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 en genoeg 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.