Nieuwe soorten van calamiteiten, crises en rampen zijn manifest geworden. Bijna allemaal zijn deze vanuit een beleids effectieve 'Push' binnen Business Continuity Management opgenomen om de weerbaarheid te verhogen en de afhankelijkheden & kwetsbaarheden te verlagen.

Er is relatief gezien voldoende kennis, vaardigheid en besef welke aangewend kan worden als we spreken van 'traditionele' bedreigingen en disrupties binnen het primaire proces van organisaties. Opvallend is echter dat het 'cyberdomein' op zichzelf al een 'black hole' is op de wijze waarmee organisaties hun weerbaarheid trachten te verhogen.

Bij natuurrampen, de 'Acts Of God', calamiteiten en disrupties binnen de interne en externe fysieke omgeving van organisaties en door de mens veroorzaakte crises kan een effectief stelsel van maatregelen de risico's vermijden, effectief bestrijden en/of van voldoende afweer voorzien.

Opvallend is dat volgens de laatste uitkomsten van de expert analyses binnen het 'cyber crisis' domein en de praktijkanalyse van BCM Academy er een dominante logic zou zijn die evenals alle andere bedreigingen en door de mens veroorzaakte 'crises' er ook voldoende potentieel aanwezig is om 'cyber crisis' te voorkomen.

Organisaties, communities en individuen bezigen nog steeds de dominante denk-richting door oplossingen centraal te plaatsen en instrumenten te gebruiken om de veiligheid te vergroten. Voor nu, maar ook in de toekomst gaat het echter daar niet langer om. De focus zal aangebracht dienen te worden om juist een stelsel te creëren en te implementeren welke agencies, organisaties, individuen en onze manier van leven ('Ways Of Life' en Ways Of Working') kunnen beschermen en disorders kunnen voorkomen.

'CyBerHyPer' laat zich omschrijven als een soort 'debunking' (ontmaskering) van oorzaak & gevolg door uiterst dynamisch met het begrip 'cyber' om te gaan. Wetenschappers worstelen nogal met de prefix, het voorvoegsel, 'cyber', zeker omdat de academische absurditeit van de terminologie discursieve coördinaten oproept evenals het begrip 'virtueel'. Immers, every body goes Cyber, Virtual, Hybrid en Nano. Zonder twijfel zal het toenemend nog vaker gecanoniseerd worden en 'sweeping' gegeneraliseerd worden.

Niettemin zal dit niets afdoen aan de crux om met CyBerHyPer de positie enplaats te bepalen binnen elke vorm van segmentatie binnen het domein en juist ook los te denken van enkel push oplossingen en gefragmenteerde (detail)technologie. Zeker nu heeft het begrip 'vermijden' een belangrijkere lading gekregen ten opzichte van recovery. Puur illustratief is het feit dat met de groei van BYOD,(bring your own device), IoT, (internet van de dingen) en de uitbreiding van gedistribueerde servers, IT-beveiliging niet in staat is geweest om bij te blijven. De traditionele perimeters zijn niet meer voldoende en zelfs diepgaande defensieve maatregelen werken niet. Veel deskundigen vinden dat micro-segmentatie is een nieuwe strategie zal worden. De dreiging van een exponentieel toenemende eindpunten maakt niet alleen het aanval oppervlak groter, maar ook het aantal devices buiten het 'netwerk', de perimeter. Bij het in gedrang komen daarvan wordt de 'dreiging vector' vermenigvuldigt.

Vanuit de tradionele push van gegevensbeveiliging zal nadrukkelijker de focus aangebracht dienen te worden op de pull van het totale gebruikersveld en structureel integratie van beleid tot oplossingen gebracht dienen te worden die naadloos acteren en reageren vanuit een offensieve inzet en dus geen defensieve.

> *"Some people don't like change, but you need to embrace change if the alternative is disaster "*- Elon Musk

Cyber Disaster Planning en Cyber Crisis Management kunnen een belangrijke bijdrage leveren aan de vergroting van de weerbaarheid echter dan wel met het doel dat verankering plaats heeft op Strategisch/tactisch niveau en integraal onderdeel uitmaakt van de brede(re) Business Continuity Management inrichtings- en werkings gebieden. Het opzoeken van geprojecteerde 'doodlopende' wegen horen daarbij en traditionele segmentaties dienen geïsoleerd te worden simpelweg omdat het te foutgevoelig, tijdrovend en veelal geldverslindend is.

'Some people don't like change, but you need to embrace change if the alternative is disaster' - Elon Musk. Sommige mensen houden niet van verandering, maar je moet verandering omarmen als het alternatief een ramp is.