Auteur: Jelle Groenendaal is lector Risk Management & Cybersecurity aan de Haagse Hogeschool en adviseert als zelfstandig adviseur publieke en private organisaties over risico- en crisismanagement. Hij is bereikbaar via j.groenendaal@hhs.nl.

Cybercrises vragen om anticipatie en improvisatie

De ransomware-aanval op de Universiteit Maastricht (2019) en de wiperware-aanval op Maersk (2017) hebben pijnlijk aangetoond dat grote incidenten niet te voorkomen zijn en zelfs kunnen uitmonden in een cybercrisis. De mate waarin organisaties in staat zijn om de impact van cybercrises te beperken, wordt onder andere bepaald door de bedrijfscontinuïteit- en crisismanagement organisatie. Maar hoe richt je deze beheersmaatregelen adequaat in?

Het nieuwe Lectoraat Risk Management & Cybersecurity van de Haagse Hogeschool gaat deze en andere vragen op het snijvlak van risicomanagement en cybersecurity de komende vier jaar onderzoeken. In dit artikel geven we alvast een eerste reflectie op basis van een aantal bekende wetenschappelijke inzichten. De malware-aanval op de Universiteit Maastricht en de wiperware-aanval op scheepvaart- en transportgigant Maersk hebben onomstotelijk duidelijk gemaakt dat cyberincidenten dermate veel impact kunnen hebben op de bedrijfsvoering dat er gesproken kan worden van een cybercrisis. Een cybercrisis definiëren we als uitval, verstoring of misbruik van IT-systemen en/of diensten die het voortbestaan, integriteit en/of reputatie van de organisatie bedreigt en waarbij er onder (een perceptie van) tijdsdruk en onzekerheid besluiten genomen moeten worden. Naast grote impact op de organisatie, kan een cybercrisis een verstorende invloed hebben op maatschappelijke processen. In het uiterste geval zou een cybercrisis volgens de NCTV kunnen leiden tot maatschappelijke ontwrichting. Ter illustratie: door de aanval op Maersk raakte de Rotterdamse APM Terminals bijvoorbeeld volledig buiten bedrijf, waardoor schepen moesten uitwijken en er in de haven bijna een verkeersinfarct ontstond (1).

Impact beperken

De cyberweerbaarheid van organisaties wordt bepaald door hun vermogen om cyberincidenten te voorkomen en (als ze zich voordoen) de impact ervan te beperken. Nu partijen zoals de NCTV steeds nadrukkelijker stellen dat grote cyberincidenten niet voorkomen kunnen worden (2), moeten organisaties zich in toenemende mate gaan toeleggen op het treffen van maatregelen om de impact te beheersen. Bedrijfcontinuïteitsmanagement (BCM) en crisismanagement zijn twee beheersmaatregelen die daarvoor bedoeld zijn. BCM is het proces gericht op het beheersen van dreigingen die kunnen leiden tot verstoringen en daarmee tot het niet meer kunnen leveren van producten of diensten op aanvaardbare, vooraf vastgestelde niveaus (3). Hiertoe worden de dreigingen en belangrijkste organisatieprocessen in kaart gebracht en vervolgens bepaalt hoe de continuïteit in het geval van een verstoring gewaarborgd kan worden. Dit wordt beschreven in een zogeheten bedrijfscontinuïteitsplan waarin voor een aantal scenario's een handelingsperspectief wordt geschreven. Denk hierbij aan wat te doen bij de uitval een kritisch IT-systeem door een patch of bij de onbeschikbaarheid van een kantoorgebouw door brand. Crisismanagement kan gedefinieerd worden als het vermogen van organisaties om zich voor te bereiden en te reageren op een (cyber)crisis en daarvan te herstellen (3). Crisismanagement komt in beeld wanneer het bedrijfscontinuïteitsplan niet afdoende is of ontbreekt voor de situatie waarmee de organisatie geconfronteerd wordt. De huidige coronacrisis is een treffend voorbeeld: veel organisaties hadden geen rekening gehouden met een lockdown en daarmee de noodzaak om grote delen van het personeelsbestand thuis te kunnen laten werken. Een crisismanagementteam kan in dat geval besluiten om de capaciteit thuiswerkplekken uit te breiden en thuiswerken te faciliteren.

Noodzakelijk onderzoek naar BCM

Veel van de kennis die voor de inrichting, besturing en organisatie van informatiebeveiliging gebruikt wordt, is afkomstig uit (internationale) standaarden. Dit geldt ook voor BCM en crisismanagement. Denk aan de ISO 22301 of BCI 'Good Practice Guidelines' voor BCM en de BS 11200 of TS 17091 voor crisismanagement. Deze standaarden worden wereldwijd door vele organisaties gebruikt en zijn ontwikkeld door professionals die veel ervaring hebben in het vakgebied. Naar de werking en effectiviteit van deze standaarden is nog niet veel onderzoek verricht. Daarmee is tot op heden niet aangetoond dat het implementeren van dergelijke standaarden leidt tot een hogere continuïteit of beter beheerste (cyber)crisis. Empirisch onderzoek binnen organisaties naar het functioneren en de effectiviteit van BCM en cybercrisismanagement is schaars. Toegepast onderzoek is daarom noodzakelijk om te achterhalen in hoeverre en hoe organisaties zich adequaat kunnen voorbereiden en reageren op cybercrises.

Dat er eigenlijk nog maar weinig toegepast onderzoek gedaan is naar de werking en effectiviteit van BCM en cybercrisismanagement binnen organisaties, neemt niet weg dat er al een aantal voorlopige bevindingen kunnen worden gedaan op basis van bestaand onderzoek. In dit artikel geven we hiervan enkele voorbeelden.

BCM is in theorie vooral geschikt voorspelbare risico's (4). BCM is gebaseerd op de klassieke managementtheorie die veronderstelt dat de wereld en daarmee organisaties in grote mate voorspelbaar en (daardoor) beheersbaar zijn. Het instrumentarium van BCM is er dan ook op gericht om organisatieprocessen en (kenbare) risico's in kaart te brengen en vervolgens maatregelen te nemen die helpen om de continuïteit te waarborgen als zo'n vooraf geïdentificeerd risico zich opeens manifesteert. Voorbeelden van deze kenbare risico's zijn een bedrijfsgebouw dat tijdelijk

niet gebruikt kan worden door brand of een niet functionerend betalingssysteem door de uitval van een server.

Anticiperen op een cybercrisis

BCM kan bruikbaar zijn om organisaties voor te bereiden op een scenario waarbij producten of diensten door een cyberincident tijdelijk niet of niet op tijd geleverd kunnen worden. Zo kan er bijvoorbeeld een draaiboek worden gemaakt voor wat te doen bij een grootschalige ransomwarebesmetting of DDoS aanval. Hierbij zijn een aantal aandachtspunten van belang. Ten eerste moet bedacht worden dat veel bedrijfscontinuïteitsplannen handelingsperspectieven bevatten die uitgaan van de veronderstelling dat het netwerk en de reguliere communicatiemiddelen zoals e-mail en telefoon beschikbaar blijven tijdens een verstoring. Maersk heeft aangetoond dat een cyberincident kan leiden tot een complete uitval van het IT-netwerk en systemen. Daardoor kon er geen gebruik gemaakt worden van e-mail en telefonie (die afhankelijk zijn van het netwerk) met als gevolg dat het merendeel van de plannen niet uitgevoerd kon worden. Hetzelfde zou kunnen gebeuren wanneer een netwerk gecompromitteerd is en daardoor de communicatie niet meer te vertrouwen is. Ten tweede en voortbouwend op het vorige punt, is dat veel bedrijfscontinuïteitsplannen digitaal worden opgeslagen en bij een mogelijke uitval van het netwerk dus niet meer benaderd kunnen worden. Ten derde moet rekening gehouden worden met het risico dat back-ups besmet kunnen worden met kwaadaardige software die zich bijvoorbeeld drie maanden stilhoudt zodat er geen mogelijkheid meer bestaat om terug te gaan naar een schone versie (tenzij de back-ups nog langer teruggaan en/of er nog offline back-ups zijn gemaakt). Ten vierde moet bij een scenario van een grote ransomwarebesmetting rekening gehouden worden met de belasting voor de IT-organisatie om een groot aantal werkstations op te schonen en opnieuw in te spoelen.

De tweede bevinding is dat een planmatige respons die BCM kenmerkt alleen effectief kan zijn wanneer die respons met enige regelmaat beoefend en uitgevoerd wordt (5). De consequentie van deze bevinding is tweeledig. Ten eerste betekent het dat BCM vooral geschikt is voor (kleinere) risico's die zich met enige regelmaat manifesteren, zodat er een feedbackloop kan ontstaan tussen plan en uitvoering en de plannen niet verworden tot 'papieren tijgers'. Ten tweede betekent het dat BCM zich maar kan richten op een beperkt aantal risico's, omdat de tijd die nodig is om plannen te testen begrensd is. Een goede BCM organisatie beperkt zich daarom op een aantal meest voorkomende (kenbare) risico's en zorgt ervoor dat inzichten uit testen, oefeningen en echte incidenten verankerd worden in de plannen en trainingen voor personeel.

Snel veranderende omgeving

BCM kent echter ook een aantal beperkingen. De derde bevinding is dat BCM minder geschikt is voor organisatieomgevingen die aan veel verandering onderhevig zijn. BCM legt veel nadruk op het documenteren van organisatieprocessen en het vastleggen van een responsstrategie die past bij hoe de organisatie op papier beschreven is. In de praktijk blijkt echter dat die omschrijving vaak niet meer actueel is op het moment dat er een verstoring optreedt. IT-systemen zijn bijvoorbeeld uitgefaseerd of juist in productie genomen, bepaalde sleutelpersonen zijn door een reorganisatie niet meer werkzaam in de organisatie of een leverancier is vervangen. Hoewel in het bedrijfscontinuïteitsmanagementsysteem (BCMS) in de regel wordt opgenomen dat plannen jaarlijks herzien moeten worden of vaker bij grote veranderingen, lijkt de organisatiepraktijk weerbarstiger (4). Sommige organisaties en hun omgeving zijn zo aan verandering onderhevig, dat het ondoenlijk is om te allen tijde een actueel en diepgaand beeld te hebben van alle kritieke processen. In dergelijke omgevingen loopt BCM vaak achter de feiten aan en is veel van het voorbereidingswerk verspilde moeite.

Zwarte zwanen

Naast de kenbare, kleine risico's zijn er ook nog een aantal bedreigingen die zich niet vooraf laten kennen. Donald Rumsfeld noemde deze 'unknown unknowns', ofwel impactvolle, onvoorspelbare gebeurtenissen die per definitie buiten het bereik van risicobeheersing en dus BCM liggen. De vierde bevinding is dan ook dat BCM niet goed overweg kan met wat Nassim Nicholas Taleb 'zwarte zwanen' noemt. Eén van de eerste stappen van BCM is het identificeren van bedreigingen en bepalen in hoeverre deze dreigingen een risico voor de organisatie vormen. Grote, impactvolle gebeurtenissen laten zich echter niet altijd adequaat voorspellen. De huidige coronacrisis laat dit fraai zien. Grieppandemieën komen zo om de paar jaar voor, maar de huidige wereldwijde reactie met grootschalige lockdowns en reisrestricties zijn nog nooit eerder

vertoond. In de laatste vijf jaarrapportages van de Global Risk Rapportage van het World Economic Forum (WEF) - voor risicomanagers een belangrijke bron - stond infectieziekte dan ook niet in de top 10 van meest waarschijnlijke grote risico's. In de laatste editie van 2020 bungelde infectieziekte onderaan de ranglijst van risico's met grootste impact. Saillant detail: COVID-19 of corona komen helemaal niet voor in het op 15 januari 2020 gepubliceerde rapport (6).

Een belangrijke beperking van een planmatige respons is bovendien dat de plannen weinig houvast bieden wanneer de werkelijkheid anders is dan in het plan beschreven wordt. Als bij een cyberaanval de systemen veel langer platliggen dan van tevoren verwacht, of er treden onverwachte cascade-effecten op, zal de organisatie dus ter plekke inzicht moeten krijgen in het probleem en een responsstrategie moeten bepalen en uitvoeren. Dit is het domein van (cyber)crisismanagement.

Improviseren als een jazzmusicus

Crisismanagement helpt de organisatie om snel expertise en mandaat bij elkaar te brengen en (zodoende) betekenisvolle beslissingen te nemen. Crisismanagement speelt zich veelal op drie niveaus af: operationeel (bijvoorbeeld in het SOC of CERT), tactisch (hoofd CERT) en strategisch (CISO) (7). Hoewel naar cybercrisismanagement nauwelijks onderzoek is verricht, kunnen er wel op basis van de algemene literatuur over crisismanagement een aantal conclusies worden getrokken. Ten eerste blijkt uit onderzoek dat professionals onder crisisomstandigheden terugvallen op routinegedrag en daardoor doen wat ze altijd al deden (5). Een belangrijke aanbeveling is dan ook om de (cyber)crisisorganisatie zoveel mogelijk te laten aansluiten op de reguliere organisatie en van mensen tijdens crises geen contra-intuïtieve handelingen te verwachten c.q. te vragen. Dat mensen tijdens crises terugvallen op ingesleten gewoonten, verklaart waarom uit evaluaties vaak blijkt dat crisisdraaiboeken en specifieke crisisplannen niet of nauwelijks geraadpleegd zijn in de acute fase van crises. De waarde van dergelijke plannen zit hem dan ook vooral aan de 'voorkant': tijdens het opstellen maken ze experts en management bewust van hun rol, taken en verantwoordelijkheid tijdens een cybercrisis.

Uit de literatuur blijkt dat improvisatie tijdens crises onvermijdelijk is (8). In sommige gevallen zullen medewerkers namelijk geen routine hebben opgebouwd voor de situatie waarmee ze geconfronteerd worden of voldoet die routine simpelweg niet. Bij Maersk waren bijvoorbeeld ook verschillende vormen van improvisatie zichtbaar: bij een gebrek aan IT boekte de organisatie nieuwe orders in via WhatsApp en Gmail, bedacht het een offline systeem om containers te labelen en stampte het binnen enkele weken een totaal nieuw IT-netwerk uit de grond (9).

Improviseren heeft dikwijls een negatieve connotatie. Voor sommigen suggereert improvisatie dat de organisatie niet voorbereid was en beter voorbereid had kunnen zijn op een bepaalde verstoring. In de wetenschappelijke literatuur wordt er echter veel genuanceerder naar improvisatie gekeken. Improvisatie wordt gezien als een noodzakelijke vaardigheid van mensen en organisaties om adequaat te kunnen reageren op onverwachte kansen en bedreigingen (10). Het is een misvatting dat improvisatie geen voorbereiding vergt. In de wetenschappelijke literatuur wordt vaak de analogie van de jazzpianist gebruikt. Jazzpianisten kunnen pas improviseren – dat wil zeggen afwijken van de standaard – wanneer zij die standaard tot in de finesses beheersen (10). In de context van crisismanagement betekent dit bijvoorbeeld dat crisismanagementteams regelmatig 'standaard' crisisscenario's oefenen, maar ook de afwijkingen daarop. En leren strategische crisismanagementteams dat veel besluiten tijdens crises 'in de frontlinie' genomen worden en hoe zij die besluitvorming zo goed mogelijk kunnen faciliteren en waar nodig bijsturen.

Wees bewust van besluitvormingsvalkuilen

(Cyber)crises worden gekenmerkt door tijdsdruk, onzekerheid en de grote belangen die op het spel staan. Een derde conclusie is dat de literatuur laat zien dat professionals onder deze omstandigheden in de meeste gevallen adequate beslissingen nemen, maar ook vatbaar zijn voor besluitvormingsvalkuilen (5). Die valkuilen zijn van toepassing op ieder niveau – operationeel, tactisch en strategisch – al manifesteren ze zich soms op een andere manier. De betekenis voor de cybercrisismanagementpraktijk is dat crisismanagers bewust moeten zijn van deze valkuilen in hun eigen besluitvorming en die van hun ondergeschikten. Bekende valkuilen zijn de confirmatiebias (de neiging om een initieel gevormde hypothese te bevestigen door alle gekregen informatie als zodanig te interpreteren en vervolgens uitsluitend te zoeken naar aanwijzingen die de hypothese bekrachtigen) en gezonken kosten (de neiging om een taak die de eindfase nadert af te willen maken

Help mee bij het vormgeven van het onderzoeksprogramma

Moet het onderzoek zich de komende jaren vooral richten op supply-chain risico's en cascade-effecten? Of op de effectiviteit van security standaarden voor industrial control systems? Of zou het goed zijn als de kosten-baten van cyberinvesteringen beter wordt onderbouwd door middel van feiten? Geef je mening in de vragenlijst die het Lectoraat Risk Management en Cybersecurity heeft ontwikkeld. Deze vragenlijst is bedoeld om input vanuit het werkveld op te halen. De resultaten worden gebruikt bij het vormgeven van het vierjarige onderzoeksprogramma van het lectoraat. Het invullen van de vragenlijst kost slechts 5 minuten: https://bit.ly/2XHN7iP

omdat er veel tijd in heeft gezeten). Deze biases kunnen bijvoorbeeld optreden bij CERT professionals die bij een groot incident te lang een bepaalde hypothese proberen te bekrachtigen. Het is aan cybercrisismanagers om deze valkuilen te (h)erkennen en hier op te sturen.

Meer onderzoek nodig naar BCM

In dit artikel hebben we op basis van de wetenschappelijke literatuur enkele BCM en cybercrisismanagement inzichten beschreven. Wie de impact van cybercrises wil beperken, moet volgens de literatuur inzetten op anticipatie (BCM) en improvisatie – wat met behulp van crisismanagement kan worden gefaciliteerd en bijgestuurd. Velen vragen blijven echter nog onbeantwoord en meer toegepast onderzoek is nodig. Een paar voorbeelden: hoe zien effectieve BCM en cybercrisismanagementoefeningen eruit? Hoe ziet een robuuste cybercrisismanagementorganisatie eruit? Hoe kun je BCM slim automatiseren zonder concessies te doen aan de effectiviteit? In welke mate helpen besluitvormingsmodellen bij het voorkomen van besluitvormingsvalkuilen door cybercrisismanagementteams? Wat is de rol van de CISO in crisismanagement? Het lectoraat Risk Management & Cybersecurity hoopt deze en andere vragen de komende jaren samen met het werkveld te kunnen onderzoeken.

Referenties

(1) Van Duin, M. Maan, J. (2018). Cyberaanval op Maersk. Lessen uit crises en mini-crises 2017. Instituut Fysieke Veiligheid: Arnhem.

(2) NCTV (2020). Cybersecuritybeeld Nederland 2020.

(3) NVN-CEN/TS 17091: 2018. Crisismanagement – Handreiking voor het ontwikkelen van strategisch vermogen.

(4) Groenendaal, J. Helsloot, I. (in druk). Organizational Resilience: Shifting from a planning driven Business Continuity Management to Anticipated Improvisation. Journal of Business Continuity & Emergency Management.

(5) Groenendaal, J. Helsloot, I. (2016). The application of Naturalistic Decision Making (NDM) and other research: lessons for frontline commanders. Journal of Management and Organization, 22(2), 173.

(6) Van der Linden, L. (2020). Wat kunnen we met risicomanagement leren van virusinfecties die al dan niet uitgroeien van een pandemie. Genootschap voor Risicomanagement.

(7) Groenendaal, J. Helsloot, I. Scholtens, A. (2013). A critical examination of the assumptions regarding centralized coordination in large-scale emergency situations. Journal of Homeland Security and Emergency Management. 10(1), 113-115.

(8) www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

(9) Mendonca, D. Wallace, W.A. (2004). Studying organizationally-situated improvisation in response to extreme events. International Journal of Mass Emergencies and Disasters, 22(2), 5-30.

(10) Weick, K. E. (1998). Introductory essay – improvisation as a mindset for organizational analysis. Organization Science. 9(5), 543.