Een plan is nog geen crisisrespons

Zes vaardigheden die bepalen hoe een team een cybercrisis doorstaat en waarom ze zich niet door lezen, maar door oefening laten ontwikkelen.

Kaja Möller, CyberMaster

Samenvatting

Voor veel organisaties is een ernstig cyberincident eerder een kwestie van wanneer dan van of. In de voorbereiding ligt de nadruk daarbij vaak op de techniek en minder op de mensen die moeten beslissen wanneer die techniek faalt. Dit artikel richt zich op die mensen. Het beschrijft zes vaardigheden die bepalen hoe een team een cybercrisis doorstaat: overzicht behouden, beslissen op onvolledige informatie, prioriteren onder tijdsdruk, kalm blijven onder druk, improviseren en veerkracht. Elk van deze zes is verankerd in wetenschappelijk onderzoek naar crisis, besluitvorming en gedrag onder druk. Het artikel zet uiteen wat dat onderzoek aantoont, waarom het zich laat vertalen naar de cybercrisis en waarom deze vaardigheden zich niet door erover te lezen laten ontwikkelen, maar door oefening onder realistische druk. Het model is praktijkgedreven en brengt bestaande onderzoeken samen.

1. De crisis die zich niet aan de IT-afdeling laat uitbesteden

Wanneer systemen zijn uitgevallen, de eerste persvragen binnenkomen en een aanvaller losgeld eist, moeten mensen onder hoge druk beslissen. Op papier ligt vast wie welk besluit neemt. In de vergaderkamer zelf is die verdeling van verantwoordelijkheden vaak minder eenduidig. Dat geldt zowel bij aanvallen als bij een omvangrijke storing, een datalek of de uitval van een kritieke leverancier. Wanneer een situatie de organisatie ontregelt wordt er besluitvaardigheid onder druk verwacht. Wat wordt getest is dus niet alleen de technische oorzaak, maar juist ook het menselijke handelen eromheen.

Op dat moment wordt duidelijk waar een cybercrisis werkelijk om draait. De bepalende vragen zijn niet uitsluitend technisch van aard. Zij betreffen de afweging of klanten worden gewaarschuwd voordat zekerheid bestaat, welke informatie naar buiten wordt gebracht, of er aan criminelen wordt betaald en wie tot dat besluit bevoegd is. Deze vragen worden doorgaans niet beantwoord in een technisch document. Zij horen thuis in de bestuurskamer.

De veronderstelling dat cyberveiligheid alleen een aangelegenheid van technische specialisten is, houdt hardnekkig stand. Zodra een incident zich voordoet, verschuift het zwaartepunt echter van de techniek naar de mens. Een cyberincident is niet alleen een technisch probleem dat toevallig mensen raakt, maar evenzeer een bestuurlijk probleem dat langs technische weg binnenkomt.

Over dit bestuurlijke en menselijke aspect is opvallend weinig gepubliceerd. Sapriel (2024) stelt dat crisisleiderschap in de cybercontext nauwelijks afzonderlijk is onderzocht en bepleit, gezien de aard van de cyberdreiging, meer aandacht voor de competenties waarmee mensen een crisis

besturen. Dit artikel beoogt die leemte te verkleinen, niet met een nieuw abstract kader, maar met zes concrete vaardigheden en het onderzoek waarop zij berusten.

2. Van crisismanagement naar crisisleiderschap

Er bestaat een onderscheid tussen het managen en het leiden van een crisis. Crisismanagement betreft de voorbereiding: draaiboeken, scenario's, meldketens en vooraf geformuleerde antwoorden op lastige vragen. Die voorbereiding blijft noodzakelijk. Een crisis brengt alleen altijd een mate van onzekerheid met zich mee die zich niet laat plannen. Op dat punt begint crisisleiderschap (Sapriel, 2024).

Wooten en James (2008) analyseerden welke leiderschapscompetenties in de onderscheiden fasen van een crisis van belang zijn, van vroegtijdige signalering tot evaluatie achteraf. Zij betogen dat niet elke leider deze eigenschappen van nature bezit, maar dat deze vaardigheden wel aan te leren zijn. Daarin ligt de kern van dit betoog. De vaardigheden die in een crisis het verschil maken hoeven geen aangeboren talent te zijn, maar kunnen worden geleerd, mits ze op de juiste wijze worden getraind.

3. Zes crisisvaardigheden

Het model onderscheidt zes vaardigheden. Ze komen voort uit de praktijk van crisissimulaties en zijn stuk voor stuk te herleiden tot bestaand onderzoek naar het betreffende construct. Het merendeel van dat onderzoek is afkomstig uit domeinen waarin crises (in algemene zin) onder hoge druk uitvoerig zijn bestudeerd: brandbestrijding, luchtvaart, militaire commandovoering, rampengeneeskunde en organisatiegedrag. Waar mogelijk worden deze inzichten verbonden met het opkomende onderzoek naar cyberincidentrespons.

3.1 Overzicht behouden

Inzicht houden in een voortdurend veranderende situatie is nauw verbonden met de overige vaardigheden, in het bijzonder met de besluitvorming. Endsley (1995a) duidt dit als situatiebewustzijn en omschrijft het als meer dan het waarnemen van afzonderlijke gegevens. Het veronderstelt begrip van de situatie als geheel en een projectie van haar verdere verloop: waarnemen, begrijpen en vooruitzien. In dynamische omgevingen kan volgens Endsley reeds een geringe hapering in dit bewustzijn ernstige gevolgen hebben. Hij verwijst naar het incident met de USS Vincennes, waarbij een onjuist situatiebeeld leidde tot het neerhalen van een burgervliegtuig. Endsley noemt daarnaast de brandweer, delen van de politie en militaire commandovoering als domeinen die er sterk op steunen. Situatiebewustzijn laat zich bovendien meten. Endsley (1995b) beschrijft daarvoor een bevriezingsmethode waarbij een oefening op willekeurige momenten wordt stilgelegd en deelnemers naar hun beeld van de situatie wordt gevraagd, waarna dat wordt vergeleken met de werkelijke stand van zaken. Zo ontstaat een objectieve maat voor hoe goed een team het overzicht bewaart, een benadering die dicht ligt bij hoe een simulatie het overzicht van een team zichtbaar maakt.

In de cybercrisis wordt dit aangeduid als gedeeld en gedistribueerd situatiebewustzijn en geldt het als een kerncomponent van effectieve verdediging. Veldonderzoek bij drie incident-responseteams beschrijft het handhaven van een gezamenlijk en actueel beeld als een van de voornaamste uitdagingen, juist omdat de informatie verspreid is over mensen, niveaus en systemen (Nyre-Yu, Gutzwiller en Caldwell, 2019).

3.2 Beslissen op onvolledige informatie

In een crisis dient het beslissende moment zich vaak te vroeg aan, met weinig informatie en grote belangen. Klein (1993) onderzocht hoe ervaren brandweercommandanten onder die omstandigheden beslissen. Zijn bevinding is contra-intuïtief: zij wegen geen opties tegen elkaar af, maar herkennen het patroon van de situatie en simuleren mentaal of de eerste werkbare handeling toereikend zal zijn. Een zoektocht naar de optimale keuze zou de commandant volgens Klein zozeer vertragen dat hij de controle over de operatie verliest. Ervaren beslissers zoeken geen perfecte oplossing, maar een werkbare en tijdige.

Dit patroon keert terug in cyberincidentrespons, waar filteren en beslissen tot de kern van het werk behoren (Nyre-Yu et al., 2019).

Deze herkenningsgestuurde besluitvorming laat zich trainen. Crichton, Flin en Rattray (2000) beschrijven hoe tactical decision games, korte scenario-oefeningen onder tijdsdruk, beslissers in commando- en hulpverleningscontexten laten oefenen met het snel taxeren van een situatie en het kiezen van een werkbaar besluit. Juist de blootstelling aan realistische, onvolledige informatie bouwt het herkenningsvermogen op waar Klein op wijst.

3.3 Prioriteren onder tijdsdruk

Prioriteren onder tijdsdruk is meer dan een wachtrij afwerken. Het is het ordenen van aandacht tussen doelen die met elkaar botsen, waarbij de volgorde van handelen de uitkomst sterk beïnvloedt. In een crisis staan belangen tegenover elkaar die niet allemaal tegelijk gediend kunnen worden: snelheid tegenover zorgvuldigheid, het beheersen van de aanval tegenover het doorlopen van de bedrijfsvoering, naar buiten treden tegenover juridische voorzichtigheid. Wie het ene voortrekt, stelt het andere uit. Prioriteren is daarmee vooral het afwegen van tegenstrijdige belangen, niet het simpelweg afvinken van taken op urgentie.

De meest gecodificeerde vorm van deze afweging komt uit de rampengeneeskunde: triage, het prioriteren van slachtoffers naar de ernst van hun toestand wanneer de vraag de beschikbare middelen overstijgt. Ghanbari en collega's (2021) tonen in een kwalitatieve studie hoe complex en besluitafhankelijk dat is. Bij de aardbeving in Haïti en de SARS-uitbraak twijfelde een deel van de betrokken triageofficieren aan de juistheid van de eigen beslissingen. Triage is echter maar één, sterk uitgewerkte, verschijningsvorm van een bredere vaardigheid.

In de cybercrisis keert die afweging in volle breedte terug. Op operationeel niveau moet een eerste lijn signaal van ruis scheiden in de getrapte triage van incidenten. Op organisatieniveau is prioritering kritiek omdat beveiligingsmaatregelen rechtstreeks kunnen botsen met de continuïteit

van de dienstverlening (Nyre-Yu et al., 2019; ISO/IEC 27035). De kern blijft telkens dezelfde: onder tijdsdruk bepalen welke belangen voorgaan, in het besef dat elke keuze een ander belang opoffert.

3.4 Kalm blijven onder druk

Voor deze vaardigheid is gekeken naar empirisch bewijs. King en collega's (2026) voerden een gerandomiseerde gecontroleerde studie uit binnen een special-forces-eenheid. De groep die een training in emotionele intelligentie ontving, met emotieregulatie als kern, vertoonde onder gesimuleerde gevechtsstress lagere biologische stresswaarden dan de controlegroep (gemeten via cortisol) en presteerde beter op schietnauwkeurigheid, op het onthouden van missiekritische informatie en op rekentaken onder druk. De auteurs concluderen dat het reguleren van emoties essentieel is voor het behoud van kalmte en besluitvermogen onder hoge druk.

Het spiegelbeeld ondersteunt dit. Staw, Sandelands en Dutton (1981) beschreven wat geschiedt wanneer de kalmte wegvalt. Onder dreiging vernauwt de informatieverwerking en verstart de gedragscontrole. Het individu valt terug op de meest ingesleten reactie, ook wanneer die in de gewijzigde situatie ongepast is. Het gedrag wordt minder gevarieerd en minder flexibel, juist op het moment dat variatie en flexibiliteit geboden zijn.

Deze vaardigheid laat zich gericht trainen. Driskell, Johnston en Salas (2001) tonen aan dat stress-exposure-training, het stapsgewijs oefenen van taken onder oplopende en realistische druk, zijn effect behoudt wanneer mensen daarna een nieuwe taak onder een onbekende stressor uitvoeren. Kalmte onder druk is daarmee niet louter aanleg, maar een geoefende reactie die overdraagt naar situaties die men nog niet eerder zag.

3.5 Improviseren

Een crisis voegt zich niet altijd naar het draaiboek. Weick (1993) analyseerde de ramp bij Mann Gulch, waarbij dertien brandweerlieden omkwamen toen hun vertrouwde werkwijze niet langer toereikend was. Hij benoemt vier bronnen van veerkracht die groepen minder kwetsbaar maken voor het ineenstorten van hun gedeelde begrip van de situatie. Improvisatie staat daarbij voorop. Het vermogen te handelen wanneer de gebruikelijke weg is afgesneden, is in zijn analyse geen laatste redmiddel maar een kerncompetentie.

Kendra en Wachtendorf (2007) noemen improvisatie een kenmerk van vrijwel elke ramp: gebeurt er niets onverwachts, dan is het waarschijnlijk geen echte crisis. Plannen zijn in hun woorden hypotheses over een toekomst die zich zelden precies zo aandient. Het vermogen om te improviseren verslapt bovendien wanneer het niet regelmatig wordt geoefend, wat verklaart waarom het onder een simulatie moet worden beproefd en niet mag worden verondersteld.

De threat-rigidity van Staw en collega's helpt verklaren waarom improviseren moeilijk is. Juist wanneer de omgeving ingrijpend is veranderd en afwijking geboden is, drijft de dreiging het individu naar de oude, ingesleten respons. Improviseren is daarmee een vaardigheid die juist nodig is op het moment dat de menselijke natuur haar tegenwerkt. Dat pleit ervoor haar te oefenen en niet te veronderstellen.

3.6 Veerkracht bij tegenslagen

Een crisis bestaat zelden uit één klap. Zij is een opeenvolging van tegenslagen waarbij bepalend is of een team daarvan herstelt en zich verder ontwikkelt. Sutcliffe en Vogus (2003) omschrijven veerkracht als het handhaven van positieve aanpassing onder uitdagende omstandigheden. Van belang in hun analyse is dat veerkracht niet zeldzaam of uitzonderlijk is, maar voortkomt uit betrekkelijk gewone aanpassingsprocessen die competentie herstellen en groei mogelijk maken. Zij positioneren veerkracht bovendien expliciet als tegenhanger van de threat-rigidity: verstarring is niet het onvermijdelijke lot van een organisatie onder druk. Veerkracht is in hun analyse een capaciteit op team- en organisatieniveau, niet een individuele reactie in het moment. Alliger en collega's (2015) werken dat teamniveau verder uit: teamveerkracht is meer dan de som van veerkrachtige individuen en laat zich versterken, onder meer doordat teams die vaker samenwerken elkaar beter aanvoelen en sneller herstellen van tegenslag. Daarmee is veerkracht geen vaststaand gegeven, maar iets wat een team gericht kan opbouwen en dus ook zichtbaar kan worden gemaakt in een oefening.

4. De gevolgen van het ontbreken van deze vaardigheden

Een belangrijk deel van de onderbouwing voor deze zes vaardigheden komt niet alleen voort uit hun aanwezigheid, maar uit wat er gebeurt bij hun afwezigheid. De threat-rigidity-these (Staw, Sandelands en Dutton, 1981) laat zien dat een team onder dreiging vernauwt in zijn waarneming, verstart in zijn besluitvorming en terugvalt op ingesleten gedrag. Dat raakt in één beweging het overzicht, de kalmte en het vermogen tot improvisatie. Weick (1993) toont bij Mann Gulch een uiterste consequentie daarvan: waar deze vaardigheden ontbreken, kan niet alleen de respons instorten, maar ook het gedeelde begrip van de situatie zelf.

5. Waarom kennis van crisis nog geen crisisbekwaamheid is

Op dit punt komen de bevindingen samen tot een praktische gevolgtrekking. Het bewijs achter deze vaardigheden komt grotendeels uit de studie van mensen die onder reële of gesimuleerde druk handelden. Klein observeerde het bij brandweercommandanten in het veld, King toonde het experimenteel aan bij militairen onder gesimuleerde gevechtsstress en Weick reconstrueerde het bij een dodelijke bosbrand. Een ander deel van de onderbouwing is theoretisch van aard, zoals het werk van Endsley en van Sutcliffe en Vogus.

Dat is geen toeval. De threat-rigidity helpt verklaren waarom een plan dat uitsluitend aan tafel is besproken tekort kan schieten op het moment dat het ertoe doet. Onder dreiging handelt het individu eerder naar wat is ingesleten dan naar het draaiboek. Een crisisplan dat nooit onder druk is uitgevoerd, biedt daarom geen zekerheid, maar een gevoel van zekerheid.

Bij een crisis wordt niet alleen het plan beproefd, maar ook het team. Een team laat zich niet toetsen met een presentatie of een table-top simulatie, maar door het de meldingen zelf te laten verrichten, de onderhandelingen zelf te laten voeren en de besluiten zelf te laten nemen, met alle onzekerheid, ruis en tijdsdruk die daarbij horen.

6. De waarneming van de zes vaardigheden

In een CyberMaster-simulatie doorleeft een team zelf een cybercrisis. Gedurende dat verloop wordt het gedrag van het team beoordeeld aan de hand van vooraf vastgestelde regels. Elk observatiepunt wordt tegen een vooraf vastgesteld criterium als positief of negatief gescoord. Uit die combinatie ontstaat een beeld per vaardigheid, steeds op team- of organisatieniveau en nooit als individuele score naast een naam. Doordat de beoordeling berust op vaste criteria en niet op de algemene indruk van de trainer, beoogt de methode de uitkomst zo veel mogelijk onafhankelijk van de waarnemer te maken.

Improvisatie vergt daarbij een andere maatstaf dan de overige vaardigheden. Zij is per definitie effectief handelen buiten het draaiboek en wordt daarom beoordeeld gedurende de simulatie en niet op een voorgeschreven handeling, opdat een creatieve maar doeltreffende keuze niet als afwijking wordt bestraft.

7. Verantwoording en reikwijdte

Het CyberMaster Crisis Readiness Model is een praktijkgedreven model waarvan elk element is verankerd in gevestigd onderzoek naar crisis, besluitvorming en gedrag onder druk. Het dient als gestructureerd observatiekader in het trainingsaanbod van CyberMaster.

De zes vaardigheden zijn niet aan één studie ontleend. Juist omdat naar leiderschap en besluitvorming in de cybercrisis specifiek nog weinig onderzoek is verricht, is bewust voor deze aanpak gekozen. Bevindingen uit domeinen waarin crises onder hoge druk wel uitvoerig zijn onderzocht worden samengebracht en verbonden met het opkomende onderzoek naar cyberincidentrespons. De samenvoeging vormt daarmee geen tekortkoming, maar een weloverwogen antwoord op een jong onderzoeksveld. Het model wordt gepresenteerd als een goed onderbouwde combinatie van bestaand onderzoek, niet als een door de wetenschap bevestigd geheel. De keuze om juist deze zes vaardigheden te verenigen is een eigen bijdrage. Daarbij bestaan ook andere taxonomieën van cybercompetenties die niet een op een met deze zes samenvallen.

Bij de beoordeling passen enkele eerlijke kanttekeningen. Ten eerste is de voorspellende waarde van de score niet empirisch getoetst, aangezien dan in een daadwerkelijke crisis moet worden geobserveerd. Een hoge score in de simulatie vormt daarmee een aanwijzing, maar geen zekerheid dat een team een werkelijke cybercrisis goed zal doorstaan. Hoe realistisch een cybercrisis namelijk ook wordt gesimuleerd, het zal nooit hetzelfde zijn als een daadwerkelijke crisis. Ten tweede blijven verscheidene van deze constructen inhoudelijk verwant. Er wordt niet geclaimd dat het zes statistisch onafhankelijke factoren betreft. Ten derde berust het cyberspecifieke deel van de onderbouwing grotendeels op kwalitatief, beschrijvend veldonderzoek, dat aantoont dat deze vaardigheden ertoe doen in de praktijk.

8. Conclusie

De vraag is niet langer of een organisatie een cybercrisis meemaakt, maar of de mensen die daarin moeten beslissen daarop zijn voorbereid. In veel organisaties krijgt de techniek in die voorbereiding meer aandacht dan de mensen die de crisis moeten aanvliegen. Dat is zelden een kwestie van onvermogen, maar van gebrek aan oefening onder realistische druk.

Sinds 15 augustus 2026 is dit niet alleen verstandig, maar in bepaalde gevallen zelfs verplicht. De Cyberbeveiligingswet, de Nederlandse uitwerking van NIS2, verplicht ieder bestuurslid van een essentiële of belangrijke entiteit te beschikken over de kennis en vaardigheden om risico's te identificeren, risicobeheersmaatregelen te beoordelen en de gevolgen daarvan voor de eigen dienstverlening te wegen (artikel 24, tweede lid, Cyberbeveiligingswet). Bestuursleden dienen daaraan binnen twee jaar na inwerkingtreding van die bepaling aantoonbaar te voldoen (artikel 24, derde lid) en beschikken daartoe over een certificaat van een training die deze onderwerpen behandelt (artikel 24, vijfde lid). Deze zes vaardigheden dragen daaraan bij. Dat resultaat bereikt men niet met een presentatie, maar door te oefenen onder realistische druk.

Zes vaardigheden bepalen hoe een team die druk doorstaat: overzicht, beslissen, prioriteren, kalm blijven, improviseren en veerkracht. Elk is verankerd in onderzoek naar mensen die handelden onder druk. Ze hebben één kenmerk gemeen. Ze laten zich niet door lezen verder ontwikkelen, maar door het zelf te doen, voordat de ernst zich aandient.

Referenties

Alliger, G. M., Cerasoli, C. P., Tannenbaum, S. I. en Vessey, W. B. (2015). Team resilience: How teams flourish under pressure. *Organizational Dynamics*, *44*(3), 176-184.

Crichton, M., Flin, R. en Rattray, W. A. (2000). Training decision makers: Tactical Decision Games. *Journal of Contingencies and Crisis Management*, *8*(4), 208-217.

Driskell, J. E., Johnston, J. H. en Salas, E. (2001). Does stress training generalize to novel settings? *Human Factors*, *43*(1), 99-110.

Endsley, M. R. (1995a). Toward a theory of situation awareness in dynamic systems. *Human Factors*, *37*(1), 32-64.

Endsley, M. R. (1995b). Measurement of situation awareness in dynamic systems. *Human Factors*, *37*(1), 65-84.

Ghanbari, V., Ardalan, A., Zareiyan, A., Nejati, A., Hanfling, D., Bagheri, A. en Rostamnia, L. (2021). Fair prioritization of casualties in disaster triage: a qualitative study. *BMC Emergency Medicine*, *21*, 119.

ISO/IEC 27035. Information technology, Information security incident management.

Kendra, J. M. en Wachtendorf, T. (2007). Improvisation, creativity, and the art of emergency management. In H. Durmaz e.a. (red.), *Understanding and responding to terrorism* (pp. 324-335). IOS Press.

King, J. B., Li, Y., Gillespie, N. A. en Ashkanasy, N. M. (2026). Emotional intelligence training improves stress regulation and performance in high-stress occupations. *Scientific Reports*, *16*, 6673.

Klein, G. A. (1993). A recognition-primed decision (RPD) model of rapid decision making. In G. A. Klein, J. Orasanu, R. Calderwood en C. E. Zsambok (red.), *Decision making in action: Models and methods* (pp. 138-147). Ablex.

Nyre-Yu, M., Gutzwiller, R. S. en Caldwell, B. S. (2019). Observing cyber security incident response: Qualitative themes from field research. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*.

Sapriel, C. (2024). Why crisis leadership competencies matter in the effective management of a cyber crisis. *Cyber Security: A Peer-Reviewed Journal*, *8*(2), 160-168.

Staw, B. M., Sandelands, L. E. en Dutton, J. E. (1981). Threat-rigidity effects in organizational behavior: A multilevel analysis. *Administrative Science Quarterly*, *26*(4), 501-524.

Sutcliffe, K. M. en Vogus, T. J. (2003). Organizing for resilience. In K. S. Cameron, J. E. Dutton en R. E. Quinn (red.), *Positive organizational scholarship: Foundations of a new discipline* (pp. 94-110). Berrett-Koehler.

Weick, K. E. (1993). The collapse of sensemaking in organizations: The Mann Gulch disaster. *Administrative Science Quarterly, 38*(4), 628-652.

Wooten, L. P. en James, E. H. (2008). Linking crisis management and leadership competencies: The role of human resource development. *Advances in Developing Human Resources, 10*(3), 352-379.