Oude Waalsdorperweg 63
2597 AK Den Haag
Postbus 96864
2509 JG Den Haag

www.tno.nl

T +31 88 866 10 00
F +31 70 328 09 61

TNO-rapport

Kwantificering cyberrisico's: rapportage 2020

Datum	3 december 2020
Auteur(s)	Peter Langenkamp, Marie Beth van Egmond, Marieke Klaver
Exemplaarnummer	
Oplage	
Aantal pagina's	27
Aantal bijlagen	
Opdrachtgever	
Projectnaam	
Projectnummer	

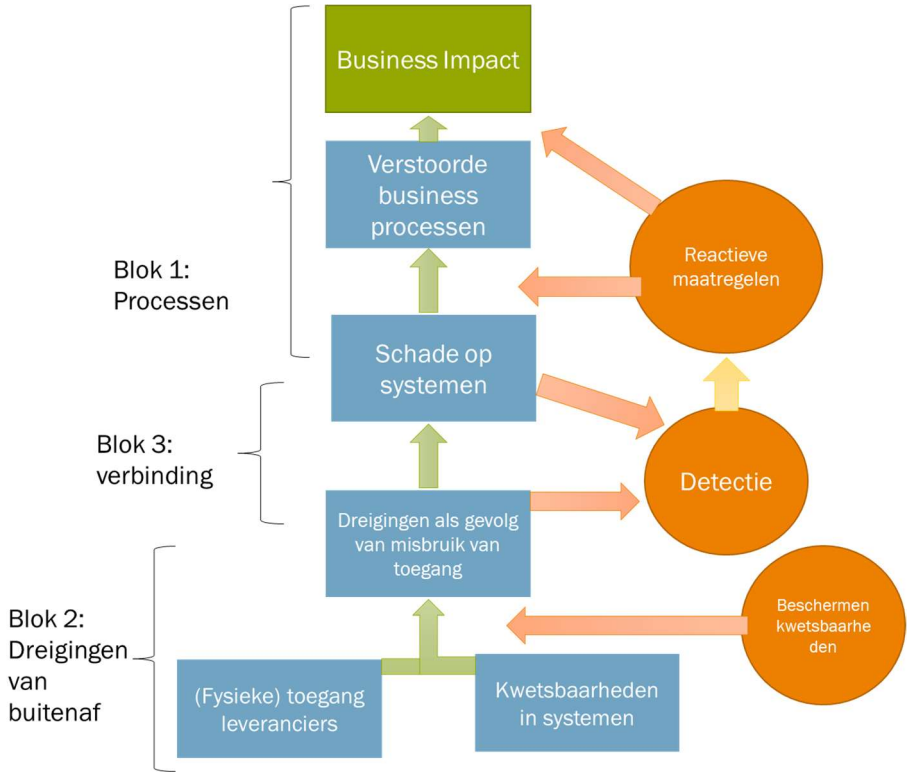
Inhoudsopgave

Management samenvatting

Aanleiding en werkwijze
Veel van de momenteel voor cybersecurity uitgevoerde risicoanalyses zijn kwalitatief van aard. Dit gebrek aan kwantitatieve inschattingen van de mogelijke risico's en daarbij behorende schade maakt het soms moeilijk om de voor cybersecurity benodigde investeringen te agenderen bij organisaties waar niet altijd draagvlak is voor het investeren in digitale beveiliging.
Een mogelijk aanknopingspunt om dit te versterken is het integreren van cyberrisico's met bestaand risicomanagement. Dit onderzoek richt zich op methoden om cyberrisico's meer kwantitatief in kaart te brengen en af te wegen hoe deze zich verhouden tot andere bedrijfsrisico's. Om maximaal te kunnen aansluiten op de bestaande praktijk rond cyber risicoanalyses worden deze mogelijke methoden getoetst en verder ontwikkeld in casestudies met organisaties uit de vitale infrastructuur.
In de werkzaamheden voor 2020 heeft de nadruk gelegen op het verder ontwikkelen van een methodiek voor het kwantificeren van cyberrisico's en het toetsen van deze methodiek in een case studie. Om de bredere toepasbaarheid te toetsen is het geanonimiseerde model en resultaat besproken met een andere vitale organisatie.

Bereikte resultaten
Het onderzoek heeft de volgende resultaten opgeleverd.

Snelle opzet van een basismodel
In de case studie bleek het mogelijk om op basis van een aantal overleggen met de vertegenwoordiger van de case studie en op basis van sectorspecifieke informatie snel een eerste opzet voor een basismodel te maken. De generieke opzet van het model bood de mogelijkheid om reeds bij de case organisatie beschikbare informatie te integreren en het relatief snel (in de eerste workshop) meer bedrijfsspecifiek te maken. De case studie liet zien dat de opzet van het basismodel voldoende herkenbaar bleek voor de verschillende deelnemers uit de case organisatie.
Ook voor een andere vitale organisatie bleek de hoofdstructuur van het model zeer herkenbaar. De organisatie herkende hierin een *bowtie* structuur die door hen wordt gebruikt. Ook de systematiek van de keuze voor verschillende routes door het model sprak aan ("knikkerbaan").



Figuur 1: gelaagde opzet van het basismodel

Opbouw gezamenlijk beeld verschillende expertises
Tijdens de eerste workshop met de case organisatie hielp het model bij het opbouwen van een gezamenlijk beeld van de samenhang tussen systemen en bedrijfsprocessen. Aan de workshop werd deelgenomen door medewerkers met een verschillende achtergrond (zowel IT- als OT-expertise, zowel technisch als meer bedrijfsvoering gericht). Het bijeen brengen van de verschillende expertises binnen de organisatie leidde tot nieuwe inzichten in de mogelijke effecten van het beschouwde scenario en de onderlinge relaties tussen de systemen en de bedrijfsprocessen.

Kwantificering bleek niet mogelijk door gebrek aan gegevens
In de tweede workshop werd duidelijk dat het voor de deelnemers uit de case organisatie moeilijk was om de gevraagde kwantitatieve inschattingen te maken. Dit expliciet maken van inschattingen en afwegingen bleek vooral moeilijk door gebrek aan ervaringscijfers binnen de case organisatie.
Ook de andere vitale organisatie gaf aan dat het maken van kwantitatieve inschattingen een uitdaging is. Hierbij werd een onderscheid gemaakt tussen verschillende dreigingen. Zo werd aangegeven dat een kwantitatieve inschatting wel mogelijk is voor een deel van de dreigingen (bijv. DDoS). Hiervoor zijn voldoende ervaringscijfers beschikbaar. Voor andere typen dreigingen (bijv. advanced persistent threats) is dit niet het geval. Van de methodiek sprak vooral het expliciet maken van de inschattingen aan de hand van de modelstructuur aan. Ook de hierbij behorende kanstabellen werden als meerwaarde gezien.

1 Inleiding

1.1 Achtergrond en probleemstelling

Het kunnen kwantificeren van de mogelijke risico's en daarbij behorende schade is een middel om cybersecurity te agenderen bij organisaties waar niet altijd draagvlak is voor het investeren in digitale beveiliging. Veel van de momenteel voor cybersecurity uitgevoerde risicoanalyses zijn kwalitatief van aard. Er wordt nog niet systematisch data verzameld om kwantitatieve inschattingen mee te kunnen maken. Historische data van financiële instellingen en verzekeraars, en bijvoorbeeld de jaarlijkse incidentenoverzichten van ENISA kunnen een potentieel startpunt vormen. Daarnaast ligt er ook een behoefte om de complexiteit en onderlinge verbanden op een begrijpelijke manier te verwerken en toe te passen in organisaties, om zo besluitvorming in organisaties te verbeteren. Een mogelijk aanknopingspunt hiervoor is het integreren van cyberrisico's met bestaand risicomanagement. De uitdaging hierin is het in kaart brengen van cyberrisico's en hoe deze zich verhouden tot andere bedrijfsrisico's. Om maximaal te kunnen aansluiten op de bestaande praktijk rond cyber risicoanalyses zal het onderzoek zich richten op casestudies uit de vitale processen. Hierbij wordt voortgebouwd op kennis opgedaan uit andere domeinen.

1.2 Doelstelling van het onderzoek

Het onderzoek kent de volgende doelstellingen:

- het ontwikkelen van een methode voor het kwantificeren van de mogelijke cyberrisico's en daarbij behorende schade,
- het ontwikkelen van daarbij ondersteunende datasets,
- het integreren met bestaande risicomanagement-methodieken.

De werkzaamheden in 2020 richtten zich op de eerste doelstelling. De overige doelstellingen zullen in 2021 en 2022 worden uitgewerkt.

1.3 Dit document

Dit document beschrijft achtereenvolgens de werkwijze tijdens het project, het resultaat van de literatuurstudie, het voor de case studie ontwikkelde model en het resultaat van de case studie.
Het laatste hoofdstuk bevat een reflectie op de resultaten en een aantal richtingen voor vervolgwerkzaamheden.

2 Werkwijze

2.1 Aanpak

Dit meerjarige onderzoek richt zich op het versterken van de kwantitatieve vertaling van cybersecurityrisico's op bedrijfsniveau.
Om te bepalen waar organisaties in de vitale sectoren tegenaan lopen bij het kwantificeren van cyberrisico's in hun risicomanagementproces wordt een eerste case studie uitgevoerd. Hierbij wordt nagegaan welke knelpunten worden ondervonden bij het identificeren en kwantificeren van cyberrisico's en welke behoefte bestaat aan aanvullende tools of data.
Daarnaast wordt voor het identificeren van mogelijke oplossingsrichtingen een literatuuronderzoek uitgevoerd naar innovatieve methoden voor het kwantificeren van cyberrisico's. Het literatuuronderzoek richt zich op de mogelijke toepassing van simulaties en andere modellen en op methoden voor de kwantificatie (benoemen metrics, categorie-indelingen van incidenten, mogelijke sector-overstijgende factoren). Hierbij wordt voortgebouwd op eerder TNO onderzoek. In deze opzet werden mogelijke dreigingen gemodelleerd, waarna het model wordt gevoed met actuele en historische informatie.
Daarnaast wordt gezocht naar de beschikbaarheid van ondersteunende gegevens in het cyberdomein. Hierbij wordt ook gebruik gemaakt van eerdere ervaringen met een door TNO ontwikkelde incidentendatabase voor incidenten in de vitale sectoren[1].
Vervolgens vindt de analyse plaats van de resultaten van de case studie en de literatuurstudie. Het resultaat van deze analyse is vastgelegd in het laatste hoofdstuk van dit document. Op basis van de resultaten en de bevindingen wordt een voorstel gedaan voor de richting van de vervolgwerkzaamheden.

2.2 Werkzaamheden in 2020

In 2020 is de literatuurstudie uitgevoerd. Hiervoor zijn de recente ontwikkelingen rond kwantificering van cyberrisico's beschouwd. Tevens is gezocht naar ondersteunende datasets.
Vervolgens is een case studie uitgevoerd bij een organisatie. Voor de selectie van de case studie zijn een aantal gesprekken gevoerd met geïnteresseerde organisaties. Tevens is de aanpak van de case studie uitgewerkt. In nauw overleg met de bij de case betrokken organisatie zijn de doelstelling en werkwijze voor de case studie nader aangescherpt. Hierbij wordt aandacht besteed aan:

- de gezamenlijk overeen gekomen doelstelling,
- de uit te voeren werkzaamheden,
- de benodigde informatie en de planning (doorlooptijd en gewenste afstemmingsmomenten).

Tevens zijn in deze fase afspraken gemaakt over de vertrouwelijkheid van de informatie. Hiervoor is een Non-Disclosure Agreement (NDA) opgesteld.
Na de afronding van de case studie zijn de resultaten besproken met de bij de case studie betrokken organisatie. Om een breder beeld te krijgen van de

[1] Zie hiervoor bijvoorbeeld de rapportage: Luiijf, Klaver, Quick-Scan Analyse TNO's Critical Infrastructure Incident Database, juli 2016 (vertrouwelijk).

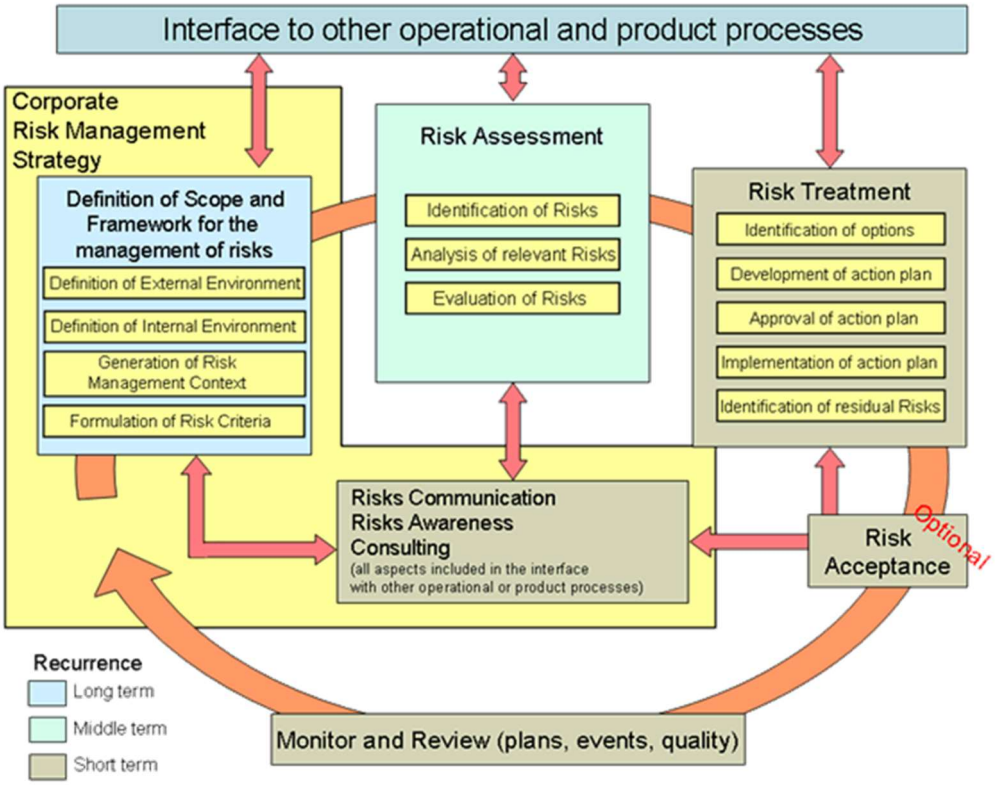
toepasbaarheid van het model, is het geanonimiseerde model en resultaat besproken met een andere vitale organisatie.

Op basis van de ervaringen en de feedback is een aantal richtingen voor vervolgwerkzaamheden geïdentificeerd. Hiervan worden in overleg met de klankbordgroep de meest relevante en kansrijke optie geselecteerd.
In de vervolgfases van het onderzoek wordt deze oplossingsrichting verder uitgewerkt, en vindt het ontwerp en de ontwikkeling plaats van eventueel benodigde tools en datasets. Tevens wordt de oplossingsrichting getoetst in de volgende case studies.

3 Literatuurstudie naar kwantificering cyberrisico's

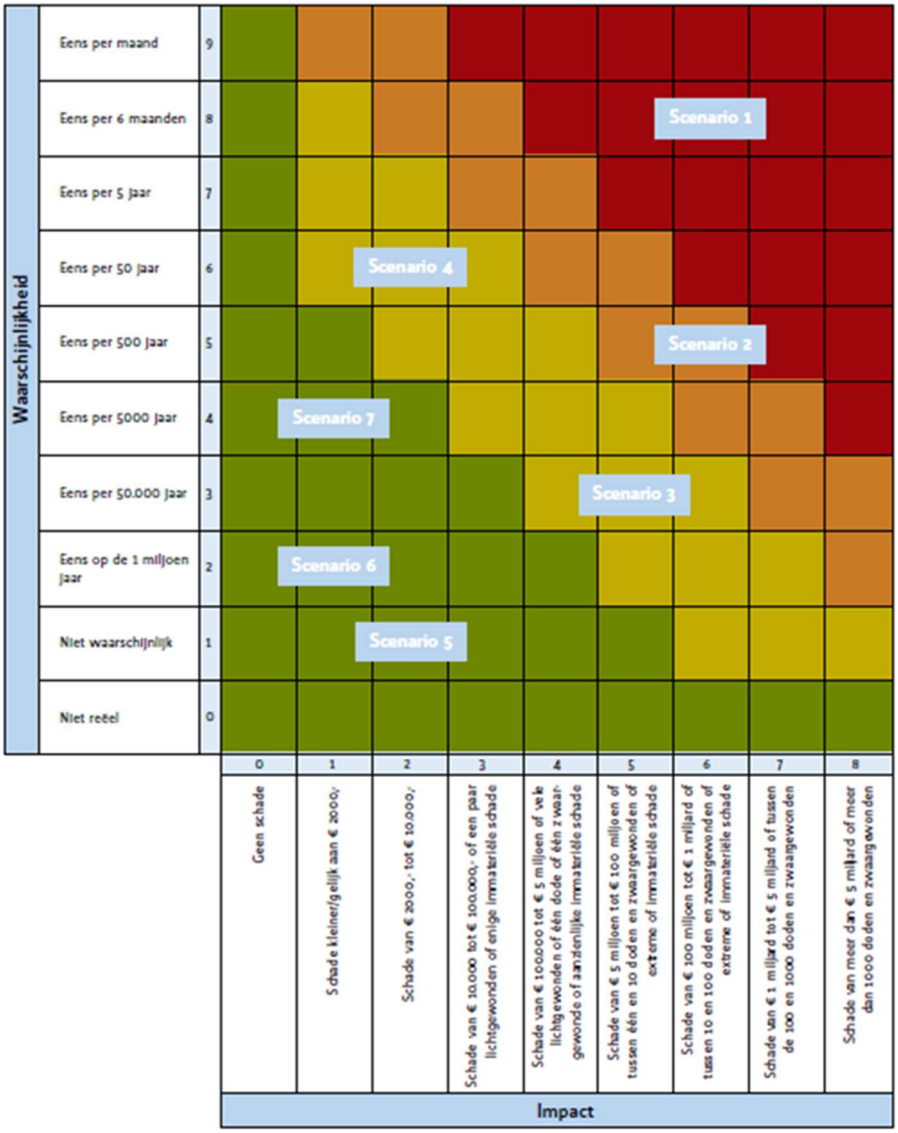
3.1 Inleiding risicomanagement

Er bestaan diverse methoden voor risicomanagement. Vrijwel alle vitale sectoren gebruiken methoden voor risicomanagement, zowel voor safety als voor security risico's. Ook bestaan er meerdere risicomanagement methoden en tools die specifiek gericht zijn op cybersecurity en/of de vitale infrastructuur (zie bijvoorbeeld het overzicht van ENISA [6], of van JRC [8]).
In vrijwel alle methoden is eenzelfde standaardstructuur goed herkenbaar.



Figuur 2: structuur risicomanagement (bron: ENISA, [6])

De resultaten van een risicoanalyse worden veelal inzichtelijk gemaakt door middel van risicodiagrammen (*risk heat map*).



Figuur 3 : voorbeeld van een risk heat map [11]

Deze diagrammen bieden een overzicht van de waarschijnlijkheid en de impact van mogelijke risico's. Binnen cybersecurity risicomanagement zijn deze inschattingen veelal kwalitatief van aard.
In aanvulling op deze kwalitatieve methoden zijn er een aantal ontwikkelingen in gang gezet om de risico's ook meer kwantitatief in beeld te brengen. Een overzicht van dergelijke ontwikkelingen is bijvoorbeeld te vinden bij Waldron15]). Er zijn zowel voor- als nadelen te onderkennen in kwantitatief risicomanagement ten opzichte van kwalitatief risicomanagement.

	Voordeel	Nadeel
Kwalitatief	• Kwalitatieve inschattingen zijn gemakkelijker te maken.	• Meer subjectief van aard. • Moeilijker om (automatisch) de

	Voordeel	Nadeel
	• Een kwalitatieve insteek is bekend bij veel organisaties. • Op het eerste gezicht eenvoudiger te interpreteren, men hoeft geen getallen in perspectief te plaatsen.	nauwkeurigheid van inschattingen te monitoren. • Minder stevige basis voor investeringsbeslissingen
Kwantitatief	• Inschattingen van aspecten als waarschijnlijkheid, impact en kosten van maatregelen worden expliciet gemaakt. • De nauwkeurigheid van eerdere inschattingen kan beter (automatisch) worden gemonitord waardoor de inschattingen in de loop der tijd kunnen worden verbeterd. • De resultaten sluiten nauwer aan bij andere investeringsbeslissingen op managementniveau.	• Het maken van kwantitatieve inschattingen is veelal complex en kan een grote inspanning vergen. • Er is een historische gegevensbasis gewenst als startpunt voor de inschattingen. • Minder concrete maatregelen (bijv. awareness) kunnen lastig in een kwantitatief model op te nemen zijn.

Voor de kwantificering van cyberrisico's richt het onderzoek zich vooral op de volgende twee variabelen die centraal staan in de resultaten van een risicoanalyse:

- inschattingen van de mate van waarschijnlijkheid,
- inschattingen van de mate van impact.

Recent zijn er een aantal methoden ontwikkeld die deze beide variabelen sterker kwantitatief proberen te onderbouwen. Hierbij wordt een probabilistische aanpak toegepast**.** Hierbij worden de impact en waarschijnlijkheid gerepresenteerd met behulp van kansverdelingen. Deze geven aan hoe waarschijnlijk de verschillende mogelijke eindtoestanden zijn gegeven een bepaalde begintoestand (bijvoorbeeld kennis over middelen van dreigingsactoren).

3.2 Probabilistische methoden

Er bestaan een aantal methoden die binnen de traditionele risico-inschattingen voor cybersecurity probabilistische functies introduceren. Per methode wordt aangegeven wat het resultaat is, en of er ondersteunende tools en datasets beschikbaar zijn.

FAIR methodiek

De methodiek Factor Analysis of Information Risk (FAIR) is een vooraanstaande kwantitatieve risicomanagementmethode op het gebied van cybersecurity. De methodiek ondersteunt de prioritering van risico's en maatregelen door gebruik te maken van vooraf gedefinieerde modellen en economisch gerichte schalen voor de beoordeling [13, 14].

FAIR gebruikt een standaard onderverdeling van de assen 'frequentie' en 'impact'. Door gebruik te maken van een gestructureerde werkwijze en gestandaardiseerde schalen wordt beoogd onderling vergelijkbare analyses en uitkomsten te verkrijgen. De methode maakt gebruik van probabilistische functies en volgt een gestructureerd stappenplan.

Resultaat

De resultaten van een risicoanalyse met FAIR worden vaak samengevat in een risicotabel. De onderstaande figuur geeft een voorbeeld van de mogelijke output.

	Minimum	Average	Mode	Maximum
Primary				
Loss Events/Year	0.05	0.17	0.14	0.43
Loss Magnitude	$70,805	$393,005	$441,760	$784,037
Secondary				
Loss Events/Year	0.02	0.07	0.05	0.17
Loss Magnitude	$248,815	$3,689,381	$1,102,702	$17,564,462
Total Loss Exposure	$28,319	$316,229	$172,200	$1,908,713

Figuur 4: voorbeeld van de mogelijke output van een FAIR analyse

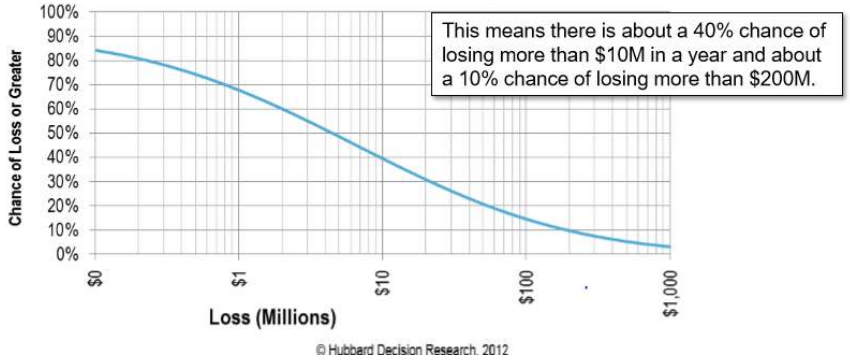
Ondersteunende tools en /of datasets

De FAIR methodiek is geïntegreerd in de RISKLens tool. Daarnaast zijn er tools beschikbaar via bijvoorbeeld GitHub. De methodiek wordt bijvoorbeeld gebruikt in combinatie met de dataset van Advisen waarin data wordt omgezet in mogelijke startwaarden voor FAIR (IRIS 2020).

Hubbard en Seiersen

Hubbard en Seiersen [9] betogen dat de kwalitatieve 'risk heat maps' niet voldoende expliciet zijn om de risico's inzichtelijk te maken voor de board. Ze beschrijven in hun boek een methode om door middel van relatief simpele probabilistische functies cybersecurity beter meetbaar te maken. De methodiek maakt gebruik van statistische en Monte Carlo methoden om de waarschijnlijkheid van risico's nauwkeuriger in te schatten. Tevens kunnen de inschattingen nader worden aangescherpt als er meer informatie beschikbaar komt. Het resultaat wordt niet gerepresenteerd door risk heat maps, maar door zogeheten 'loss exceedance' curves.

Resultaat
Het resultaat wordt vastgelegd in een zogeheten ‘loss exceedance curve’. Hierin wordt aangegeven hoe groot de kans is dat de schade beneden een bepaald bedrag valt (x-as).



Figuur 5: voorbeeld van een loss exceedance curve

Ondersteunende tools en /of datasets
Het boek van Hubbard en Seiersen beschrijft een werkwijze voor het maken van probabilistische inschattingen.

Gebruik Bayesian Belief Networks voor de financiële sector
TNO heeft in het kader van eerder onderzoek een kwantitatieve risicomanagement methode ontwikkeld. De methode richt zich op het kwantificeren van de waarschijnlijkheid van het optreden van een risico en maakt hiervoor gebruik van modellering op basis van Bayesian Belief Networks (BBN). In het model staat het dreigingsscenario centraal. Bij de beoordeling van de waarschijnlijkheid van de verschillende risico’s worden de assets en maatregelen meegenomen. Tevens is ondersteunende tooling beschikbaar.

Resultaat
Het resultaat van de methodiek is een kansverdeling. Voor een specifiek dreigingsscenario wordt een kansverdeling bepaald van de mogelijke (vooraf gedefinieerde) impactniveau's van de Business Impact waarvoor gemodelleerd wordt.

Ondersteunende tools en /of datasets
Bij de methode hoort een basismodel en zijn processtappen beschreven voor het uitvoeren van een risicoanalyse voor een bepaald dreigingsscenario. Daarnaast zijn ondersteunende tools beschikbaar o.a. voor het invullen van de benodigde kanstabellen.

Overige ontwikkelingen
Naast de hierboven beschreven aanpakken werkt de organisatie Internet Security Forum aan methoden voor de kwantificering van cyberrisico’s. Hierover bleek geen gedetailleerde informatie vrij beschikbaar.

3.3 Beschikbare gegevens

De genoemde methoden verschillen op een aantal punten, maar hebben gemeen dat de beschikbaarheid en standaardisatie van de benodigde onderliggende gegevens een belangrijke uitdaging is [17]. De uitdagingen gelden op de volgende punten [17]:

- beschikbaarheid van data en standaard formats, met meer specifiek historische data rond incidenten en risico's.
- standaardisatie van de bepaling van de impact, bijvoorbeeld ook in het meenemen van minder grijpbare aspecten zoals bijvoorbeeld imagoschade.
- geringe bereidheid om data te delen.

Voor het gebruik van deze gegevens is een generieke structuur gewenst. Hierin zijn een aantal ontwikkelingen, maar er is nog geen standaard taxonomie beschikbaar. Op basis van de case studies zal worden bepaald aan welk type informatie het sterkst behoefte is en welke structuur het beste aansluit bij de behoefte van vitale organisaties die vanuit de case studies naar voren komt.

3.4 Conclusies voor de opzet van de eerste case studie

Op basis van de beschikbaarheid van tools, en de reeds bewezen toepasbaarheid voor een Nederlandse vitale sector, wordt voor de eerste case studie de BBN methode als uitgangspunt gebruikt. Deze richt zich op de waarschijnlijkheid. Voor de inschatting van de impact lijkt de FAIR methodiek of Hubbard goede mogelijkheden te bieden.
Voor de eerste case studies wordt derhalve een combinatie gebruikt van de bovenstaande methoden. Hiervoor wordt de volgende werkwijze gekozen:

- Het stappenplan op basis van BBN voor het inschatten van de waarschijnlijkheid,
- Indien gewenst wordt de aanpak aangevuld met de FAIR methodiek of Hubbard voor het inschatten van de impact.

4 Opzet en resultaat van een case

Dit hoofdstuk bevat een geanonimiseerde beschrijving van de case studie. In een aanpalende vertrouwelijke rapportage worden de resultaten teruggekoppeld naar de organisatie waar de case is uitgevoerd.

4.1 Werkwijze case studie

De case studie werd in een aantal fases onderverdeeld. In de eerste fase is basisinformatie verzameld betreffende: relevante dreigingen, dreigingsactoren, assets, business processen en mitigerende maatregelen bij de organisatie. Op basis van deze informatie heeft TNO in de tweede fase gewerkt aan een eerste basismodel voor kwantificering van waarschijnlijkheden, met de intentie deze in de laatste fase verder uit te werken aan de hand van enkele workshops met experts (zie "Workshops") van desbetreffende organisatie.

4.1.1 Verzamelen basisinformatie

In de eerste fase van de case studie is schriftelijk basisinformatie uitgevraagd aan de hand van de volgende punten.

1. Informatie over de op dit moment gebruikte risicomethode, bijvoorbeeld een *bowtie*-analyse. Hierbij kan gedacht worden aan:
    a. De eventueel gebruikte methoden voor het inschatten van waarschijnlijkheden en impact.
    b. Eventueel gebruikte ondersteunende tools.
    c. De frequentie waarmee risicoanalyses worden gemaakt of bijgewerkt
    d. De typen functionarissen die normaliter bij het analyseproces betrokken zijn.
2. Informatie over de risico-inschatting voor de betreffende dreiging en over de business impact analyse voor de betreffende dreiging. Hierbij valt te denken aan:
    a. De uitkomst(en) van recente analyses en;
    b. voor zover (eenvoudig) beschikbaar, informatie over aannames en overwegingen die tijdens het analyseproces gemaakt zijn.
3. De voor de dreiging relevante business processen en assets. Maatregelen die zijn genomen tegen de dreiging.
    a. Processen en assets zijn relevant als ze mogelijk het directe doelwit zijn, maar ook als ze een 'ingang' bieden en lateral movement mogelijk maken, dan wel een ander proces of asset kunnen ontregelen.
    b. Wat zijn de directe onderlinge afhankelijkheden tussen processen en assets? i.e. als asset x succesvol wordt aangevallen, heeft dat consequenties voor proces y?
    c. Maatregelen kunnen preventief zijn (i.e. voorkomen dat een aanval slaagt), maar ook mitigerend (i.e. beperken van eventuele impact bij een geslaagde aanval). Ook kunnen maatregelen variëren van het voorlichten van medewerkers, tot technische oplossingen.
4. Informatie over dreigingsactoren en hun motivatie
    a. Dit kan vrij algemene categorieën betreffen zoals: activisten, criminelen, 'Scriptkiddy', buitenlandse mogendheden. Maar als daar

aanleiding toe is, kunnen ook specifieke partijen worden opgenomen.
b. Motivaties zoals: aandacht, geld, afpersing, informatie
c. Dit hoeft zich niet te beperken tot enkel de top 2 of 3 van dreigingsactoren, maar ook andere actoren waar tijdens een analyse aandacht aan is besteed.

4.1.2 Analyse door TNO en ontwikkeling basismodel

De door de organisatie aangeleverde informatie is door TNO geanalyseerd en gebruikt om aan de hand van de kwantitatieve BBN methodiek te werken aan een eerste versie van het basismodel (zie sectie 4.2) en deze zoveel mogelijk te vullen op basis van de bestaande informatie. De ontwikkeling van het basismodel is uitgevoerd door TNO waarbij de case organisatie beschikbaar was voor aanvullende vragen.

4.1.3 Workshops

Tot slot zijn er twee workshops georganiseerd. De deelname vanuit de organisatie werd in samenspraak vastgesteld. Voor de deelnemers werd gedacht aan een bijdrage van de volgende rollen: business verantwoordelijke (proceseigenaren), CISO, Risicomanager, Cyber Threat Intelligence experts, en security architecten / cyber experts. Het streven was om met twee workshops van een dagdeel het model verder uit te werken. Ter voorbereiding op de eerste workshop was in een korte sessie tezamen met de organisatie gekeken naar de verdere afbakening. Hierbij stond centraal wat de precieze dreiging is waar de organisatie bezorgd over is. De exacte vraag die de organisatie graag beantwoord wilde zien is bepalend voor de invalshoek voor de dreiging en daarmee het startpunt van het model.

De eerste workshop was gericht op de elementen die in het model moeten worden opgenomen en hoe deze met elkaar in verbinding staan. Tevens had de workshop tot doel te identificeren over welke business impact de organisatie bezorgd was; wat de effecten konden zijn van de dreiging en wanneer heeft bijvoorbeeld het slecht functioneren van kritieke high-level assets (grote) gevolgen voor de bedrijfsresultaten.

De tweede (en tevens laatste) workshop had als doel de elementen van het model in meer detail te behandelen met als de uiteindelijke intentie het inschatten van waarschijnlijkheden (dat iets in het model zich voordoet, en of iets consequenties heeft voor een volgend element in het model), waar mogelijk mede aan de hand van historische gegevens.

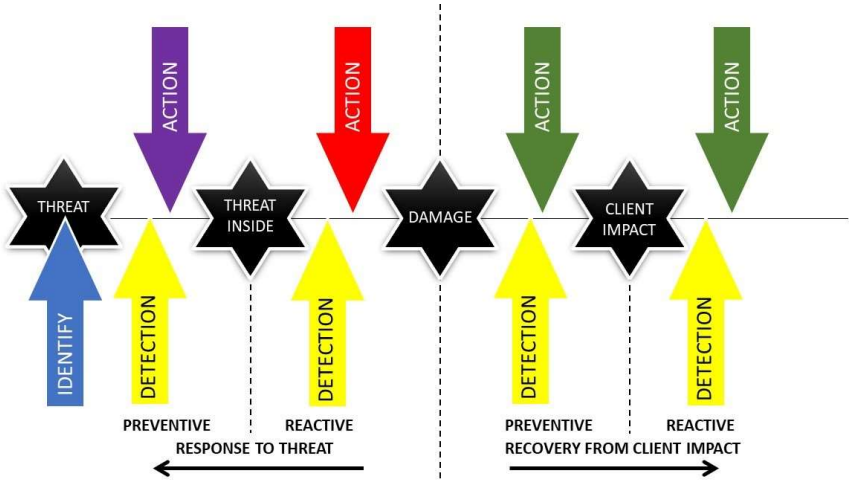
4.2 Basismodellen

Het uitgangspunt van deze case studie was het onderzoeken van ‘toegang van externe leveranciers’. De onderzoeksvraag die in samenwerking met de case organisatie was vastgesteld, luidde als volgt: :

- Wat is het effect van bepaalde maatregelen op de mogelijke schadelijke gevolgen van (fysieke) toegang van externe leveranciers?

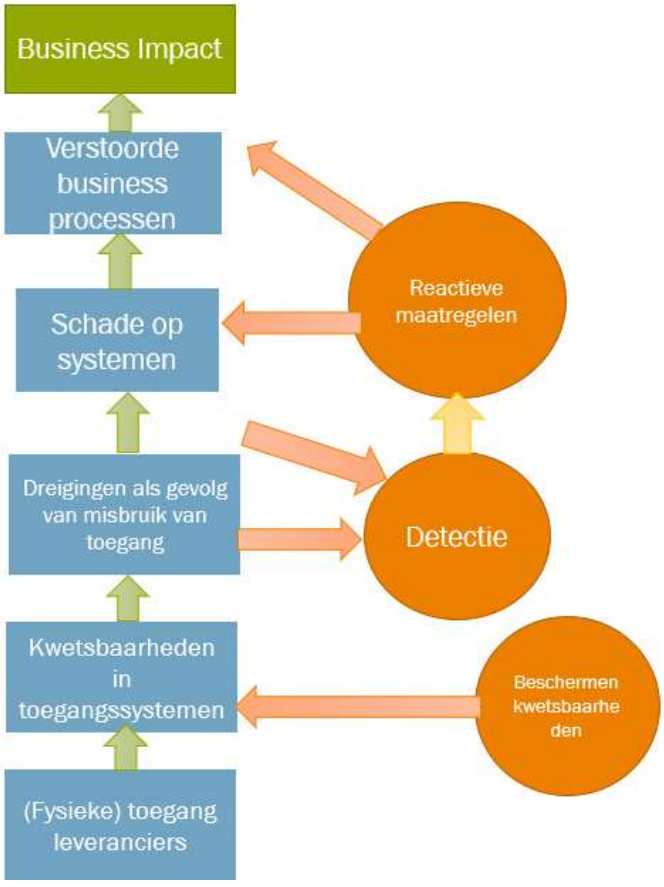
In het basismodel, zie Figuur 7, voor het kwantificeren wordt gekeken naar de verschillende fases van de dreiging: ‘(original) threat’, ‘threat inside’, ‘damage’ en

'client impact'. Gerelateerd aan deze fases zijn de preventieve en reactieve maatregelen in de vorm van detectie en mitigerende acties.



Figuur 6 *Basismodel kwantificeren van cyberrisico's*

Voor de specifieke onderzoeksvraag hebben we dit generieke basismodel vertaald naar een basismodel voor deze case, zie Figuur 7.



Figuur 7: *Basismodel use case*

Belangrijk om op te merken in dit model is dat ‘dreigingen als gevolg van misbruik van fysieke toegang’ vaak kunnen ontstaan via bepaalde kwetsbaarheden in systemen. Een van de experts beschreef dit als volgt: ‘Je hebt een goed beveiligd huis, maar er komen steeds meer ramen bij die het huis kwetsbaarder maken’.
In de uitwerking van het basismodel hebben we gekeken naar de invulling van de individuele blokken. We hebben hier met name gefocust op het identificeren van de kwetsbaarheden in systemen, welke dreigingen deze tot gevolg hebben en wat voor beschermende maatregelen er al bestaan en nog zouden kunnen worden ingevoerd.

4.3 Uitwerking basismodel

Op basis van de workshops is het basismodel verder uitgewerkt, het resulterende model staat in Figuur 8 weergegeven. Per laag in het model (van onder naar boven) zullen we de observaties beschrijven.

Verschillende soorten leveranciers & Moedwilligheid
In de workshops kwam naar voren dat het belangrijk is om een onderscheid te maken tussen dreigingen die moedwillig dan wel niet-moedwillig plaatsvinden. In het eerste geval heeft een leverancier (bijvoorbeeld uit een risicoland) kwade bedoelingen en kan deze bijvoorbeeld via een kwetsbaarheid proberen data te stelen. In het tweede geval kan er bijvoorbeeld door middel van een typefout een verkeerde configuratie ontstaan. Uit de workshop kwam naar voren dat de opdeling van verschillende soorten leveranciers op meerdere manieren gedaan zou kunnen worden, bijvoorbeeld:

- Risicoland/ niet-risicoland.
- Nederlands/EU/buiten EU.
- Al bekende leverancier/ nieuwe leverancier.

Op basis van de gekozen indeling van leveranciers kan er een verband worden gelegd naar het blokje van moedwilligheid: Hoe groot is de kans dat leverancier van type X moedwillig kwaad wil doen aan de organisatie?

(Kwetsbaarheden in) toegangssystemen (Remote & On site)
De toegangssystemen zijn primair op te delen in remote en on site toegang, waarbij er soms enige overlap mogelijk is. Voorbeelden zijn:

- On site: de mogelijkheid van het insteken van een USB-stick in een computer.
- Remote: Leveranciers nemen soms eigen remote access oplossingen mee. Dit kan een kwetsbaarheid opleveren.

Preventieve maatregelen
In het model zijn een aantal preventieve maatregelen opgenomen, die invloed hebben op de moedwilligheid van leveranciers om schade aan te richten. Voorbeelden hiervan zijn leveranciersmanagement en sancties.

Dataverlies
Apart in het model (de driehoek in het midden) is dataverlies genoemd. Dataverlies kan ontstaan door kwetsbaarheden in de toegangssystemen maar heeft (meestal) geen invloed op de systemen. Dataverlies heeft echter wel impact op de reputatie van de organisatie en kan tot financiële schade leiden.

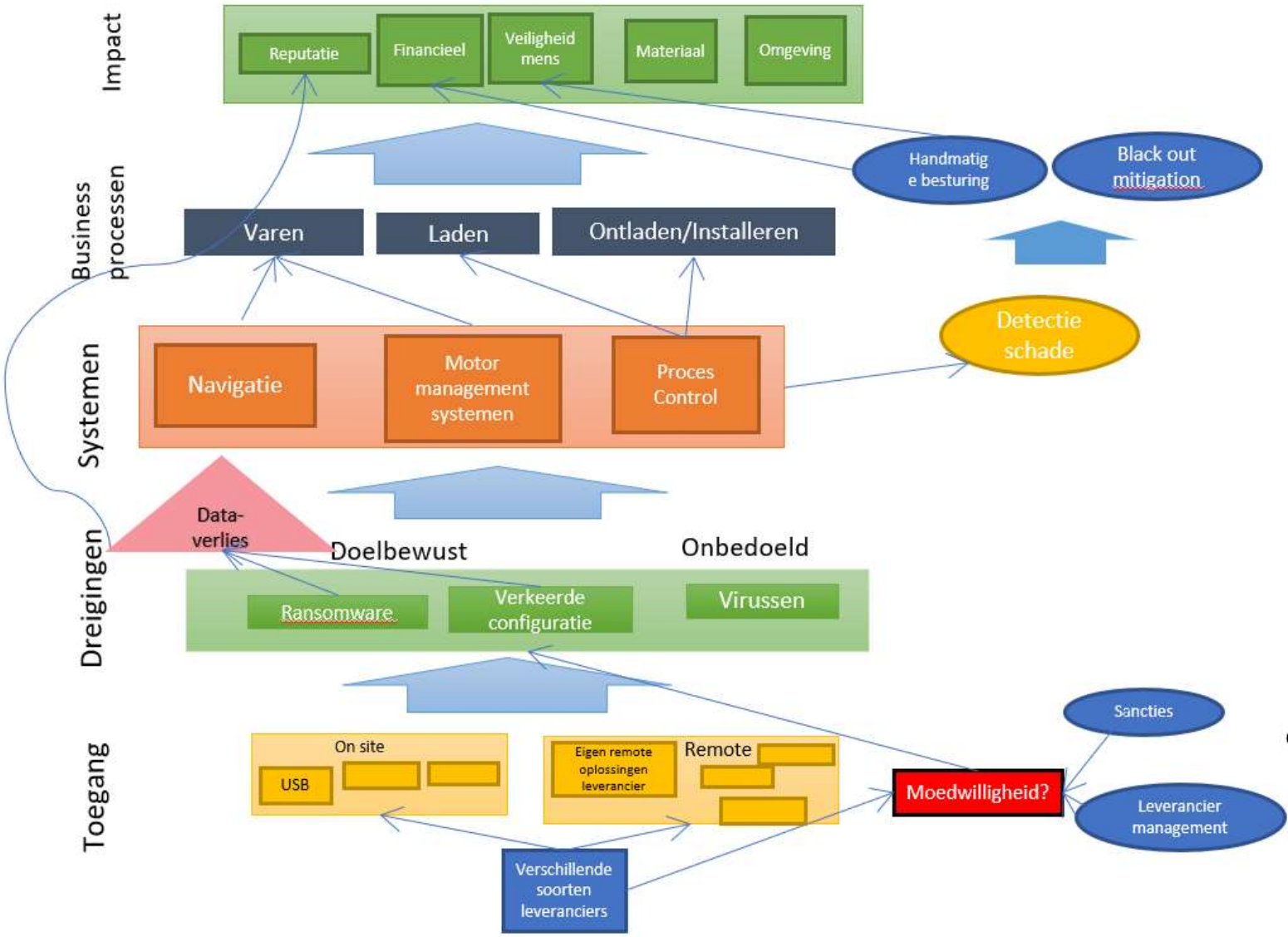
Dreigingen
Uit de workshop kwam naar voren dat het belangrijk is om een onderscheid te maken tussen bedoelde en onbedoelde dreigingen. Ransomware wordt vaak doelbewust ingezet, bijvoorbeeld voor criminele doeleinden. Virussen kunnen onbedoeld het systeem in komen, bijvoorbeeld door de eerder genoemde USB-stick, en liggen minder voor de hand als gerichte aanval. Verkeerde configuraties kunnen zowel doelbewust als onbedoeld voorkomen.

Systemen & detectie
Voor de organisatie, uit de scheepvaartsector, zijn vele systemen te onderscheiden. Een belangrijke observatie van de experts is dat deze systemen nauwelijks los van elkaar te zien zijn en dat mogelijk een bijzonder goed begrip van de relaties tussen de systemen benodigd zal zijn voor een echt gedetailleerde analyse.
Voor het model kozen wij drie categorieën van systemen die binnen dit vraagstuk passen: Navigatie, Motor Management Systemen (MMS) en Process Control. De rechterkant van het model (figuur 8) beschrijft elementen met betrekking tot maatregelen. Als er schade op de systemen wordt gedetecteerd kan dit leiden tot het in werking treden van “blackout mitigation”[2] of zelfs overgaan op handmatige besturing. Overigens kunnen deze maatregelen ook weer effect hebben op de impact . Dit effect kan zowel positief als negatief zijn. Zo zorgt de maatregel “Handmatige besturing” ervoor dat de veiligheid van de mens is gewaarborgd, maar dit brengt ook kosten met zich mee.

Business processen
De business processen van de organisatie zijn ruwweg op te delen in varen, laden en ontladen/installeren. Navigatie en de MMS hebben voornamelijk invloed op het varen, de proces control heeft invloed op het laden en ontladen.

Impact
De impact is te verdelen in reputatie, financieel, veiligheid mens, materiaal en omgeving. Eventueel zou hierin nog een onderscheid gemaakt kunnen worden tussen OT en IT, een wens die werd uitgesproken door de case organisatie vanwege verschillen in de mogelijke impact en consequenties voor besluitvorming.

[2] Dit zijn maatregelen die de uitval van de elektriciteitsvoorziening aan boord van de schepen moeten mitigeren.



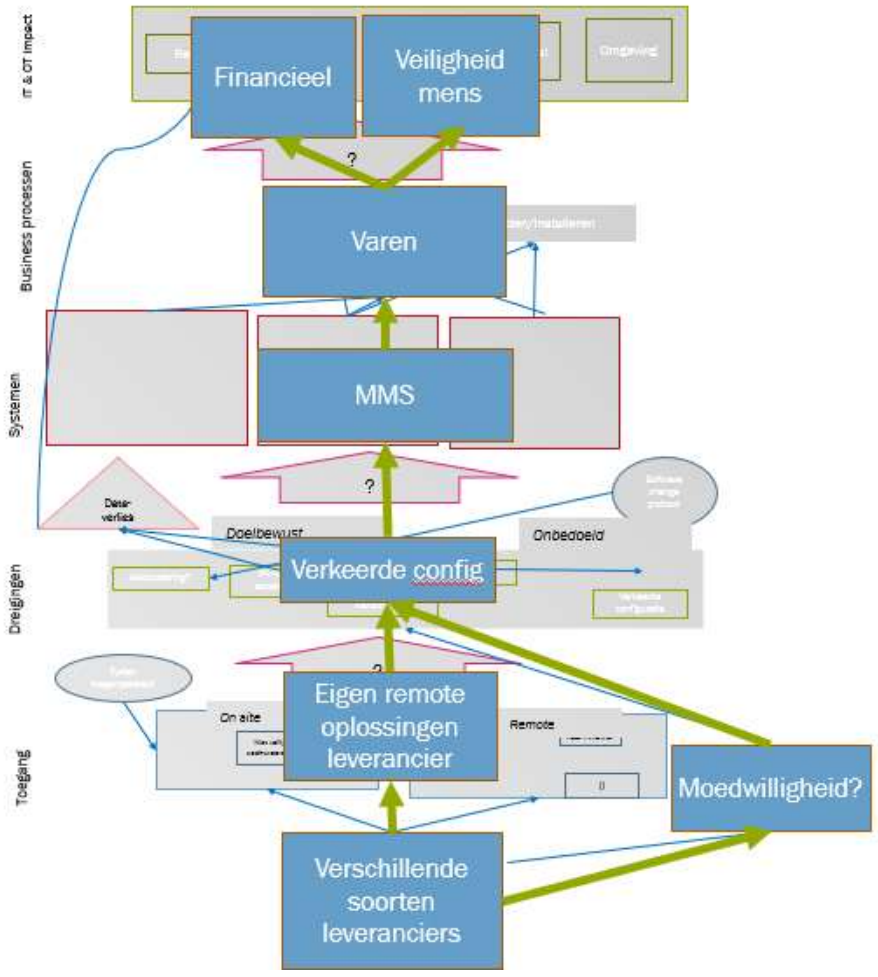
Figuur 8: Uitwerking basismodel (dit is een versimpeling waarin omwille van vertrouwelijkheid bepaalde informatie is weggelaten.)

4.4 Kwantitatief invullen van het model en beantwoorden onderzoeksvraag

De uitwerking van het basismodel in Figuur 8 biedt een overzicht van 'routes' die vanuit een externe leverancier zouden kunnen lopen om, al dan niet moedwillig, schade aan te richten op systemen. Bij het invullen van het model kan men twee kanten op gaan. Een eerste mogelijkheid is het invullen van alle 'blokjes' met als doel een algemeen beeld te schetsen van de situatie. Een andere mogelijkheid is om meer focus te leggen op een specifieke route. In de workshops hebben wij één van deze routes geïdentificeerd om nader te bekijken (zie hieronder). Helaas ontbraken er

ervaringscijfers om daadwerkelijk een kwantitatief antwoord te geven op de onderzoeksvraag.

Eigen remote oplossingen van leveranciers veroorzaken verkeerde configuratie
Een van de geïdentificeerde routes is te zien in Figuur 9. Leveranciers werken soms via eigen remote oplossingen die kwetsbaarheden met zich mee kunnen brengen. Al dan niet moedwillig kan dit resulteren in verkeerde configuraties, wat consequenties heeft voor het Motor Management Systeem (MMS). Dit heeft vervolgens weer invloed op het varen, wat onder andere een gevaar kan opleveren voor de veiligheid van de mens. Door het invullen van de waarschijnlijkheidstabellen van de betrokken elementen in te vullen kan men onderzoeken in hoeverre het toelaten van deze eigen remote oplossingen invloed heeft op de business impact. Zo zou het kunnen zijn dat het aan banden leggen van deze eigen remote oplossingen de kans op financiële impact van deze organisatie verkleint. Aan de andere kant zullen er mogelijk legitieme redenen zijn waarom een organisatie de voorkeur geeft aan een eigen remote oplossing, bijvoorbeeld efficiëntie. Ook zal het afdwingen van een bepaalde manier van werken, afhankelijk van de machtsverhoudingen t.o.v. de organisatie, niet altijd mogelijk zijn.



Figuur 9: Een mogelijke route in het model om nader te onderzoeken.

5 Evaluatie en vervolgstappen

De methodiek die in dit project is gebruikt, bouwt voort op een methodiek die oorspronkelijk is ontwikkeld voor en samen met de financiële sector. Deze ervaringen zijn meegenomen binnen dit project. Voor een korte samenvatting van de ervaringen binnen de financiële sector wordt verwezen naar bijlage A.
Dit hoofdstuk beschrijft de bevindingen van de case studie die binnen dit project is uitgevoerd, en van een korte toetsing van het model bij een ander vitaal bedrijf uit een andere sector. Op basis van deze bevindingen wordt een voorstel gedaan voor de richting van de vervolgwerkzaamheden.

5.1 Evaluatie van de casus en lessons learned

5.1.1 Activiteiten en resultaat van de case studie

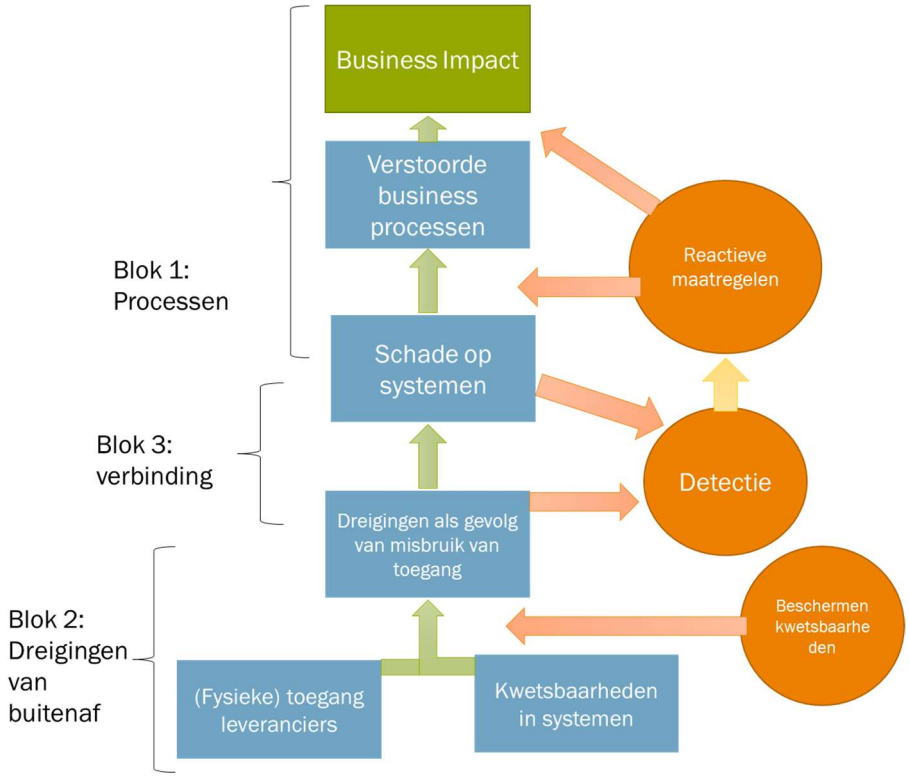
De activiteiten van de case studie bestonden uit een aantal voorbereidende overleggen met de case organisatie, en een tweetal workshops met een aantal vertegenwoordigers uit het bedrijf. In de voorbereidende overleggen is relevante sector specifieke informatie geïnventariseerd en is het te behandelen dreigingsscenario afgebakend. Op basis hiervan heeft TNO een aanzet voor het basismodel ontwikkeld. Dit is vervolgens aangescherpt in de eerste workshop. Voor de tweede workshop die gericht was op het maken van kwantitatieve inschattingen stond een concrete route door dit model centraal.

5.1.2 Positieve punten van de aanpak

Snelle opzet van een basismodel
In de case studie bleek het mogelijk om op basis van een aantal overleggen met de vertegenwoordiger van de case studie en op basis van sector-specifieke informatie snel een eerste opzet voor een basismodel te maken. De generieke opzet van het model bood de mogelijkheid om reeds bij de case organisatie beschikbare informatie te integreren en het relatief snel (eerste workshop) meer bedrijfsspecifiek te maken. De case studie liet zien dat de opzet van het basismodel voldoende herkenbaar bleek voor de deelnemers aan de eerste workshop.

Gelaagde opbouw van het model
De bespreking van het basismodel in de eerste workshop hielp bij het opbouwen van een gezamenlijk beeld bij de deelnemers. Hierbij bleek de geleidelijke opbouw van het model een positieve rol te spelen. Hierbij werd de inhoud van het model gelaagd opgebouwd en toegelicht.

- Blok 1: in het eerste blok staat de mogelijke verstoring van de bedrijfsprocessen en de mogelijke impact daarvan centraal;
- Blok 2: hierin staan de dreigingen van buitenaf centraal,
- Blok 3: hierin staan de effecten en dreigingen op systemen centraal.



Figuur 10: gelaagde opzet van het basismodel

Opbouw gezamenlijk beeld verschillende expertises
Tijdens de eerste workshop hielp het model bij het opbouwen van een gezamenlijk beeld van de samenhang tussen systemen en bedrijfsprocessen. Aan de workshop werd deelgenomen door medewerkers met een verschillende achtergrond (zowel IT- als OT-expertise, zowel technisch als meer bedrijfsvoering gericht). Het bijeen brengen van de verschillende expertises binnen de organisatie leidde tot nieuwe inzichten in de mogelijke effecten van het beschouwde scenario en de onderlinge relaties tussen de systemen en de bedrijfsprocessen.

Keuze voor één route
Het gekozen dreigingsscenario bleek nog te breed om in één workshop verder op te pakken. Daarom is in de voorbereiding van de tweede workshop gekozen om één route op te pakken voor verdere kwantificering. Dit maakte een meer afgebakende aanpak mogelijk.

5.1.3 Aandachtspunten voor vervolgactiviteiten

Voorbereiding van de workshops
De voorbereiding van de workshops vergt goede afstemming met de case organisatie. In de voorbereiding van de eerste workshop is meermaals overlegd met de case organisatie. Door de korte doorlooptijd tussen workshop 1 en 2 bleek het niet mogelijk om tussendoor nog een en ander af te stemmen.
Verbeterpunt: In de komende case studies zal nog sterker de nadruk worden gelegd op het vooraf inplannen van een aantal voorbereidende gesprekken, ook in de periode tussen de verschillende workshops.

Kwantificering bleek niet mogelijk door gebrek aan gegevens
In de tweede workshop werd duidelijk dat het voor de deelnemers moeilijk was om de gevraagde kwantitatieve inschattingen te maken. Dit expliciet maken van inschattingen en afwegingen bleek vooral moeilijk door het huidige gebrek aan ervaringscijfers binnen de organisatie. In de nabije toekomst verwacht de organisatie hier meer gegevens beschikbaar te hebben.
Daarnaast werkte de diversiteit van de deelnemers nu mogelijk enigszins belemmerend, terwijl de diversiteit in de eerste workshop juist van sterkte toegevoegde waarde was gebleken. In het bijzonder de abstractere vraagstelling in deze fase bleek niet alle deelnemers te liggen.
Verbeterpunt: In de voorbereiding van de workshop zal worden gezocht naar ondersteunende gegevens, bijvoorbeeld trendgegevens vanuit de overheid of incidentgegevens.

5.2 Feedback vanuit een vitaal bedrijf

Om te toetsen of het model ook voor andere sectoren herkenbaar is en of de werkwijze aanspreekt, is het ontwikkelde model voorgelegd aan een vitaal bedrijf in een andere vitale sector. Dit overleg bracht de volgende punten aan de orde:

Herkenbaarheid basismodel
De hoofdstructuur van het model bleek ook voor de andere sector zeer herkenbaar. De organisatie herkende hierin een *bowtie* structuur die door hen wordt gebruikt. Ook de systematiek van de keuze voor verschillende routes door het model sprak aan (“knikkerbaan”).

Mogelijkheid tot het maken van kwantitatieve inschattingen
De betrokken organisatie gaf aan zelf ook bezig te zijn om zaken meer kwantitatief te maken. Dit bleek ook voor dit bedrijf een uitdaging (er lopen nu langdurige activiteiten in het kader van cyber verzekeringen). Hierbij werd een onderscheid gemaakt tussen verschillende dreigingen. Zo werd aangegeven dat een kwantitatieve inschatting wel mogelijk is voor een deel van de dreigingen (bijv. DDoS). Hiervoor zijn voldoende ervaringscijfers beschikbaar. Voor andere typen dreigingen is dit niet het geval.

Aansprekende elementen uit de methodiek
Van de methodiek sprak vooral het expliciet maken van de inschattingen aan de hand van de modelstructuur aan. Ook de hierbij behorende kanstabellen werden als meerwaarde gezien.

Inschatting van de impact:
De organisatie herkende de indeling van de impactfactoren uit de casus.
De organisatie gaf aan dat het vrij goed lukt om de impact op bedrijfsniveau in te schatten. Er werd aandacht gevraagd voor het inschatten van de maatschappelijke impact (dit valt buiten de directe scope van het bedrijf); Dit aspect werd vooral van belang geacht voor vitale organisaties. Met name op dit aspect werd aanvullende ondersteuning gewenst.

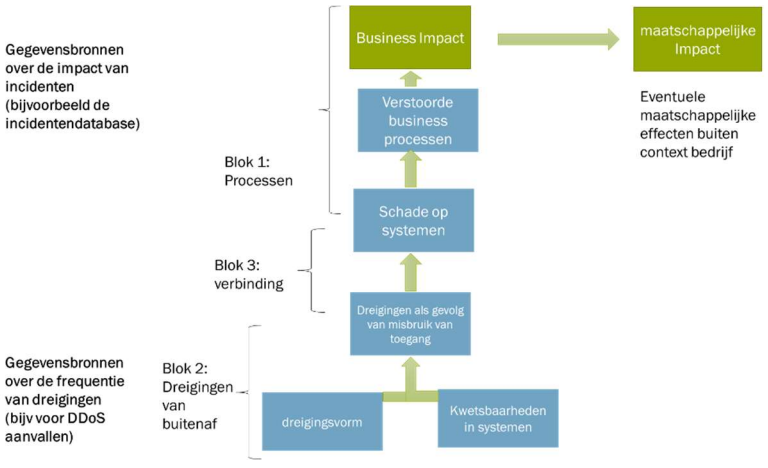
Aandachtspunten voor vervolgactiviteiten
Op basis van hun ervaring met risicomanagement werden de volgende aandachtspunten genoemd:

- Kies een hybride insteek: de organisatie gaf aan dat zij in de praktijk een hybride insteek het meest zinvol achtten; Hierbij kan een deel van de dreigingen ((bijv. DDoS) kwantitatief worden benaderd, en andere typen dreigingen meer kwalitatief.
- Besteed aandacht aan de schaalbaarheid: Wanneer verschillende routen worden behandeld dient te worden gezorgd dat dit overzichtelijk blijft. Een tiental routen werd een nog te behandelen aantal genoemd.

5.3 Voorstel vervolgstappen

In de case studie in 2020 heeft de nadruk gelegen op de opzet van een modelstructuur voor een organisatie. Het basismodel hiervoor bleek relatief snel meer bedrijfsspecifiek te maken. In de uitgevoerde case studie bleken minder mogelijkheden voor het maken van kwantitatieve inschattingen. Dit werd vooral veroorzaakt door een gebrek aan ervaringscijfers en ondersteunende datasets. Als voorstel voor de vervolgwerkzaamheden zal daarom naast het uitvoeren van nieuwe case studies, in eerste instantie aandacht worden besteed aan het verzamelen van mogelijke gegevensbronnen ter ondersteuning van de kwantitatieve inschattingen.

Verzamelen en analyseren gegevensbronnen
Op basis van een literatuuronderzoek in het eerste kwartaal van 2021 zal worden nagegaan welke mogelijkheden er zijn om gebruik te maken van bestaande datasets. Hiervoor zal worden geïnventariseerd welke data beschikbaar is voor de te beschouwen dreiging en of dit organisaties kan ondersteunen bij het maken van meer kwantitatieve inschattingen. In deze fase zal ook een nadere afbakening worden gemaakt over de te beschouwen dreigingen die relevant zijn voor de voorziene case organisaties.
Op basis van de indeling in blokken in het basismodel kunnen verschillende typen gegevens worden benoemd:



Figuur 11 indeling verschillende typen gegevens die zullen worden onderzocht

- *Gegevens over de impact van mogelijke verstoringen (blok 1).*
  Hiervoor kan de indeling van impact vanuit het basismodel als uitgangspunt worden gehanteerd. Mogelijk kan hierbij ook worden gekeken of naast de impact op bedrijfsniveau ook gegevens over de maatschappelijke impact kunnen worden meegenomen, conform de feedback uit paragraaf 5.2;

- *Gegevens over de frequentie van specifieke dreigingen (blok 2):* Hierbij kunnen bijvoorbeeld periodieke rapportages een rol spelen (bijvoorbeeld het CSBN, de ENISA trendtrapportages, of rapportages vanuit commerciële security organisaties).

Uitvoeren case studies
Voorgesteld wordt om in 2021 in twee uit te voeren case studies de nadruk te leggen op de uitwerking van de kanstabellen en om te toetsen in hoeverre reeds voor een andere sector ontwikkelde modellen overdraagbaar zijn naar een andere organisatie. Hiervoor zal worden voortgebouwd op zowel het ontwikkelde basismodel als specifieke modellen binnen de financiële sector.
Op basis van de bevindingen in de case studie wordt voorgesteld dat voor de processtappen voor de case studies de werkwijze wordt gevolgd die in 2020 is toegepast. Hierbij worden de volgende verbeterpunten meegenomen:

- nog sterker de nadruk leggen op het vooraf inplannen van een aantal voorbereidende gesprekken, ook in de periode tussen de verschillende workshops;
- in de voorbereiding aandacht besteden aan de beschikbaarheid van ondersteunende gegevens, niet alleen bij de case organisatie maar ook mogelijke bronnen bij andere organisaties.

6 Literatuur

1. Antoine Bouveret, *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment,* IMF working paper, 2018.
2. Cherdantseva Y., Burnap P., Blyth A. e.a., *A review of cyber security risk assessment methods for SCADA systems*, Computers & Security, Volume 56, February 2016, Pages 1-27
3. CRO Forum, *Concept Paper on a proposed categorisation methodology for cyber risk*, 2016
4. CRO Forum, *Supporting on-going capture and sharing of digital event data*, 2018.
5. ENISA, *Reference Incident Classification Taxonomy Task Force Status and Way Forward*, 2018.
6. ENISA, Overzicht RM methoden: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory
7. Freund J., Jones J., *Measuring and Managing Information Risk: a FAIR approach,* Butterworth-Heinemann, 2014
8. Giannopoulos G., Filippini R. and Schimmer, M., *Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art*, JRC report, 2012. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC70046/lbna25286enn.pdf
9. Hubbard D.W.. Seiersen R., *How to Measure Anything in Cybersecurity Risk*, 2017
10. *ISO, standaarden rond risicomanagement: ISO31000/31010 en ISO27005*
11. *NAVI, Handreiking Risicoanalyse, 10 praktische modellen voor de risicoanalist, 2008.*
12. *NIST, Guide for Conducting Risk Assessments, SP 800-30, 2012.*
13. *Open Group,* FAIR – ISO/IEC 27005 Cookbook*, technical guide, 2010*
14. *Open Group, Risk Analysis (O-RA). 2013*
15. *Waldron K., Resources for Measuring Cybersecurity,* R-street*, 2019.*
16. *Wolthuis R., Philipson e.a.,* Quantifying Cyber security Risks*, 2019*
17. World Economic Forum*, Partnering for Cyber Resilience Towards the Quantification of Cyber Threats, 2015.*

Appendix: samenvatting van de ervaringen in de financiële sector

De gebruikte methode is ontwikkeld binnen het Shared Research Program (SRP) Cybersecurity, een samenwerkingsverband tussen TNO en de volgende Nederlandse financiële instellingen: ABN AMRO, Rabobank, ING, De Volksbank, en Achmea. In de Proof of Concept fase is dan ook nauw samengewerkt. Enkele ervaringen:

- Er is aanzienlijke inspanning vereist om een model voor een dreiging op te stellen. Dit is echter de moeite waard omdat het tot nuttige nieuwe inzichten leidt. Daarnaast is de verwachting dat het model en de kanstabellen over tijd niet snel zullen veranderen, en resultaten daarom voor lange tijd kunnen worden gebruikt.
- De aanbeveling is om iedere specifieke dreiging apart te modelleren. Hierbij kunnen grote delen van andere modellen worden hergebruikt.
- De sector beschikt over historische gegevens; dit vergemakkelijkt het maken van inschattingen.
- Er zijn modellen uitgewerkt voor verschillende typen dreiging, specifiek DDoS, Ransomware en Phishing.
- Het model bleek ook grotendeels zelfstandig door organisaties toe te passen. TNO had hier nog wel enige bemoeienis omdat de methode onderwijl verder werd uitgewerkt.
- Het volledig vullen van het model is ook binnen deze sector een uitdaging. Informatie bevindt zich in verschillende delen van de organisatie of zelfs extern. Ook moet er een vertaalslag worden gemaakt van informatie naar waarschijnlijkheid. Om het proces te vergemakkelijken is er gewerkt aan ondersteunende tooling voor het invullen van grote (conditional) kanstabellen.