen."

Van corrigeren naar mitigeren

Maatregelen van overheidswege, nieuwe normenkaders en striktere beleidskaders helpen in mate 'noodzakelijke' stappen te nemen om Business Continuity Management sterker 'positie' te geven. Maar hebben onvoldoende correctiekracht om resilience (weerbaarheid) als voorwaarde van beleid binnen organisaties 'af te dwingen'.
Bovendien loopt de snelheid van afstemming op actualiteit en de projectie op de toekomst veelal asynchroon met de uiteindelijke maatregelen.

Er is evenwel de laatste periode veel gerichte regelgeving ingevoerd, terwijl vele nieuwe andere worden opgesteld en voor invoering en activering op de rol staan.

Binnen de Europese Unie legt de veelbesproken algemene verordening inzake gegevensbescherming (GDPR) progressieve boetes op aan bedrijven die de vertrouwelijkheid van persoonsgegevens in gevaar brengen. Gerichte mandaten voor de openbaarmaking van schendingen van zowel autoriteiten als betrokkenen is een 'voorschrijvende verplichte' van en voor opvolging. Echter daarmee is de 'synchroniciteit' nog niet geborgd en lopen organisaties nog steeds niet in de pas.

Beheren of Beheersen

De richtlijn betreffende de beveiliging van (NIS), netwerken en informatiesystemen en NOS, (Netwerk Operating Systemen) introduceert Cyber beschermingseisen en incident openbaarmakingsverplichtingen voor belangrijke spelers in sectoren zoals energie & utilities, finance & banking en gezondheidszorg, pharma & life science. Voorstellen, nu actueel voor regelgeving (2018) van de Europese Commissie voorziet in een EU-breed kader voor veiligheidscertificering van hardware en software, gevormd na de beruchte strikte CE-regeling voor onder andere veiligheid, gezondheid en milieubescherming.

Noodzakelijke stappen, maar lang niet voldoende om integraal Business Continuity Management effectief te plaatsen. Ondertussen kan beschikt worden over normenkaders, ISO (2018) Crisis Management (223300), de 45001 (safety en health) en de aanvullingen op ISO 22301 (Business Continuity Management) welke beleidsmatig kunnen 'borgen & beheersen', maar tussen denken en doen blijft een kloof bestaan.

De effecten van bijvoorbeeld GDPR en NIS (Netwerken en Informatie-Systemen) zijn beperkt tot bepaalde gevallen of sectoren. Tot nu toe zijn er (nog) geen algemene beginselen, criteria of parameters vastgesteld voor de verdeling van de aansprakelijkheid wanneer aanvallers hun uiteindelijke doel raken door gebruik te maken van/door inzet (middels) derden kwetsbaarheden, zoals tijdens een DDoS-aanval. Het is duidelijk dat er meer werk en beheersmaatregelen nodig zijn binnen deze onderwerpen. Immers de 'basale management aansprakelijkheden' blijven overeind, schuld, of geen schuld. Dus zou deze beheersmaatregelen in elk geval op de bestuur(der)s agenda dienen te staan.

"BCM Academy kent het kennen en herkennen"