

Een high-level beheersingsmodel voor cyberrisico's

Abbas Shahim, Ronald Batenburg en Joost Geusebroek

SAMENVATTING In dit artikel presenteren wij een high-level model voor de integrale beheersing van cyberrisico's. Het model is ontworpen om organisaties strategische ondersteuning te bieden op dit nieuwe en complexe terrein. Het is generiek opgezet zodat organisaties systematisch hun huidige situatie kunnen analyseren en de belangrijkste verbeteringen vast kunnen stellen. Het model is opgebouwd rondom cyber als centrale component die door vier bouwstenen wordt omsloten, te weten: risico's, reputatie en middelen, respons, en bronnen. Hiervoor zijn handvatten uitgewerkt die bedrijven helpen om cyberrisico's op een integrale manier te beheersen.

RELEVANTIE VOOR DE PRAKTIJK Het beheersen van cyberrisico's is één van de belangrijkste uitdagingen van organisaties geworden in het digitale tijdperk. Door het gebrek aan een integrale en high-level aanpak hiervoor is in de praktijk de behoefte ontstaan aan een toegepast-wetenschappelijk model. Het in dit artikel gepresenteerde model is gebaseerd op zo'n aanpak en biedt naast een high-level model ook handvatten voor verbeteringen.

1 Inleiding

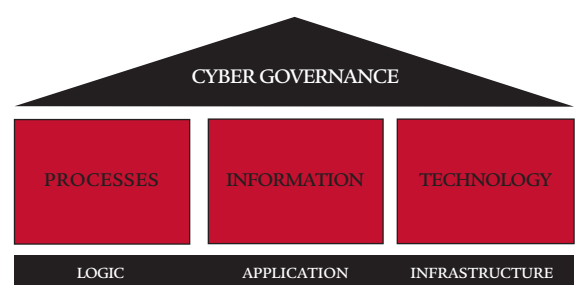
De hedendaagse bedrijfsvoering is sterk afhankelijk van IT-systemen om een efficiënte uitvoering en ondersteuning van bedrijfsprocessen te realiseren. Opkomende technologieën dragen bij aan een snel veranderend 'cyberlandschap' (Choo, 2011). Web-technologieën volgen elkaar in een hoog tempo op en bieden bedrijven kansen en financieel aantrekkelijke oplossingen. Echter, het gebrek aan kennis met betrekking tot de nieuwe en vooral complexe innovaties levert ook beheersingsvraagstukken en -problemen op. Nieuwe risico's bestaan uit ongewenste indringers die zich op velerlei mogelijke manieren toegang verschaffen tot IT-omgevingen en de hierin opgeslagen kritische bedrijfsinformatie (Thayer et al., 2013). De inter-connectiviteit van systemen met het internet biedt hackers een platform voor kwaadaardige handelingen. Cybercrime-activiteiten oefenen op bepaalde groepen een sterke aantrekkingskracht uit om voor eigen gewin of 'voor de kick' de beveiligingstechniek te allen tijde een stap voor te zijn. Het landschap met cy-

berrisico's is dan ook in een snel tempo geëvolueerd in de afgelopen decennia (Hult & Sivanesan, 2014). Om met een metafoor te spreken, hackers zijn tegenwoordig niet enkel gefocust op het uitpakken van het cadeau, maar vooral ook wat in de verpakking zit is net zo aantrekkelijk.

In het cyberlandschap gebruiken en misbruiken mensen IT. Dit komt met name aan het licht wanneer bedrijven om moeten gaan met in- en externe cyberrisico's. Het is een veelomvattend probleem dat een aanpak vergt waarbij leiderschap, aansprakelijkheid en adequate managementvaardigheden komen kijken. Een voorbeeld ter illustratie is het groeiende zakelijke gebruik van mobiele apparaten als smartphones en tablets door medewerkers. Hoe kunnen de daarbij behorende risico's op een adequate wijze worden gemitigeerd? Wat kan gedaan worden met technische maatregelen, en als deze niet afdoende zijn, hoe dient te worden omgegaan met 'de mens als zwakke schakel'?

Effectief beheer en beleid van het cyberbeheersingslandschap behelst meer aspecten dan alleen technologie. Figuur 1 is gebaseerd op het veel gebruikte model van Betz (2011) en geeft een integrale kijk op het cyberbeheersingslandschap. Deze drie pijlers representeren de hoofddimensies van het IT-landschap. De informatie-, proces- en technologiepijler worden ondersteund door respectievelijk logische regels, applicaties en infrastructuur. Deze drie pilaren en dimensies dienen onder één dak en integraal beheerst te worden, samengevat met de term cyber governance.

Figuur 1 Een integrale kijk op cyber-beheersing, gebaseerd op het model van Betz (2011)



Veel wetenschappelijk onderzoek is uitgevoerd naar elk van de pilaren in dit model, maar veel minder naar het overkoepelende cyber governance. Onderzoek naar de technologie-pilaar is bijvoorbeeld rijkelijk vertegenwoordigd door best-practices en frameworks zoals ITIL. Onderzoek tot nu toe heeft vooral de nadruk gelegd op een *bottom-up* aanpak waarbij technologie als startpunt wordt gehanteerd. Zoals reeds gezegd is het beheersen van cyberrisico's echter niet enkel een technologische bijkomstigheid. De bedrijfsvoering staat hierbij ook centraal (Von Solms & Von Solms, 2004).

Er zijn tevens modellen beschikbaar (ISF, 2011; Bodeau et al., 2010; WEF, 2012; Department of Homeland Security, 2009a, 2009b) die aansluiten bij een integrale kijk op het beheersen van cyberrisico's. Deze modellen schenken echter onvoldoende aandacht aan een evenwichtige en algehele focus op alle aspecten en deelgebieden van cyberbeheersing.

Er is dus specifiek onderzoek gewenst dat een integrale kijk presenteert op het gebied van het beheersen van cyberrisico's en de nieuwe ontwikkelingen die zich daarbij aanbieden. Een high-level benadering is daarvoor nodig, dat een overzichtelijke samenhang van alle componenten en gebieden bestrijkt waar technologie, processen en informatie logische onderdelen vormen voor het beheersen van risico's.

Dit artikel is als volgt opgebouwd. Aan de hand van een literatuurstudie benoemen we eerst de tekortkomingen en witte vlekken die de aanleiding vormden tot het ontwerp van een nieuw model. Daarna beschrijven wij het ontwerpproces, de keuze voor de bouwstenen, de visualisatie van het beheersingsmodel en hoe het is gevalideerd door academici en praktijkexperts.

2 Onderzoeksvraag en aanpak

In dit artikel stellen we de vraag hoe een high-level model ontworpen kan worden dat organisaties kunnen gebruiken om cyberrisico's op een integrale wijze te beheersen. We beantwoorden deze vraag met behulp van de *design science research*-methode van Vaishnavi & Kuchler (2008). Deze methode bestaat uit vier verschillende fasen die het methodologische proces vormen voor het ontwerpen van een cyber beheersingsmodel. De eerste fase is daarin de 'bewustzijns-fase'.

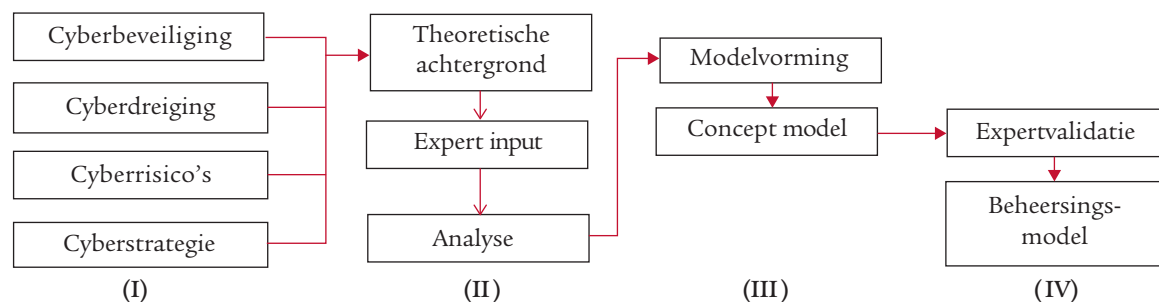
Deze definieert de onderzoeksaanleiding en aanpak. De tweede fase is de 'suggestie-fase', in deze fasen wordt (wetenschappelijke) literatuur in kaart gebracht die te vinden is in dit onderzoeksveld. Als toevoeging in deze fase kunnen experts in het vakgebied geïnterviewd worden om aanvullende kennis uit de praktijk te vergaren. De verzamelde onderzoekdata worden dan in de derde 'ontwikkel-fase' geanalyseerd, waarna ze gebruikt worden voor het model zelf. De laatste en vierde fase is de 'validatie- en conclusie-fase' die gaat over de bijdrage van het model en het onderzoek aan het veld, en bestaat uit de uiteindelijke conclusies. Tabel 1 (Takeda et al., 1990; Vaishnavi & Kuechler, 2008) toont een overzicht van deze vier fasen en de gebruikte onderzoeksmethode in combinatie met de activiteiten en deelproducten.

Tabel 1 Overzicht onderzoeksfasen

Fase	Stap	Activiteiten	Deelproducten
I	Bewustzijn	Doel onderzoek & aanpak Desk research	Opzet en doel onderzoek Theoretische achtergrond
II	Suggestie	Expert input Analyse	Onderzoekdata
III	Ontwikkel	Analyse & concept modelvorming	Concept beheersingsmodel
IV	Validatie en conclusie	Validatie van model Expert validatie	High-level beheersingmodel

De vier fasen en ons ontwerponderzoek is ook in figuur 2 schematisch weergegeven. Allereerst is onderzocht hoe het cyberrisico-landschap zich kenmerkt en heeft ontwikkeld. Door gedetailleerd te kijken naar het concept cyber in de literatuur is de focus gelegd op de gebieden beveiliging, strategie, dreiging en risico's (fase I). De vergaarde informatie is als theoretische achtergrond aangevuld met input van deskundigen die in uiteenlopende sectoren werkzaam zijn. De uitkomst hiervan is nader geanalyseerd en heeft de basis gevormd van een conceptversie van het beheersingsmodel (fase II & fase III). Vervolgens is dit model door experts gevalideerd en hun commentaar en opmerkingen zijn verder verwerkt. Hierna is het uiteindelijke high-level beheersingsmodel tot stand gekomen (fase IV).

Figuur 2 Onderzoeksaanpak



3 Cyberrisico's, gerelateerde basisbegrippen en concepten

Als we teruggaan naar de oorsprong, dan zien we dat de term 'cyber' of 'cyberspace' in het verleden gebruikt werd in gevallen waarbij sprake was van netwerken en computers (Ottis & Lorents, 2010). Het concept 'cyber' is afkomstig van de term *cybernetics* van Wiener (1948). Later transformeerde deze term naar *cyberspace* die heden ten dage wordt gebruikt, en waarvan technologie het uitgangspunt is (Geers, 2011; ISF, 2011). Tot op heden is er nog geen uniformiteit over de exacte definitie van *cyberspace* (b.v. Ottis & Lorents, 2010; ISF, 2011; Department of Homeland Security, 2009a, 2009b). ISF (2011) definieert het als volgt: "Cyberspace is the always-on, technologically interconnected world; it consists of people, organizations, information and technology". Cyber is nu een veelgebruikt voorvoegsel voor nieuwe termen als cyber-oorlog, cyber-aanval of cyber-terrorisme. Cyber maakt een onmiskenbaar onderdeel uit van het dagelijkse sociale en zakelijke leven. Tussen 2000 en 2010 is het dagelijks internetgebruik gegroeid van 360 miljoen naar 2 miljard gebruikers.

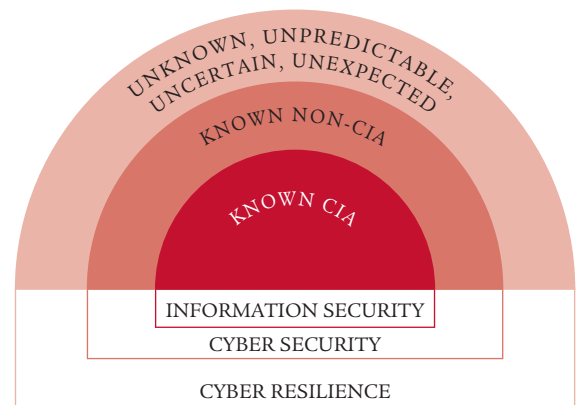
3.1 Cyberbeveiliging

Als we de literatuur overzien dan zijn er drie verschillende basisbegrippen betreffende beveiliging die betrekking hebben op het domein van cyberspace: *information security* (informatiebeveiliging), *cyber security* en *cyber resilience*. Figuur 3 toont de relatie tussen deze concepten volgens ISF (2011). Deze is gebaseerd op zogeheten CIA (Confidentiality, Integrity & Availability)-driehoek. Dreigingen in *cyberspace* hebben direct invloed op deze drie aspecten en vormen de basis binnen informatiebeveiliging. Er zijn echter ook dreigingen die verder strekken dan CIA. Denk hierbij aan reputatieschade wanneer een bedrijfskritisch informatiesysteem niet meer beschikbaar is voor klanten, het onverwachts lekken van vertrouwelijke informatie via een verloren USB-stick, of inbraak in een IT-omgeving. Enkel technische oplossingen zijn geen garantie meer voor succes. Nieuwe risico's met een hoge impact op de bedrijfsvoering, die onvoorspelbaar en moeilijk te mitigeren zijn, vragen om een veerkrachtige organisatie, ook wel gedefinieerd als *cyber resilience*.

Figuur 3 geeft de CIA-concepten weer in relatie tot informatiebeveiliging. De definitie voor information security volgens ISF (2011) richt zich op CIA. Ook in andere definities worden deze concepten benoemd. Een voorbeeld hiervan is de definitie van Whitman & Mattord (2011): "To protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission". Dit wordt bewerkstelligd door beleid, training, technologie en bewustzijn. ITGI (2006) definieert informatiebeveiliging als: "Information security addresses the protection of information, confidentiality, availability and integrity throughout the life cycle of the infor-

mation and its use within the organization". Vaak wordt het begrip IT-beveiliging verweven met informatiebeveiliging. IT-beveiliging staat in relatie met informatiebeveiliging en legt doorgaans de nadruk eigenlijk op infrastructuur en de ondersteunende technologie. Informatiebeveiliging kan breder getrokken worden aangezien het zich niet enkel richt op technologie, maar ook op mensen en processen.

Figuur 3 Positionering concepten door ISF (2011)



In vergelijking met informatiebeveiliging vereist cyberbeveiliging een uitgebreidere kijk op potentieel negatieve uitkomsten, met name op reputatie. Het concept cyberbeveiliging heeft dan ook betrekking op bijkomende dreigingen die verder uitstrekken dan CIA van systemen. Organisaties dienen rekening te houden met alle potentiële risico's en dreigingen. Deze bredere kijk gaat over het werkveld van *cyber resilience*. Deze invalshoek vraagt om een wendbare organisatie die snel en doelgericht kan reageren op mogelijk nieuwe dreigingen. *Cyber resilience* dekt een extra dimensie van cyberisicomanagement (WEF, 2012; Williams & Manheke, 2010). ISF (2011) definieert *cyber resilience* als volgt: "The organization's capability to withstand negative impacts due to known, predictable, unknown, unpredictable, uncertain and unexpected threats from activities in cyberspace". *Cyber resilience* omvat CIA, de onbekende CIA en onbekende dreigingen zoals afgebeeld in figuur 3.

3.2 Cyberdreiging

Dreigingen in het cyberlandschap zijn praktisch altijd, overal en continu aanwezig. Deze dreigingen zijn zowel intern als extern. Interne dreigingen kunnen ontstaan vanuit het personeel door gebrek aan kennis en vaardigheden, of door een gebrouilleerde werknemer. Een dreiging kunnen we definiëren als een categorie van objecten, personen of andere entiteiten die gevaar brengen ten aanzien van systemen (Whitman & Mattord, 2011). Een cyberdreiging is een potentiële gebeurtenis met mogelijke consequenties die een IT-systeem of organisatie negatief kunnen beïnvloeden (WEF, 2012).

3.3 Cyberrisico's

Cyber-risico's zijn door Whitman & Mattord (2011) gedefinieerd als de mogelijkheid dat iets ongewenst kan gaan gebeuren. WEF (2012) definieert een risico als: "The probability of an event within the realm of networked information systems and the consequences of this event on assets and reputation". Cyber(gerelateerde) risico's zijn een zorg voor organisaties aangezien zij een impact kunnen hebben op alle lagen binnen een organisatie. Het is voor hen dan ook een continu proces van het managen van deze risico's versus de opbrengst (ISF, 2011). Nagedacht dient te worden in welke mate het aanvaardbaar is om risico's te accepteren, hetgeen in de vakterminologie als *risk appetite* wordt aangeduid (Whitman & Mattord, 2011). Belangrijk hierbij is dat een methodiek is vereist met een risicomangement-gerichte aanpak (Siegel et al., 2002).

3.4 Cyberstrategie

Er zijn veel consequenties verbonden aan cyber-gerelateerde risico's voor een organisatie. Denk bijvoorbeeld aan een mogelijke nasleep van een inbreuk op de beveiliging die aanhoudend de bedrijfscontinuïteit in gevaar brengt. Figuur 4 geeft een overzicht van mogelijke consequenties waarmee een organisatie geconfronteerd kan worden. De voornaamste interne drijfveren binnen de organisatie zijn *assessment* en detectie. Extern gekeken zal een risico mogelijk leiden tot diefstal of verlies van informatie. Dit kan een domino-effect in gang brengen waarbij de continuïteit van de bedrijfsvoering wordt aangetast. Dit kan weer resulteren in een verlies en reputatieschade voor de desbetreffende organisatie. Gesteld kan worden dat cyber-gerelateerde risico's strategisch een continue en brede benadering behoeven die verschillende lagen van organisaties betreft. Het omsluit een *cyber risk beheersing* aanpak die geïntegreerd dient te worden in het bedrijfsrisicomanagement (*Enterprise Risk Management - ERM*) teneinde effectief te zijn. Het beheersen van cyberrisico's heeft een centrale focus

op technische maatregelen. Tevens is deze essentiële actie gericht op zowel het beïnvloeden van gedrag en normen van werknemers als op processen en activiteiten om negatieve impact te voorkomen (WEF, 2012).

3.5 Cyberbeheersing

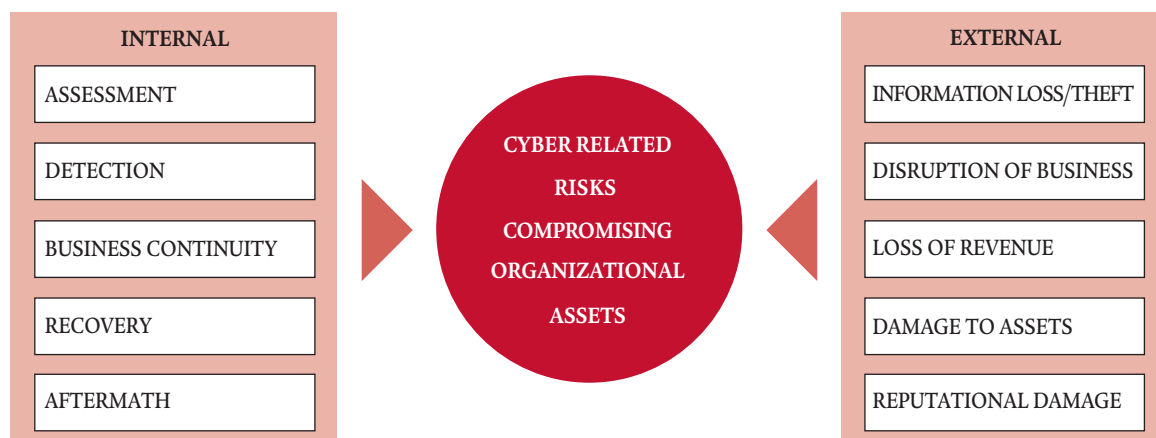
Als we nadenken over een beheersingsmodel voor cyberrisico's dan is een algehele en brede kijk op de aspecten van cyberbeheersing nodig. Om dit te bewerkstelligen is een uitgebreid onderzoek gedaan op basis van bestuderen van academische publicaties alsmede vakbladen. Een kwalitatieve data-analyse (Seidel, 1998) bracht vijf bouwstenen en individuele karakteristieken naar voren die op high-level niveau het fundament vormen voor het beheersen van cyberrisico's. De vijf hoofdbouwstenen, te weten: *cyber, risico's, reputatie & middelen, respons en bronnen* vormen de basis voor het model. Hieronder wordt het gepresenteerd op basis van de hierboven genoemde bouwstenen die een algemene bijdrage leveren aan de behoefte van een integrale kijk op het cyberbeheersingslandschap.

4 High-level beheersingsmodel voor cyberrisico's

In deze paragraaf presenteren we een beheersingsmodel voor cyberrisico's dat gebaseerd is op de hiervoor gepresenteerde literatuur en overzicht van concepten. Het beheersingsmodel dat we voor ogen hebben heeft ten eerste als doel vanuit een strategisch (of: high-level) perspectief een integrale kijk te bieden op de risico's die in het cyberlandschap voorkomen. Daarnaast is het bedoeld als instrument voor het identificeren en beheersen van cyberrisico's en organisatorische activiteiten die daarbij horen. En tenslotte dient het model een hulpmiddel te zijn dat richtlijnen en handvatten biedt voor een organisatie. Daarmee kan het dus ook tactisch en operationeel ingezet worden.

We zullen nu eerst ingaan op de vijf bouwstenen van het model, die afgeleid zijn uit de literatuurstudie en de concepten zoals hierboven aangegeven. Het basismodel en

Figuur 4 Consequenties van cyber gerelateerde risico's (Ponemon Institute, 2011)



de bouwstenen zijn in een validatieronde aan experts voorgelegd. Op basis van hun feedback is het uiteindelijke model opgesteld, dat in de volgende sectie van dit artikel zal worden beschreven.

4.1 Bouwstenen

In het cyberlandschap zijn voor het beheersen van cyberrisico's vijf elementen van belang. Zij vormen de bouwstenen van het beheersingsmodel. Het gaat om:

- *Cyber*: dit betreft de oppervlakte van het cyberlandschap zelf, de basis waar alle mogelijke risico's uit voort komen. Het gaat om alle processen, informatie en technologie die in een organisatie op één of andere manier via cyber of cyberspace verlopen of hiervan onderdeel uitmaken;
- *Risico's*: dit zijn alle mogelijke dreigingen en zwakheden in het cyberlandschap, die voortkomen uit cyber en de daaraan verbonden processen, informatie en technologie. Deze risico's geven de aanleiding om beheersingsstructuren en -maatregelen in te richten;
- *Reputatie & middelen*: risico's verschillen in de mate waarin zij schade berokkenen aan de organisatie en de mate waarin zij een beroep doen op de middelen die een organisatie ter beschikking staan om risico's te beheersen. Zo zijn reputatie en middelen op een andere manier aan de orde bij informatiediefstal dan bij IT-sabotage;
- *Respons*: op cyberrisico's kan op verschillende manieren gereageerd worden. En ook in de beheersing van cyberrisico's zijn er verschillende benaderingen, methoden en strategieën. Dit alles valt onder 'respons' bijvoorbeeld hoe men inzet op bewustzijn (*awareness*), (tussentijdse) evaluatie, detectie, het vastleggen van aanpak en verantwoordelijkheden, hoe intern en extern wordt samengewerkt (coöperatie);
- *Bronnen*: de laatste bouwsteen bestaat uit bronnen en middelen die organisaties ter beschikking staan. Het gaat om financiering maar ook om menskracht, kennis en IT-middelen.

De vijf bouwstenen hebben een duidelijke onderlinge samenhang. Cyber als domein wordt centraal gerepresenteerd in het model. De risico's en reputatie(schade) die daaruit voorkomen mobiliseren responses en middelen van organisaties. Zij bestaan uit meerdere beleidsstructuren en hebben met diverse omgevingen te maken. Denk hierbij aan de uitbesteding (outsourcing) van IT, waarbij voor het beheersen van cyberrisico's er ook met het beleid van andere organisaties rekening dient te worden gehouden. Een basisgedachte van het model is dat organisaties dus zowel intern als extern een afhankelijkheidsanalyse uitvoeren waarbij ze alle basiselementen betrekken die invloed hebben op het cyberdomein.

4.2 Expertvalidatie

Om de bouwstenen en hun veronderstelde samenhang te valideren zijn semi-gestructureerde interviews

uitgevoerd met tien experts. Deze experts waren in verschillende sectoren werkzaam (zie tabel 2). Door deze diversiteit is zo breed mogelijk feedback verkregen. Tevens hebben we gezorgd voor een balans tussen experts uit de wetenschap en de praktijk. Onder de experts bevonden zich drie academici op twee verschillende Nederlandse universiteiten en zeven experts werkzaam in de praktijk van verschillende vakgebieden en organisaties. Alle interviews zijn digitaal opgenomen en getranscribeerd. Op de interviewverslagen is een content analyse uitgevoerd (White & Marsh, 2006; DiCicco-Bloom & Crabtree, 2006).

De interviews waren als volgt opgezet. Het interview startte met een inleiding en toelichting op het doel van het onderzoek. Daarna werden één voor één de bouwstenen voor het model voorgelegd. Per bouwsteen is een aantal (vooraf opgestelde) vragen gesteld die de richtlijn vormden voor het semi-gestructureerde interview. De vragen hadden tot doel om de compleetheid, correctheid en consistentie van de bouwstenen van het model te bepalen. Daarnaast zijn ten tijde van de interviews extra vragen gesteld. Deze creëerden ruimte voor de desbetreffende experts om hun visie te geven op basis van eigen vakgebied, expertise en inzicht. Ook is aan alle experts gevraagd om feedback te geven op de opzet van het onderzoek. De interviews namen elk zestig tot negentig minuten in beslag.

Tabel 2 Overzicht geïnterviewden

Sector	Functie
IT-dienstverlening	Country Security Officer Global Head of Defense and Security
Business consulting	Security Principal
Overheid	Information Security Manager
Bankwezen	Risk Manager
IT-consulting	Cyber Competence Lead
Telecom	Risk and security officer
Onderwijs	Hoogleraar Universitair hoofddocent Universitair hoofddocent

Uit de interviews kwamen verschillende resultaten naar voren. De experts konden zich in het algemeen goed vinden in de bouwstenen van het model. De oordelen van de experts van de compleetheid, correctheid en consistentie van de bouwstenen corresponderden goed met elkaar. Ondanks dat er geen grote of uitzonderlijke verschillen in oordelen bestonden, gaven de experts wel diverse aanbevelingen mee hoe bouwstenen en elementen nog verder verbeterd konden worden. De belangrijkste opmerkingen en verbeteringsuggesties vatten we hieronder samen:

1. Een aandachtspunt is dat er verschillende visies kunnen zijn bij het toepassen en het evalueren van de

bouwstenen van het model. Een security expert heeft een andere kijk op het werkveld in vergelijking met een expert op het gebied van risico's. Een praktisch voorbeeld hiervan is het onderscheid tussen incidentmanagement en risicomanagement. In de aanpak om cyberrisico's te beheersen, kan het gaan om beschermen, mitigeren, verdedigen of afschrikken. In de bouwsteen 'respons' zou dus onderscheid gemaakt moeten worden tussen verschillende benaderingen. Organisaties zijn immers vrij in het kiezen van de aanpak die het beste past bij hun middelen en bronnen.

2. Het tweede aandachtspunt betrof de gelaagdheid van het te ontwerpen model. Er zit een onderscheid in tussen strategisch, tactisch en operationeel niveau, hetgeen niet in de bouwstenen duidelijk wordt. Uiteenlopende suggesties werden gedaan om die gelaagdheid aan te brengen. Bijvoorbeeld in de omloopsnelheid van het beheersingsproces (operationeel – snel, tactisch – gemiddeld, strategisch – langzaam).
3. Met verschillende experts is gesproken over de gevallen waarin het model de 'grenzen van de organisatie' zal overstijgen. Dit punt stipten we hiervoor reeds aan. De bouwstenen van het model gaan over de activiteiten van een individuele organisatie maar dit gebeurt vaak in combinatie met andere organisaties via partnering en verantwoordelijkheden. Volgens de experts diende dit in het model terug te komen. In dat verband wordt er wel gesproken van het vermogen van organisaties om te kunnen acteren in een 'cyber ecosysteem'. Het model zou daarom inzetbaar moeten zijn op de diverse beheersstructuren.
4. De laatste suggestie voor verbetering was het verduidelijken van het uiteindelijke doel van het model. Eén van de experts suggereerde dat elke bouwsteen een proces representeert. Dit zou dan gekoppeld moeten worden aan de handvatten die bij die processen te benoemen zijn. Een andere expert zag twee typen processen, cyberprocessen die specifiek een organisatie beschermen, en de primaire processen van een organisatie. Deze zijn dan wel verweven met elkaar.

De expertinterviews en de daaruit voortkomende suggesties zijn gebruikt om het model vanuit de vijf bouwstenen en hun samenhang te ontwerpen en schematisch te representeren. Dit beschrijven we in de volgende paragraaf.

5 Het (high-level) beheersingsmodel van cyberrisico's

Figuur 5 is het hoofd-resultaat van ons onderzoek op 'high-level' niveau. Het is de visuele weergave van een beheersingsmodel voor cyberrisico's dat een integraal perspectief biedt hetgeen organisaties op verschillende niveaus kunnen gebruiken. Op tactisch en operationeel niveau worden de bouwstenen van het model verder uitgewerkt.

De centrale hoofdcomponent, *cyber*, vormt het hart van het model. Dit wordt door de vier andere bouwstenen omsloten: *risico's*, *reputatie & middelen*, *respons* en *bronnen*. Deze vier bouwstenen hebben een directe relatie met 'cyber' in het centrum van het model en draaien als het ware continue om het cyberlandschap heen. Alle bouwstenen bestaan elk uit individuele eigenschappen en onderlinge afhankelijkheden. En elk van de bouwstenen worden ondersteund door beleid en processen binnen de organisatie. Hoewel dit niet vermeld staat in de high-level versie van ons model zoals geïllustreerd in figuur 5, dient het menselijke aspect binnen alle bouwstenen van het model meegenomen te worden.

De vijf bouwstenen van het model kunnen nu als volgt nader worden uitgelegd:

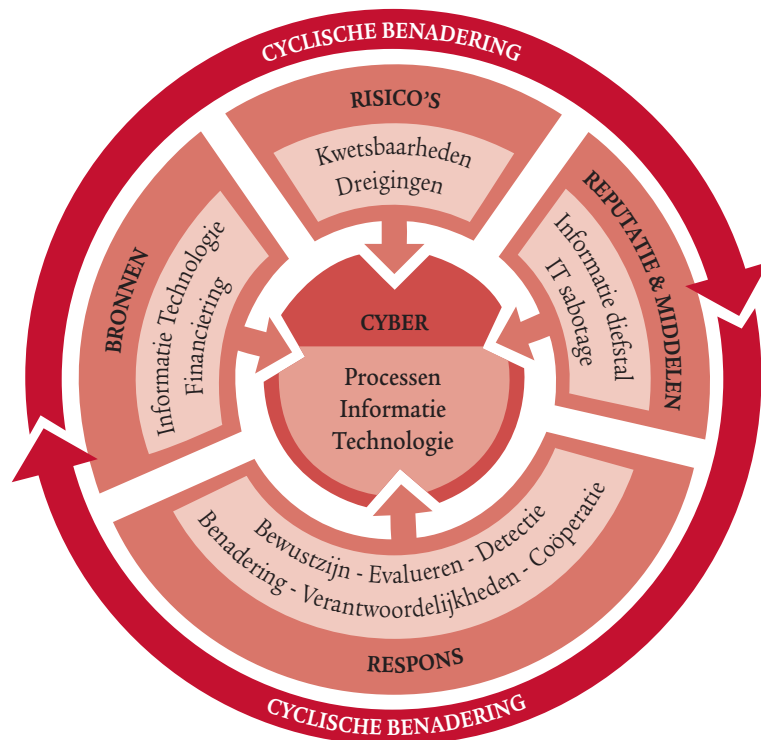
Cyber, de centrale bouwsteen van het model, bestaat uit processen die de logische laag representeren van het cyberlandschap. Deze bouwsteen representeert ook applicaties en infrastructuur die tezamen voor de verwerking en doorstroom van informatie zorgdragen. Uitgaande van deze drie pilaren van het hierboven genoemde model van Betz (2011), is het mogelijk om bijvoorbeeld bedrijfskritische informatie te stelen.

De tweede bouwsteen (*risico's*) bestaat uit dreigingen die een mogelijke impact hebben op de systemen en reputatie van een organisatie. Het zijn de mogelijke zwakheden die in potentie dreigingen en risico's veroorzaken of verhogen.

De derde bouwsteen betreft *reputatie* en *middelen*. Hierbij gaat het om de gevolgen van cyberrisico's, zoals bijvoorbeeld bij informatiediefstal en IT-sabotage. Het bepaalt waarop de organisatie moet reageren om de mogelijke consequenties van kwaadaardige activiteiten te mitigeren.

Wat een effectieve aanpak van cyberrisico's zou moeten zijn zit in de vierde bouwsteen: *respons*. Deze bouwsteen bestaat ten eerste uit het creëren van bewustzijn binnen de organisatie ten aanzien van cyber-gerelateerde risico's. Dit bewustzijn komt terug in de strategie van de organisatie om zich te beschermen tegen risico's, om deze adequaat te detecteren en af te vangen door een proactieve en effectieve aanpak. Het gaat dus om een algehele aanpak vanuit de organisatie voor het minimaliseren van cyberrisico's. De hierbij behorende processen dienen aan werknemers als taak te worden aangewezen. En tevens is samenwerking in deze bouwsteen van het model van belang, hetgeen over het delen van informatie en afstemmen tussen verschillende organisaties gaat. In complexe cyberlandschappen en eco-systemen leidt samenwerking tot een effectievere aanpak.

Bronnen is de vijfde en laatste bouwsteen van het model. Een belangrijk element daarvan, zoals in de figuur weergegeven, is *Informatietechnologie*. Hierbij gaat het om technische bronnen voor onderhoud en ontwikkeling van een veilig cyberlandschap. Daarnaast gaat het om vaardigheden en kennis van personeel zodat er bekwaam en

Figuur 5 High-level beheersingsmodel voor cyberrisico's

effectief gehandeld kan worden. Personeel wordt op haar beurt ondersteund door organisatorische bronnen (*financiering*) zodat het personeel de ruimte en tijd krijgt voor deze operationele taken. Een bron is ook dat een organisatie investeert in programma's voor het beheersen van cyberrisico's, om het eerder genoemde bewustzijn binnen de organisatie voor mogelijke cyberdreigingen en risico's te vergroten en op peil te houden. Ook dit vereist bronnen als kennis binnen de organisatie en mogelijkheden voor uitvoering.

6 Conclusie

In dit artikel hebben we het ontwerpproces beschreven, waarmee een high-level model is gecreëerd dat organisaties helpt bij het beheersen van cyberrisico's. Het model kan ingezet worden als een strategisch hulpmiddel om cyberrisico's integraal te benaderen. Het biedt handvatten bij het analyseren van de huidige situatie en het bepalen van de benodigde verbeterprocessen. Het model bestaat uit vijf bouwstenen die in dit artikel op een samenhangende wijze en high level-niveau zijn gevisualiseerd. De bouwstenen zijn tevens nader beschreven in hun functie om cyberrisico's ook op tac-

tisch en operationeel niveau te beheersen. In het modelontwerp komt terug dat beheersing van cyberrisico's een continue proces is en dus een cyclische benadering vergt. Daarnaast dient rekening gehouden te worden met hun partner-organisaties en de eco-systemen waar organisaties deel van uit maken. Deze bepalen mede het cyberlandschap en cyberrisico's. Verweven door alle bouwstenen van het model is ook het menselijke aspect, dat een kritieke succesfactor vormt in het beheersen van cyberrisico's.

Ons doel was een model te creëren dat bijdraagt aan een systematische aanpak en integrale beheersing van cyberrisico's. In de praktijk bestaan nog weinig handvatten en methodische aanpakken om als organisatie om te gaan met het steeds groter en complexer wordende cyberlandschap. Het high-level-abstractieniveau van het model maakt het in principe geschikt voor verschillende organisaties. Echter, voor de toepassing van het model is het belangrijk dat organisaties rekening houden met hun bestaande organisatiestructuren en risicomanagementprocessen.

Het in dit artikel beschreven onderzoek en model vormen de eerste stappen op weg naar een betere beheersing van cyberrisico's. Het model bevindt zich in de post-ontwerp en pilot-fase en kan verder onderzocht worden in verschillende richtingen. Een eerste vervolgonderzoek zal zich richten op de kritische succesfactoren voor de implementatie van het model binnen organisaties. Het model is generiek ontworpen wat het geschikt maakt voor verschillende typen organisaties, maar het implementatiesucces ervan zal situationeel bepaald zijn. Een tweede stap voor verder onderzoek is het verbinden van het cyberrisico-beheersingsmodel met het risicomanagement van een organisatie, zoals in *Enterprise Risk Management* (ERM). Hoe dit cybergerelateerde model zo onderdeel kan worden van ERM van een organisatie is een volgende stap. ■

Dr. A. (Abbas) Shahim RE CGEIT CRMA is associate professor aan de Vrije Universiteit Amsterdam (VU) en is tevens partner bij Atos Consulting.

Dr. R.S. (Ronald) Batenburg is associate professor aan de Universiteit Utrecht en is tevens programmaleider bij het Nederlandse Instituut voor Onderzoek van de Gezondheidszorg (NIVEL).

J. (Joost) Geusebroek MSc CISSP is IT Security consultant bij de Nováccent Group (Security & Compliance Services).

Literatuur

- Betz, C.T. (2011). *Architecture and patterns for IT service management, resource planning, and governance*. Elsevier.
- Bodeau, D., Boyle, S., Fabius-Greene, J., &

Graubart, R. (2010). *Cyber security governance*. Geraadpleegd op http://www.mitre.org/sites/default/files/pdf/10_3710.pdf.

- Choo, W-W.R. (2011). *The cyber threat lands-*

capes: Challenges and future research directions. *Computers & Security*, 30(8), 719-731.

- Department of Homeland Security (2009a). *Blueprint for a secure cyber future*. Geraad-

- pleegd op <http://www.dhs.gov/files/publications/blueprint-for-a-secure-cyber-future.shtm>.
- Department of Homeland Security (2009b). National infrastructure protection plan. Geraadpleegd op http://www.dhs.gov/files/programs/editorial_0827.shtm.
 - DiCicco-Bloom, B., & Crabtree, B.F. (2006). The qualitative research interview. *Medical Education*, 40, 314-321.
 - Geers, K. (2011). Strategic cyber security. CCD COE Publication. Geraadpleegd op http://www.ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF.
 - Hult, F., & Sivasenan, G. (2014). What good cyber resilience looks like. *Journal of business Continuity & Emergency Planning*, 7(2), 112-125.
 - ISF (Information Security Forum) (2011). Cyber security strategies: Achieving cyber resilience. Geraadpleegd op <https://www.securityforum.org/shop/p-71-134>.
 - ITGI (IT Governance Institute) (2006). *Information security governance: Guidance for boards of directors and executive management*. 2nd edition. ITGI.
 - Ottis, R., & Lorents, P. (2010). Cyberspace: Definition and implications. Presented at the Proceedings of the 5th International Conference on Information Warfare and Security, Dayton. Geraadpleegd op <http://connection.ebscohost.com/c/articles/49549168/cyberspace-definition-implications>.
 - Ponemon Institute (2011, August). First annual cost of cyber crime study. ArcSight. Geraadpleegd op http://www.hpenterprisesecurity.com/collateral/report/HPEnterpriseSecurity_Report_HPArCSightFirstAnnualCostCyberCrimeStudyPonemon.pdf.
 - Seidel, J.V. (1998). Qualitative data analysis. Geraadpleegd op http://www.qualisresearch.com/qda_paper.htm.
 - Siegel, C.A., Sagalow, T.R., & Serritella, P. (2002). Cyber-risk management: Technical and insurance controls for enterprise-level security. *Information Systems Security*, 11, 33-49.
 - Takeda, H., Veerkamp, P., & Yoshikawa, H. (1990). Modeling design process. *AI Magazine*, 11(4), 37-48.
 - Thayer, J.T., Burstein, M., Goldman, R.P., Kuter, U., Robertson, P., & Laddaga, R. (2013). Comparing strategic and tactical responses to cyber threats. In: Self-Adaptation and Self-Organizing Systems Workshops (SASOW), 2013 IEEE 7th International Conference on pp. 35-40.
 - WEF (The World Economic Forum) (2012). Partnering for cyber resilience. Geraadpleegd op <http://www.weforum.org/issues/partnering-cyber-resilience-pcr>.
 - Vaishnavi, V., & Kuechler, W. (2008). Design research in information systems. In: V. Vaishnavi and W. Kuechler (eds.), *Order: a Journal on the Theory of Ordered Sets and its Applications*. Auerbach.
 - Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, 23, 371-376.
 - White, M.D., & Marsh, E.E. (2006). Content analysis: A flexible methodology. *Library Trends*, 55(1), 22-45. Geraadpleegd op <http://hdl.handle.net/2142/3670>.
 - Whitman, M.E., & Mattord, H.J. (2011). *Principles of information security*. Cengage Learning.
 - Wiener, N. (1948). *Cybernetics or control and communication in the animal and the machine*. New York: John Wiley.
 - Williams, P., & Manheke, R. (2010). Small business - A cyber resilience vulnerability. International Cyber Resilience Conference. Geraadpleegd op <http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1013&context=icr>.