Vrijheid blijheid?

De invloed van werkplekinrichting op gevaarinschatting bij de overheid

Wietse de Graaf
wietsedegraaf@mac.com
vrijdag 8 maart 2019
Eerste lezer: Prof. Dr. Albert Meij
Tweede lezer: Dr. Peter Castenmiller

1 Contents

1 Voorwoord

Met het schrijven van deze woorden komt er een einde aan twee jaar studeren, zelfontwikkeling, maar vooral ook plezier maken. Het traineeprogramma is uitdagend en intensief, je leert veel en kunt het meteen in de praktijk brengen. In die twee jaar tijd heb ik op de opdracht in korte tijd veel geleerd en ik heb veel meer mogelijkheden gekregen dan ik van tevoren had kunnen verwachten. Deze woorden betekenen ook dat het scriptietraject er eindelijk op zit. Niet langer constant in je achterhoofd het stemmetje dat je vertelt dat 'je nog iets moet doen'. Voor het eerst in zes jaar ben ik na mijn werk en in de weekenden echt 'vrij'!

Om op je 28e zes jaar te gaan studeren en in de tussentijd te trouwen, een huis te kopen en vader te worden is op voorhand niet aan te raden. Ik zal ook niet ontkennen dat er zeker periodes zijn geweest waarop ik er genoeg van had en op het punt stond er mee te stoppen. Gelukkig is dat het allemaal waard geweest en heb ik na tien jaar studievertraging dan eindelijk mijn papiertje(s!) op zak! Ik begon aan het traineeship omdat ik altijd veel affiniteit heb gehad met computers en techniek, maar ook met beleid, plannen en strategie. Ik heb in het traineeship gevonden waar ik naar op zoek was en heb mezelf goed kunnen ontwikkelen.

Tot slot wil ik nog een aantal mensen bedanken, om te beginnen met mijn jaargenoten. De borrels, de uitjes, de vrijdagen en het hoogtepunt, de reis naar Israël. Zonder jullie was het niet zo leuk geweest en dankzij jullie zijn die momenten die ik eerder noemde ook vaak zo weer overgewaaid. Ik ben ervan overtuigd dat we elkaar blijven zien en nog vaak zullen tegenkomen, ook al slaan we na het traineeship allemaal weer onze vleugels uit. Daarnaast veel dank aan mijn familie en in het bijzonder mijn vrouw Lotte. Ik ben met deadlines in het vooruitzicht niet altijd de meest gezellige of meest aanwezige man in huis geweest en geregeld kwam het huishouden en de zorg voor Olivier op haar schouders neer. Al dat geduld en vertrouwen hebben me goed gedaan en hebben me in staat gesteld dit traject af te ronden. Heel veel dank daarvoor!

Wietse de Graaf

Maart 2019

2 Samenvatting

Informatiebeveiliging is binnen de hedendaagse samenleving van groot belang. Nieuwe technieken maken niet alleen veel meer dan ooit mogelijk op de werkvloer, ze zorgen ook dat bedreigingen van buitenaf groter zijn dan ooit tevoren. Er is dan ook veel aandacht voor zogenaamde awareness-campagnes, om medewerkers – traditioneel de zwakste schakel in elk systeem van beveiliging – scherp te houden en ze alert te maken op bedreigingen op het gebied van IT. Ook wetenschappelijk onderzoek is voornamelijk gericht op het onderzoeken van de relatie tussen die campagnes en het gedrag van medewerkers. Binnen het onderzoek ontbreekt echter twee belangrijke componenten: de werkplekinrichting en het proces van gevaarinschatting bij medewerkers. Het doel van dit onderzoek is dan ook om te onderzoeken wat de relatie is tussen werkplekinrichting als onafhankelijke variabele en gevaarinschatting als afhankelijke variabele. Door middel van een enquête die onder 15 overheidsorganisaties is uitgezet is bij 110 overheidsmedewerkers aan de hand van vier indicatoren uitgevraagd hoe hun werkplekinrichting er uit ziet en aan de hand van 30 vragen hoe zij omgaan met bedreigingen van buitenaf. Voor gevaarinschatting is gebruik gemaakt van het Protection Motivation Theory (Rogers, 1983). Werkplekinrichting is bij gebrek aan bestaande literatuur geoperationaliseerd aan de hand van consultatie van IT-experts. Uit de analyse van de resultaten bleek echter dat er geen relatie is vastgesteld tussen werkplekinrichting en gevaarinschatting. De opzet van het onderzoek kan er mee te maken hebben dat er niet voldoende correlatie is ontdekt. Ten eerste waren er te weinig respondenten en ten tweede is de vragenlijst onvoldoende gevalideerd. Hierdoor is het aantonen van een correlatie onvoldoende mogelijk gebleken. Bovendien kan er een belangrijke rol zijn weggelegd voor organisatiecultuur, een factor die helemaal niet voorkomt in dit onderzoek. Om deze reden is er dan ook uitgebreid aanbeveling gedaan voor vervolgonderzoek.

3 Inleiding

De afgelopen decennia is dankzij de opkomst van nieuwe technologie en kennis de gemiddelde werkplek drastisch veranderd. De opkomst van het internet heeft ervoor gezorgd dat iedereen constant met elkaar in verbinding is. Alle computers binnen een instelling zijn met elkaar verbonden en informatie wordt op hoge snelheid uitgewisseld. Dit zorgt voor een ongekende toename van productiviteit en efficiëntie. Beslissingen kunnen sneller worden genomen en de kennis van een individuele medewerker kan snel worden geborgd en gedeeld met de rest van de organisatie. Het maakt zelfs samenwerking met de andere kant van de wereld mogelijk, als ware het een afdeling op een andere verdieping.

Er kleven echter ook flinke nadelen aan deze toenemende connectiviteit en de daarmee ontstane afhankelijkheid van het internet. Doordat bijna alle werkprocessen zijn afgestemd op het gebruik van internet en digitale hulpmiddelen ontstaat er een groot probleem als die technologie wegvalt. De mens is in veel situaties de kwetsbare schakel. Het is namelijk de medewerker die op de link klikt in een phishing e-mail of het bestand downloadt waar een virus in blijkt te zitten. Onbedoeld kan de medewerker meer schade aanrichten dan een gerichte aanval van hackers. Een bekend voorbeeld hiervan is het recente geval van ransomware: het Wannacry virus. Dit virus is binnengekomen door middel van een phishing e-mail, waarna het virus kwetsbaarheden in oude Windows installaties misbruikte om zich met hoge snelheid te verspreiden over wereldwijde computernetwerken. Door de toenemende connectiviteit was de kwetsbaarheid van een enkele medewerker in dit geval genoeg om een virus wereldwijd te verspreiden.

Naast operationele problemen zijn er financiële gevolgen verbonden aan cybercriminaliteit. De geschatte economische schade van cyber gerelateerde activiteiten bedraagt jaarlijks zo'n 600 miljard dollar (McAfee, 2018). Dat betekent dat ongeveer één procent van het wereldwijd bruto product het risico loopt verloren te gaan door cyberaanvallen en -misdaad. Om te voorkomen dat medewerkers per ongeluk op links klikken of zorgen voor andere kwetsbaarheden zijn veel bedrijven en overheidsinstellingen begonnen met het uitvoeren van zogenaamde awareness-campagnes. De verwachting is dat deze markt tot 2023 zal toenemen tot een kleine 250 miljard dollar (Statista, 2019). Deze campagnes zijn gericht op het informeren en trainen van de medewerker. Ze leren wat de kwetsbaarheden zijn en hoe ze die kunnen herkennen. Het idee erachter is dat de medewerker in het ideale geval niet langer op 'die link' klikt en zich zelfbewust kan handhaven in het digitale domein. Het is echter aangetoond dat dit soort training vaak niet het gewenste effect heeft (Bada, Nurse, & Sasse, 2015). De belangrijkste oorzaak hiervoor is een gebrek aan vaardigheden bij de medewerker. Als de geleerde lessen niet zijn ingebed in bredere contextuele kennis over informatiesystemen, kunnen alleen specifieke kwetsbaarheden worden aangeleerd, maar veranderd er niets aan de instelling van de medewerker (Dolan, Hallsworth, Halpern, King, & Vlaev, 2010). Helaas blijkt dat de gemiddelde werknemer die brede kennis niet heeft. De mens blijft dus de zwakste schakel.

Deze thesis probeert te onderzoeken wat de relatie is tussen werkplekinrichting en de onbewuste houding van medewerkers ten opzichte van IT-bedreigingen (gevaarinschatting). Het onderzoek is op die manier een aanvulling op bestaande kennis over de relatie tussen werkplekbeleid, medewerkers en de ICT-gedrag. Dit zal gebeuren door empirisch te onderzoeken wat de invloed van werkplekinrichting is op de gevaarinschatting van medewerkers. Op basis van de bevindingen uit dit empirisch onderzoek zal bovendien een aanbeveling worden gedaan over de keuzes die er op het gebied van werkplekinrichting kunnen worden gemaakt om medewerkers zo goed mogelijk voor te bereiden op bedreigingen op ICT-gebied.

3.1 Onderzoeksvraag

Medewerkers worden geconfronteerd met verschillende keuzes in werkplekinrichting. Wat echter de invloed van deze keuzes is op het gedrag en het proces van gevaarinschatting van veiligheid van de medewerker is onduidelijk. Het is niet bekend of medewerkers van een strenge omgeving, met weinig opties, extra alert worden of juist erg laks. In een omgeving waar de mens vaak de bepalende factor is, kan dit veel effect hebben op je IT-beveiliging. Er is echter nog geen onderzoek gedaan wat de invloed is van de gekozen werkplekinrichting op het gedrag van de medewerkers.

Dit geeft voor dit onderzoek de volgende hoofdvraag:

- *Hoe is werkplekinrichting van invloed op gevaarinschatting van IT-risico's van medewerkers bij overheidsinstellingen?*

Om tot het antwoord op deze vraag te komen moeten de deelvragen worden beantwoord:

- *Welke relevante verschillen zijn er te herkennen op het gebied van werkplekinrichting?*
- *Hoe schatten medewerkers gevaren rondom IT-risico's in?*
- *Welk verband tussen werkplekinrichting en gevaarinschatting kan worden gevonden aan de hand van de resultaten van de dataverzameling?*

De eerste deelvraag is niet afdoende ondersteund door wetenschappelijke literatuur of theorie. Het antwoord op die vraag zal dan ook middels empirie worden verkregen. In het theoretisch kader zal dit nader worden toegelicht, alsmede de keuzes die vervolgens gemaakt zijn om het begrip werkplekinrichting vorm te geven. De tweede deelvraag is een theoretische deelvraag en zal de gebruikte theorie toelichten. De derde deelvraag zal worden beantwoord door de uit de empirie verkregen resultaten te vergelijken met de uit de theorie verkregen inzichten.

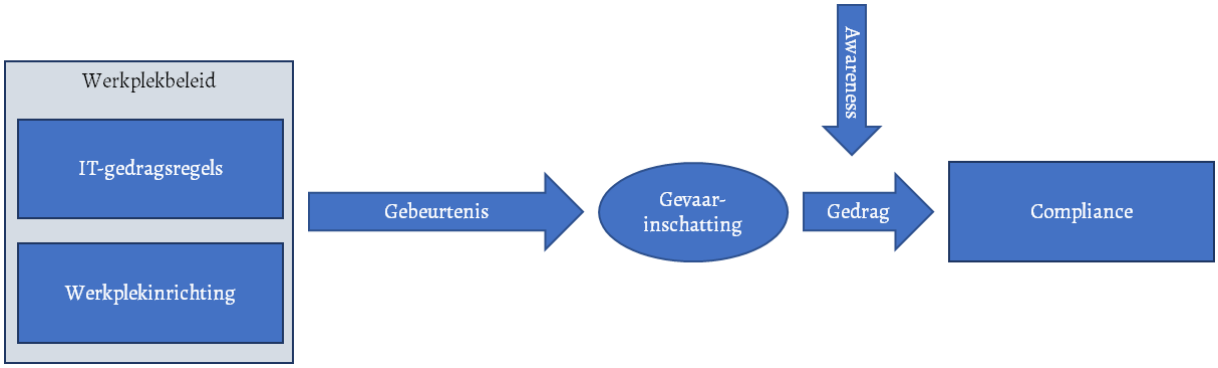
3.2 Maatschappelijke Relevantie

De inleiding gaf al aan dat er veel kwetsbaarheden zitten in de informatievoorziening van bedrijven maar vooral ook van overheden. Veel recente richtlijnen en regels zoals de NORA en de BIR moeten zorgen voor uniformiteit en een baseline van informatiebeveiliging. Tegelijkertijd zien we dat instellingen op het gebied van werkplekinrichting veel keuzes nog zelf kunnen maken. De uitkomst van dat palet aan keuzes heeft invloed op

het gedrag van medewerkers, maar daar is nog geen afdoende onderzoek naar gedaan. De keuzes die instellingen moeten maken zijn dan ook voornamelijk ingegeven door persoonlijke voorkeur van management of IT-afdelingen, of beperkt door contracten met leveranciers (Lourens, 2018). Om een extra dimensie aan die keuze toe te voegen is het van belang in te zien wat de relatie is tussen het gedrag van je medewerkers en de keuzes die je hebt gemaakt op het gebied van werkplekbeleid. Gezien het financiële risico en de enorme bedragen die worden uitgegeven aan awareness- en preventiecampagnes loont het om uit te zoeken wat de invloed is van de meest basale keuzes die er op IT-gebied moeten worden gemaakt.

3.3 Wetenschappelijke Relevantie

Op wetenschappelijk gebied is er veel geschreven over het verband tussen informatiebeleid, compliance en de invloed van awareness campagnes. Standaardwerken zoals die van Bada et al. (2015), Pahnila (2007) en Siponen (2010) bestuderen de invloed van awareness campagnes op de compliance van medewerkers. Als je kijkt naar de gehele keten van werkplekbeleid tot en met compliance van medewerkers, ligt de nadruk sterk op de interventie die door awareness campagnes wordt gedaan (figuur 1). In dit onderzoek wordt echter gekeken naar de factor gevaarinschatting en de invloed die werkplekinrichting daarop heeft. Op die manier vult dit onderzoek bestaande literatuur aan.



Figuur 1: De keten van beleid naar compliance. Onderzoek richt zich voornamelijk op de Awareness campagnes.

3.4 Leeswijzer

In hoofdstuk 4 zal uitgelegd worden welke theorie ten grondslag ligt aan dit onderzoek. Er zal worden stilgestaan bij Protection Motivation Theory en de opbouw van het begrip werkplekinrichting. De eerste theoretische deelvragen zullen aansluitend worden beantwoord. Vooruitlopend op de resultaten eindigt dit hoofdstuk met de hypotheses.

In hoofdstuk 5 komt de methodologie aan bod. Hierbij wordt uitgelegd hoe de empirische dataverzameling plaats heeft gevonden en hoe de respondenten zijn geselecteerd. Een belangrijk onderdeel hiervan is de operationalisatie, waarbij precies wordt uitgelegd hoe de begrippen zijn gemeten en hoe dat tot stand is gekomen.

In hoofdstuk 6 worden de resultaten gepresenteerd. Dit zijn de resultaten van de enquête zoals in hoofdstuk 5 beschreven. Deze resultaten zijn beschrijvend, aangezien de analyse in hoofdstuk 7 zal volgen. Tot slot zal hoofdstuk 6 ook de betrouwbaarheid van de vragenlijst aantonen.

Hoofdstuk 7 gaat over de analyse van de data. Middels een correlatiematrix wordt aangegeven wat de correlaties zijn tussen de variabelen. Tot slot wordt per hypothese aangegeven of deze kan worden aangenomen of verworpen.

In hoofdstuk 8 en 9 worden respectievelijk de discussie en de conclusie geleverd. Hierin wordt gekeken naar andere mogelijke verklaringen van de bevindingen en wordt de hoofdvraag beantwoord. Hierin wordt ook alvast een voorzet gedaan voor vervolgonderzoek, waarbij de lessen die bij dit onderzoek zijn geleerd in de praktijk worden gebracht.

Tot slot zal in de reflectie worden stilgestaan bij het persoonlijke proces van de onderzoeker. Wat is er goed gegaan, maar vooral ook wat er beter had gekund.

4 Theoretisch kader

In het theoretisch kader zal verder worden uitgelegd wat onder de begrippen gevaarinschatting en werkplekinrichting wordt verstaan. Tevens worden de eerste en tweede deelvragen beantwoord. Door middel van inzichten uit de theorie wordt uitgelegd hoe deze begrippen zich verhouden tot elkaar.

4.1 Werkplekinrichting

Elke dag worden medewerkers geconfronteerd met meerdere gevaren en risico's op het gebied van ICT. Deze gevaren variëren van actieve bedreigingen zoals virussen, hacks en phishing aanvallen tot indirecte risico's, zoals datalekken en het verlies van apparatuur. Hoe medewerkers en instellingen moeten omgaan met deze bedreigingen is bij de overheid vastgelegd in de Baseline Informatiebeveiliging Rijksdienst (BIR) 2017. Hierin is afgesproken hoe systemen van de overheid moeten worden ingericht (Rijksoverheid, 2017). Deze afspraken moeten ervoor zorgen dat de uitwisseling van gegevens op het juiste beveiligingsniveau plaats vindt. De BIR is geïmplementeerd op het comply-or-explain principe, wat betekent dat je in principe moet voldoen aan de richtlijn, tenzij je een goede reden hebt om het niet te doen. Om overheidspartijen en partners uit de particuliere sector inzicht te geven in de mate waarin ze compliant zijn aan de BIR is een zogenaamde Fit/Gap analyse beschikbaar gesteld (Ministerie van Algemene Zaken, 2018). Hierin kan op een aantal punten worden nagegaan in hoeverre je compliant bent aan de BIR. Voorbeelden van deze punten zijn: de aanwezigheid van beleidsregels (5.1.1); rollen en verantwoordelijkheden rondom informatiebeveiliging (5.1.2); scheiding van taken (6.1.2) en de aanwezigheid van logbestanden (12.4.1). Rondom werkplekbeveiliging zijn ook voorwaarden gesteld. Deze betreffen grofweg de categorieën Toegangsbeveiliging, Fysieke beveiliging, Beveiliging van bedrijfsvoering en Communicatiebeveiliging. Binnen deze categorieën is uitvoerig beschreven waar de fysieke werkplek van de medewerker bij overheidsinstellingen (of bij samenwerking met de overheid) aan moet voldoen.

Hoewel de BIR uitvoerig is en strikt geformuleerd, gaat het om randvoorwaarden. Zolang je eraan voldoet is het voor overheidsinstellingen vrij in te vullen hoe. De BIR zegt wát, niet het hóe. Een voorbeeld hiervan is de toegang tot de werkplek vanuit huis (telewerken). De BIR zegt hierover :

Het beleid voor mobiele apparatuur behoort in overweging te nemen:

a) registratie van mobiele apparatuur;

b) eisen voor fysieke bescherming;

c) beperking van installeren van software;

d) eisen voor softwareversies voor mobiele apparatuur en voor het toepassen van patches;

e) beperking van verbinding met informatiediensten;

f) toegangsbeveiligingsmaatregelen;

g) cryptografische technieken;

h) bescherming tegen malware;

i) het op afstand onbruikbaar maken, wissen, uitsluiten;

j) back-ups;

k) gebruik van internetdiensten en -apps.

Verder dan dit gaat de BIR niet. Het is aan de instelling zelf om hier invulling aan te geven. Cryptografische technieken kun je aan voldoen door middel van een VPN, een token of een inlogcode. Zo zijn er nog meer voorbeelden van keuzes die gemaakt kunnen worden binnen de richtlijnen van de BIR.

4.1.1 Geselecteerde indicatoren

Voor dit onderzoek is behoefte aan enkele indicatoren voor het meten van werkplekbeleid. Normaliter komen die indicatoren uit de theorie, maar aangezien er geen bestaande theorie te vinden is over de keuzemogelijkheden binnen werkplekinrichting moest dit onderdeel door middel van empirie worden gedestilleerd. De hieronder beschreven indicatoren en het proces heeft dan ook plaatsgevonden binnen het empirisch proces; hier wordt ten behoeve van de operationalisatie vast de beschrijving van dit proces uitgewerkt. Binnen het kader van dit onderzoek wordt gekeken naar werkplekinrichtingen die zichtbaar en merkbaar zijn voor de gebruiker. Het gaat immers om de relatie tussen werkplekinrichting en de gevaarinschatting van medewerkers. Een eerste uitvraag bij een informatiemanager van een Universiteit geeft aan dat er veel zaken geregeld moeten worden die zichtbaar en merkbaar zijn voor medewerkers (Lourens, 2018). Zoals zal blijken uit het onderzoeksontwerp wordt de werkplekinstelling uitgevraagd bij de respondenten middels een enquête. Om die enquête zo toegankelijk mogelijk te houden is er gekozen worden voor een ten eerste beperkte set aan indicatoren, en ten tweede voor een begrijpelijke vraag; de respondent moet immers ongeacht het kennisniveau kunnen aangeven wat hoe per indicator de werkplekinstellingen zijn op zijn werkplek. Met die twee uitgangspunten is contact opgenomen met vier deskundigen op het gebied van werkplekinrichting. Deze vier zijn geselecteerd op basis van de toegankelijkheid en de vereiste expertise. Hen is gevraagd wat de vier belangrijkste en meest in het oog springende indicatoren voor werkplekinstelling zijn. Deze interviews zijn uitgevoerd met:

- André de Ridder, Chief Information Security Officer van het ROC Horizon College
- Frans van Neerbos, Voormalig Hoofd ICT van het ROC van Amsterdam
- Cees Lourens, Informatiemanager Geesteswetenschappen en Concern van de Universiteit van Amsterdam
- Anoniem, Informatieadviseur van het CIO-office van de Gemeente Den Haag

De uitkomsten van de interviews waren eenduidig; alle vier de geïnterviewden kwamen met dezelfde vier indicatoren:

- Keuze in werkplek
- Rechten om software te installeren
- Mogelijkheden tot thuiswerken

- Wachtwoordbeleid

4.1.2 Keuzes binnen de geselecteerde indicatoren

Als gekeken wordt naar Keuze in werkplek zijn de volgende keuzes mogelijk: Een vaste PC, een thin-client, een laptop, Choose Your Own Device (CYOD) en Bring Your Own Device (BYOD). Bij het aanbieden van een vaste PC, een thin-client en een vaste laptop heeft de instelling alle keuzes en vrijheden om functionaliteiten wel of niet aan te bieden. Vaak wordt een dergelijke werkplek ingericht vanuit de gedachte dat onderhoud, veiligheid en gebruikservaring zo standaard mogelijk zullen zijn. Die standaardisering zorgt voor lagere kosten en een makkelijker te beheersen veiligheidsomgeving (Fenwick, 2017). Daar staat echter tegenover dat voor gebruikers de omgeving minder opties biedt. Vaak zal een dergelijke werkplek gepaard gaan met beperkte rechten tot het installeren van eigen software. Voor de gebruiker biedt de werkplek dan dus een uniforme ervaring die door IT makkelijk is te onderhouden, maar die wel minder mogelijkheden kent in het gebruik. De laatste categorie, de CYOD of BYOD, zijn hierin heel erg anders. De BYOD betekent voor de medewerker een grote flexibiliteit, aangezien hij of zij (vaak wel met een paar voorwaarden) de eigen werkplek mag uitzoeken, aanschaffen en onderhouden. IT-afdelingen zullen dan de basisdiensten zoals e-mail en documentmanagementsystemen geschikt maken voor het gebruik op een dergelijke laptop. CYOD is vergelijkbaar, maar hierbij mag de medewerker uit een vooraf opgestelde lijst een laptop selecteren. Dit verschilt van het aanbieden van een standaard laptop doordat hierbij veel meer variatie mogelijk is. De keuze waar de voorselectie op gebaseerd is hangt eerder af van aanbestedingen en leveranciers dan van hardware overwegingen (Ghosh, Gajar, & Rai, 2013). Dit biedt voor de gebruiker veel flexibiliteit en opties, wat ten koste gaat van veiligheid op het gebied van IT (Olalere, Taufik Abdullah, Mahmod, & Abdullah, 2015).

Een keuze die samenhangt met het aanbieden van de verschillende soorten werkplekken is de mogelijkheid voor de medewerker om zelf software te installeren. Soms zal bij het aanbieden van een werkplek uit de eerste categorie (vaste PC, thin-client of standaard laptop) het installeren van software door gebruikers niet mogelijk zijn. Hierdoor is de softwareomgeving veiliger en is de kans op virussen en corrupte software beduidend kleiner (Blythe, Coventry, & Little, 2015). Dit gaat evenwel ten koste van de mogelijkheden van de gebruiker. Bij het gebruik van een werkplek uit de tweede categorie (CYOD en BYOD) is er echter vaak wel onbeperkte ruimte voor de gebruiker om zelf software te installeren. Dit zorgt dan echter wel weer voor een verhoogd risico, aangezien er minder controle bij de IT-afdelingen ligt en meer bij de eindgebruikers – de medewerkers (Morrow, 2012). Verdere mogelijkheden zijn er binnen deze keuze niet: óf je staat het zelf installeren van software toe, óf je schakelt het uit.

Als gekeken wordt naar de mogelijkheden tot thuiswerken zijn er grofweg drie hoofdoplossingen te vinden: het aanbieden van een virtuele desktop, het openstellen van e-mail en agenda en het blokkeren ervan (en thuiswerken dus niet toestaan). Het aanbieden van een virtuele desktop gebeurt vaak door middel van zogenaamde Citrix licenties. Daarmee kan je middels een speciale netwerkverbinding, het Citrix programma

en een token vanaf je privécomputer thuis inloggen op je werkcomputer. Bij deze oplossing zal vrijwel altijd alle functionaliteit beschikbaar zijn die ook op de werkplek zelf aanwezig is. Als thuiswerken wordt aangeboden is dit vaak de manier waarop dat technisch wordt mogelijk gemaakt (Paquette, Jaeger, & Wilson, 2010). Mochten instelling ervoor kiezen om dit niet mogelijk te maken (dit kan bijvoorbeeld zijn omdat thuiswerken niet vaak voorkomt en Citrix licenties erg duur zijn) dan wordt vaak de e-mail middels Outlook online beschikbaar gemaakt. Op die manier kan de gebruiker nog altijd bij zijn of haar e-mail en agenda, maar is vaak te toegang tot documenten niet mogelijk. Dat zorgt ervoor dat er geen externe toegang is tot de data van het bedrijf, wat het risico op datalekken en virussen kleiner maakt. Het beperkt echter wel de gebruiker die niet volwaardig thuis zal kunnen werken aan documenten en bestanden. Aan het andere eind van het spectrum bevindt zich de instelling die thuiswerken niet mogelijk maakt.

Tot slot speelt het wachtwoordbeleid van de instelling een grote rol in de werkplekomgeving. Medewerkers worden in meer of mindere mate periodiek geconfronteerd met een melding dat het wachtwoord over enkele dagen zal verlopen. Hierin kan onderscheid worden gemaakt tussen het wachtwoord voor toegang tot de computer en het wachtwoord dat toegang verleend tot zaken als e-mail en documenten. Bij werkplekken die door de instelling worden verschaft zal het bijna altijd het eerste type betreffen: toegang tot Windows betekent dan bijna altijd toegang tot de systemen die daarop geïnstalleerd zijn. In het geval van BYOD en CYOD zal er een apart wachtwoord zijn voor de computer zelf en voor de systemen die erop staan (Chiasson & Van Oorschot, 2015). Binnen het wachtwoordbeleid worden twee dingen bepaald: het format waar het wachtwoord aan moet voldoen en de frequentie van het vernieuwen van het wachtwoord. Het format van het wachtwoord gaat over de voorwaarden die aan de inhoud van het wachtwoord worden gesteld: denk daarbij aan een minimale lengte, een verplicht leesteken of cijfers en het gebruik van een hoofdletter. De frequentie van het vernieuwen van het wachtwoord stelt de maximale geldigheidsduur van een wachtwoord vast. Als die periode is verstreken, dan moet het wachtwoord worden aangepast, conform het geldende format. Binnen dit onderzoek zal alleen worden gekeken naar de frequentie van wachtwoordupdates. Het format is ook interessant, maar biedt niet genoeg variatie tussen de verschillende werkplekken, aangezien binnen artikel 9.4.3.1 van de BIR een vaste set aan complexiteitseisen worden gesteld (Rijksoverheid, 2017). Verondersteld mag worden dat alle instellingen dan ook hetzelfde format afdwingen in hun wachtwoordbeleid. Waar het de frequentie betreft is in artikel 9.4.3.5 van de BIR vastgesteld dat wachtwoorden een maximale geldigheidsduur hebben van een jaar. Het is echter aan de instelling zelf om hiervan af te wijken naar een hogere frequentie. Hierbij geld dat hoe hoger de frequentie is, hoe vaker de medewerker met dit beleid wordt geconfronteerd. Het is echter wel veiliger, al gebruiken veel medewerkers door deze hoge frequentie een reeks waarbij steeds een leesteken wordt toegevoegd. De toename in veiligheid is daardoor minder groot dan initieel mag worden verwacht (Choong & Theofanos, 2015). Vaak zal worden gekozen voor een frequentie van eens in de 3 maanden tot eens per maand (Alomari & Thorpe, 2019).

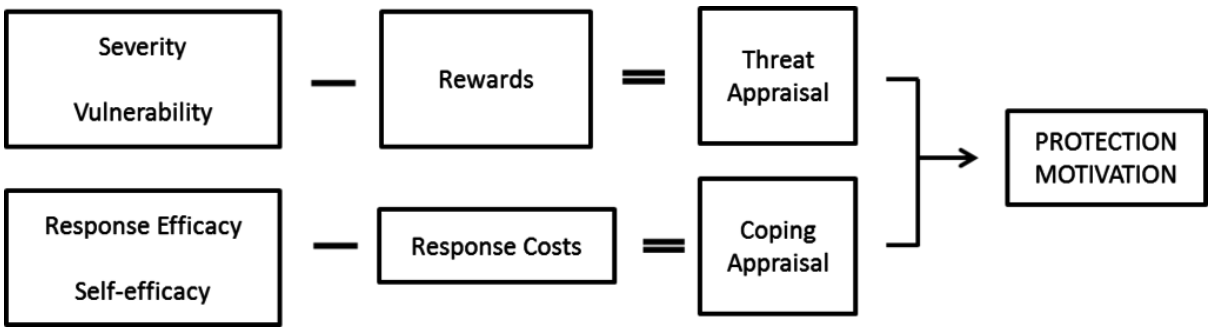
4.2 Gevaarinschatting

ICT-gedrag is een breed begrip met veel elementen. Voor dit onderzoek is gekeken naar het proces van gevaarinschatting. Dit is een deels bewust, deels onbewust proces dat plaats heeft zodra een medewerker zich geconfronteerd ziet met een bedreiging. De uitkomst van dit proces bepaald vervolgens hoe de medewerker handelt bij bedreigingen. In tegenstelling tot het kijken naar compliance zit er in dit onderzoek geen waardeoordeel aan deze uitkomst verbonden. Het gaat enkel en alleen om het proces: worden gevaren herkend, en wat is de afweging die gemaakt wordt. Om inzichtelijk te maken hoe het proces van gevaarinschatting precies werkt zal gebruik worden gemaakt van de theorie van Protection Motivation.

4.2.1 Protection Motivation Theory

Protection Motivation Theory (PMT) is een theorie die is ontstaan en oorspronkelijk is gebruikt binnen de psychologie en criminologie. Zoals gezegd verklaart de theorie hoe mensen omgaan met externe dreigingen. Binnen bestaand onderzoek naar informatiebeveiliging (IB) wordt deze theorie vooral gebruikt om de effectiviteit van awareness campagnes te onderzoeken (Abed & Weistroffer, 2016) & (D'Arcy & Herath, 2011). Het wordt gebruikt om te verklaren hoe mensen komen tot hun reactie op een (vermeende) bedreiging en wat dat betekent voor hun neiging om compliant om te gaan met de gedragsregels binnen een organisatie (Vance, Siponen, & Pahnila, 2012).

De theorie is in 1975 door de psycholoog Rogers geïntroduceerd om beter zicht te krijgen in hoe mensen reageren op een aankomende (mogelijke) bedreiging (Rogers, 1983). Het model is in eerste instantie voornamelijk gebruikt in de gezondheidszorg. De vraag waarom een respondent niet stopt met roken, ondanks de grote risico's dat het met zich mee brengt kan hiermee bijvoorbeeld worden geanalyseerd. De Rewards – de beloning – is te groot. Het voldoen aan de verslavingsprikkels wint het van de risico's die in dat geval niet tastbaar genoeg zijn voor de gemiddelde roker. Pas als het vertrouwen ontstaat dat de persoon zou kunnen stoppen met roken en er bijvoorbeeld een geval van longkanker in de directe sociale omgeving ontstaat zou de analyse de andere kant op kunnen slaan. Bij dit proces wordt dan ook gekeken naar de zes factoren die zoals in figuur 2 te zien is zijn onderverdeeld in twee categorieën. Deze twee categorieën, *Threat Appraisal* en *Coping Appraisal,* bepalen samen hoe iemand omgaat met een bedreiging. *Threat Appraisal* wordt bepaald uit de som van *Severity* en *Vulnerability,* minus de *Rewards*; *Coping Appraisal* ontstaat uit de som van *Response Efficacy* en *Self-Efficacy,* minus de *Response Costs.*



Figuur 2: Protection Motivation Theory (Rogers, 1983)

- *Severity* is onderdeel van *Threat Appraisal* en beschrijft de waargenomen hevigheid van de bedreiging. Het gaat daarbij over de hoogte van de schade die kan ontstaan als gevolg van de bedreiging. In het model is de relatie tot *Threat Appraisal* positief: hoe hoger de *Severity*, hoe hoger de *Threat Appraisal*.
- *Vulnerability* geeft aan hoe kwetsbaar het individu zichzelf inschat en hoe waarschijnlijk de dreiging is. Hoe hoger die kwetsbaarheid is, hoe sterker de *Threat Appraisal* zal zijn.
- *Rewards* beschrijft de voordelen die te behalen zijn (intrinsieke of extrinsieke) om de bedreiging in stand te houden. Als het voordelig is om de bedreiging in stand te houden of als het positieve gevolgen kan hebben zijn de *Rewards* hoger. Een hogere *Reward* heeft een negatieve invloed op *Threat Appraisal* en zal die dus verlagen. In onderzoek wordt *Rewards* vaak weggelaten omdat het lastig is om het onderscheid met *Response Costs* te maken (Norman & Seydel, 2005). Bovendien wordt *Rewards* binnen bestaand onderzoek vaak verkeerd gebruikt; omdat wordt gekeken naar de link tussen gedrag en compliance wordt *Rewards* gekoppeld aan beloningen die worden verkregen door compliant te zijn. Hierdoor gaat het model niet meer op, want Rewards zijn in het PMT-model juist die voordelen die behaald kunnen worden door de bedreiging in stand te houden. Het besparen van tijd is bijvoorbeeld een goede Reward voor het negeren van een bedreiging (Woon, Tan, & Low, 2005). Het is daarom belangrijk hier rekening mee te houden bij het ontwerp van het conceptueel model (Vance, Siponen, & Pahnila, 2012).
- *Response Efficacy* is de inschatting over de effectiviteit van een oplossing. Het vertrouwen in een oplossing is van invloed op de inschatting van de bedreiging. De relatie tussen *Response Efficacy* en *Coping Appraisal* is positief: hoe sterker de *Response Efficacy*, hoe hoger de *Coping Appraisal* (Prentice-Dunn, McMath, & Cramer, 2009)
- *Self Efficacy* beschrijft de mate van vertrouwen waarop het individu zelf een oplossing kan bieden. Volgens onderzoekers heeft dit de sterkste invloed op de uitkomst van de *Protection Motivation* (Floyd, Prentice-Dunn, & Rogers, 2000) & (Bandura, 1977). Hoe hoger het vertrouwen in het eigenhandig afhandelen van een bedreiging, hoe sterker de *Coping Appraisal* zal zijn.
- *Response Cost* gaat over de moeite en inspanning (materieel en immaterieel) die de beoogde reactie kost. Hoe hoger die moeite wordt ingeschat, hoe zwakker de *Coping Appraisal* zal zijn.

Om te illustreren hoe deze factoren in elkaar grijpen kun je kijken naar het ongeoorloofd (tegen de gedragscode in) gebruik van Dropbox. Vaak is Dropbox verboden omdat de servers buiten de EU staan en Dropbox daarom niet hoeft te voldoen aan de scherpere privacyregels. Als we dit gedrag analyseren door middel van het PMT-model, dan zien we het volgende:

1. Severity: Een datalek door gebruik van Dropbox kan, afhankelijk van het materiaal (zeer) ernstig zijn.
2. Vulnerability: De kans is klein, maar niet uit te sluiten. In dit specifieke geval is voor de gebruiker bovendien lastig in te schatten wat de kans precies is.
3. *Rewards*: Het gebruik van Dropbox maakt het makkelijk bestanden uit te wisselen met collega's. Soms maakt beleid het lastig om dit op een andere manier te doen. Door bijvoorbeeld SharePoint-omgevingen die niet toegankelijk zijn voor buitenaf is de Reward voor het gebruik van Dropbox groot.
4. *Response Efficacy*: Het is mogelijk de dreiging af te handelen door simpelweg Dropbox niet te gebruiken.
5. *Self Efficacy*: Individuele medewerkers zijn in theorie in staat om Dropbox af te sluiten, maar als er met een grote groep aan wordt gewerkt is dat minder effectief.
6. *Response Cost*: De kosten van het afhandelen kunnen hoog zijn, dat hangt ervan af in hoeverre Dropbox is ingebed in de werkprocessen. Bovendien moet er vaak een alternatief komen, wat erg kostbaar kan zijn.

In dit geval zou de analyse uitwijzen dat de ingeschatte risico's weliswaar groot zijn, maar dat de kans erop klein is. Daar staat tegenover dat het gebruik van Dropbox toch wel erg makkelijk is en het vaak moeilijk is om het volledig af te schaffen. Het gevolg is dan ook vaak dat applicaties als Dropbox gebruikt worden, ook al is het tegen de gedragscode ICT in. Het model gaat ervan uit dat Severity, Vulnerability, Response Efficacy en Self-Efficacy positieve stimulansen zijn voor het afhandelen van een bedreiging. Rewards en Response Costs zijn negatieve stimulansen. Kortom: Als er voordelen te behalen zijn aan de bedreiging of als de kosten van de respons te hoog worden ingeschat, zal de kans op handelen afnemen, hoe sterk de dreiging ook is.

4.3 Beantwoording deelvragen

De eerste twee deelvragen zijn de theoretische deelvragen en kunnen aan de hand van het theoretisch kader worden beantwoord. De eerste vraag is:

Welke relevante verschillen zijn er te herkennen op het gebied van werkplekinrichting?

De BIR is een belangrijke richtlijn voor informatiebeveiliging bij de overheid en instellingen zijn verplicht zich eraan te houden. Toch is er zoals gezien veel speelruimte waar het de werkplek betreft. Interviews met experts hebben uitgewezen dat er veel verschil is en dat er bovendien veel keuzemogelijkheden zijn bij het inrichten van de werkplek. Als er gekeken wordt naar de relevante verschillen, dan wordt er in het kader van dit onderzoek

gekeken naar de verschillen die voor medewerkers zichtbaar en merkbaar zijn. Het antwoord op het eerste deel van deze vraag is dan ook de opsomming van indicatoren voor werkplekbeleid uit paragraaf 4.1.1:

- Keuze in werkplek
    - Vaste PC
    - Thin Client
    - Vaste laptop
    - CYOD
    - BYOD
- Rechten om software te installeren
    - Wel rechten
    - Geen rechten
- Mogelijkheden tot thuiswerken
    - Middels virtuele desktop inloggen op een volledige werkplek
    - Enkel toegang tot e-mail en agenda
    - Geen mogelijkheid tot thuiswerken
- Wachtwoordbeleid
    - Vrije keuze met een maximum van 1 jaar geldigheid conform de BIR.

Het verschil zit voornamelijk in de keuzevrijheid en flexibiliteit die gebruikers hebben. Op de geselecteerde elementen van werkplekinrichting is namelijk steeds een keuzemogelijkheid waarbij de mate van opties (keuzemogelijkheden) voor de gebruikers varieert. Inhoudelijk zijn voor dit onderzoek de relevante keuzes (en daarmee verschillen) in bovenstaand overzicht opgesomd. Op een hoger abstractieniveau kiest elke organisatie voor een balans tussen controle en flexibiliteit voor de gebruiker. In de praktijk betekent het dat hoe meer flexibiliteit er voor de medewerker is, hoe meer verantwoordelijkheid er ook bij de medewerker ligt. Naar mate er meer controle naar de IT-afdeling verschuift, wordt de flexibiliteit van de werkplek voor de gebruiker echter lager. Het is een afweging, óf meer mogelijkheden voor de gebruiker, óf meer veiligheid voor de instelling.

De tweede deelvraag betrof het inschatten van IT-gerelateerde gevaren en luidde:

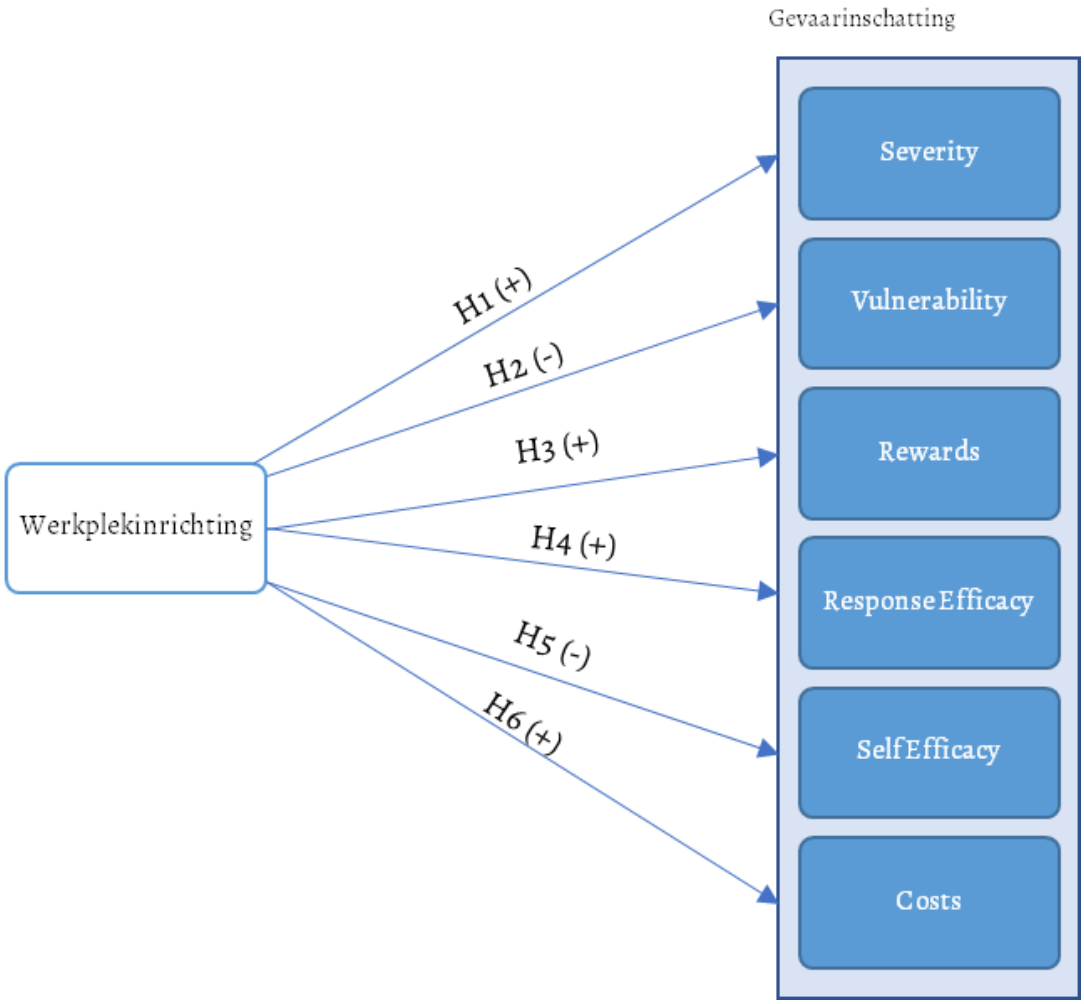
Hoe schatten medewerkers gevaren rondom IT-risico's in?

Om hier antwoord op te geven is gebruik gemaakt van Protection Motivation Theory (PMT). Zoals in paragraaf 4.2 is te lezen bestaat de inschatting van gevaren uit een aantal stappen waarbij de hevigheid, de kwetsbaarheid, het vertrouwen in een oplossing en het zelfvertrouwen ten opzichte van het kunnen geven van een oplossing worden afgewogen. De uitkomst van die optelsom wordt vervolgens verwerkt met de beloning die de instandhouding van de dreiging en de kosten/ moeite van een eventuele oplossing met zich meebrengen. Er heerst een algemene overeenstemming over het feit dat PMT ook geldig is binnen het kader van de

informatiebeveiliging (D'Arcy & Herath, 2011)& (Floyd, Prentice-Dunn, & Rogers, 2000)& (Pahnila, Siponen, & Mahmood, 2007). Vertaald naar de dagelijkse praktijk betekent het dat de houding van de medewerkers tegenover een IT-dreiging ontstaat doordat de medewerker het proces van PMT doorloopt.

4.4 Conceptueel model en hypothesen

De in de theorie opgedane inzichten uit de literatuur rondom PMT zijn weergegeven in onderstaand onderzoeksmodel. Dit model geeft de relatie tussen werkplekinrichting en de gevaarinschatting van de medewerkers weer. Binnen de PMT-theorie zijn de elementen losse entiteiten die onderling afhankelijkheden hebben. Omdat voor dit onderzoek interessant is om te zien of werkplekinrichting invloed heeft op de individuele elementen van PMT, is de theorie in het conceptueel model dan ook uit losse elementen opgebouwd. De zes elementen zullen apart worden uitgevraagd en in de analyse wordt ook per element de deelvraag beantwoord. Om dit mogelijk te maken is gekozen voor het opstellen van zes hypothesen. Daarnaast is het conceptueel model opgesteld om de relatie tussen deze individuele elementen en werkplekinrichting weer te geven.



Figuur 3: Conceptueel model.

4.5 Hypothesen

H1	Een hogere score op werkplekinrichting gaat samen met een hogere score op Severity
H2	Een hogere score op werkplekinrichting gaat samen met een lagere score op Vulnerability
H3	Een hogere score op werkplekinrichting gaat samen met een hogere score op Rewards
H4	Een hogere score op werkplekinrichting gaat samen met een hogere score op Response Efficacy
H5	Een hogere score op werkplekinrichting gaat samen met een lagere score op Self Efficacy
H6	Een hogere score op werkplekinrichting gaat samen met tot een hogere score op Response Costs

Tabel 1: Hypothesen

De opgestelde hypothesen behoeven enige toelichting. Omdat er niet geput kan worden uit onderzoek naar de relatie tussen gevaarinschatting en werkplekinrichting is de relatie op basis van argumentatie ingeschat. Een uitleg over hoe elke hypothese is opgesteld volgt hieronder. De schaal waarop werkplekinrichting is gebaseerd gaat uit van een hoge score indien er een hoge mate van controle is door de IT-afdeling. Dit betekent automatisch een lagere flexibiliteit (=minder opties) voor de gebruiker. Andersom betekent een lage score dat de gebruiker veel mogelijkheden (=flexibiliteit) kent in de omgang met de werkplek, maar dat de IT-afdeling minder controle heeft over het gebruik er van. Later zal dit bij de operationalisatie (5.4.1) verder worden uitgewerkt.

- H1: De confrontatie met een hoog gecontroleerde werkplekinrichting (=hoge score) zal de respondent constant aan veiligheid herinneren. Dit zorgt ervoor dat de ernst van bedreigingen hoger zal worden ingeschat (=hoge score).
- H2: Dezelfde confrontatie met een hoog gecontroleerde werkplekinrichting zal de respondent minder snel kwetsbaar laten voelen. Dit uit zich in een lagere inschatting van kwetsbaarheid (=lagere score)
- H3: Een hoge score op werkplekinrichting betekent een werkplek waar weinig flexibiliteit bestaat. Onveilig gedrag kan worden ingegeven door gemak of het omzeilen van afspraken en beperkingen. Een goed voorbeeld hiervan is het Dropbox voorbeeld uit het theoretisch kader. Daarom is de hypothese dat een hogere score op werkplekinrichting een positief effect heeft op de te behalen rewards.
- H4: Vergelijkbaar met de beredenering achter H2 zal een hogere score op werkplekinrichting een hogere score opleveren op Response Efficacy. Dit komt doordat alle systemen en veiligheidsmaatregelen de respondent vertrouwen geven in het kunnen oplossen van een situatie die uit een bedreiging kan ontstaan.
- H5: In lijn met H4 betekent een hogere score op werkplekinrichting echter ook dat de respondent zelf minder flexibel is in het kunnen bieden van een oplossing (= lagere score op Self Efficacy). Hoe meer de systemen dicht zitten, hoe minder er voor de respondent mogelijk is.

- H6: Tot slot sluit ook H6 aan op H4 en H5. Hoe hoger de score op werkplekinrichting, hoe minder flexibel een systeem is en hoe hoger de inspanningen van de respondent om een oplossing te bieden (= hogere score op Response Costs).

5 Methodologie

5.1 Onderzoeksstrategie

Het onderzoeksontwerp is tot stand gekomen volgens de methodologie van (Verschuren & Doorewaard, 2007). De werkwijze heet de A – door – B-methode, waarbij A de aard van het kennisdoel is en B hoe het kennisdoel wordt bereikt. Bij dit onderzoek is het onderzoeksdoel als volgt:

Het in beeld brengen van de relatie tussen werkplekinrichting en de mate van gevaarinschatting van medewerkers door overheidsinstellingen met verschillende werkplekinrichtingen te vergelijken

---

Impliciet geeft dit al aan hoe het onderzoek er uit gaat zien. Aan de hand van de gekozen theorie zal ik middels enquêtes medewerkers van overheidsinstellingen benaderen en in beeld brengen hoe de werkplek is ingericht. Deze vragen zijn opgesteld naar aanleiding van interviews met experts op het gebied van werkplekbeleid. In het tweede deel van dezelfde enquête ga ik vervolgens de gevaarinschatting van de medewerker meten. Bij het analyseren van de resultaten zal dan aan de hand van de hypothesen worden gekeken naar de relatie tussen werkplekinrichting en gevaarinschatting. Daarbij is werkplekinrichting de onafhankelijke variabele en de gevaarinschatting de afhankelijke variabele. In feite is dit onderzoek een *multiple casestudy* waarbij door gebruik van *mixed methods* getracht is om door een combinatie van onderzoeksmethoden een zo compleet mogelijk beeld te verkrijgen (Bryman & Bell, 2015). De methoden die in dit onderzoek naar voren komen zijn literatuuronderzoek, kwalitatieve dataverzameling en kwantitatieve dataverzameling.

5.2 Selectiestrategie

Voor het verkrijgen van respondenten is in dit onderzoek gebruik gemaakt van *convenience sampling*. De organisaties waar de survey is uitgezet zijn benaderd omdat er warme contacten zijn binnen die organisaties. Contactpersonen hebben persoonlijk en via Social Media de vraag gekregen om de enquête uit te zetten onder 5-10 collega's. Enige voorwaarde was dat de organisatie een (semi-) overheidsinstelling was. Dat heeft geresulteerd in de volgende (semi-) overheidsinstellingen waar de enquête is uitgezet:

- CIBG
- Gemeente Alkmaar
- Gemeente Amsterdam

- GGZ-NHN
- Inspectie SZW
- KNAW
- Ministerie van Buitenlandse Zaken
- Ministerie van OCW
- Openbaar Ministerie
- PBLQ
- ROC Horizon College
- Stadsarchief Amsterdam
- Universiteit van Amsterdam
- UWV Alkmaar
- UWV Amsterdam

5.3 Respondenten

De respondenten zijn verkregen door het doorsturen van de enquête door een contactpersoon. Bij alle organisaties heeft dat geleid tot een situatie waarbij de respondenten onderdeel uitmaakten van een team. Alleen bij de Gemeente Alkmaar en UWV Alkmaar is dit niet het geval geweest. Bij de gemeente Alkmaar is de link naar de enquête op intranet geplaatst en zijn de respondenten dus verspreid over de gehele organisatie. Bij het UWV Alkmaar zijn de respondenten door de contactpersoon uitgekozen op basis van persoonlijk contact. Deze respondenten zijn deels team-gecentreerd, maar ook gevonden op andere plekken binnen de organisatie. Er is specifiek gekozen voor de verspreiding via een contactpersoon vanwege de hogere kans op respondenten. Organisaties zijn geneigd niet te willen meewerken aan onderzoek naar IT-veiligheid omdat dit gevoelige resultaten kan opleveren. Zelfs als organisaties mee willen werken is de kans klein dat je respons krijgt omdat respondenten op dit onderwerp niet snel geneigd zijn mee te willen werken (Kotulic & Clark, 2004).

5.4 Operationalisatie

Nu volgt een beschrijving van hoe de variabelen zijn geoperationaliseerd en bij de respondenten zijn gemeten.

5.4.1 Werkplekinrichting

De uitgevragen elementen van het werkplekbeleid zijn tot stand gekomen door middel van interviews met IT-managers en experts van vijf verschillende overheidsinstellingen. In deze interviews is gevraagd welke 4 keuzes volgens hen de belangrijkste indicatoren zijn van werkplekbeleid. Deze interviews zijn uitgevoerd met:

- Chief Information Security Officer van het ROC Horizon College
- Voormalig Hoofd ICT van het ROC van Amsterdam
- Informatiemanager Geesteswetenschappen en Concern van de Universiteit van Amsterdam
- Informatieadviseur van het CIO-office van de Gemeente Den Haag

De uitkomsten van de interviews waren eenduidig; alle vier de geïnterviewden kwamen met dezelfde vier indicatoren:

- Keuze in werkplek
- Rechten om software te installeren
- Mogelijkheden tot thuiswerken
- Wachtwoordbeleid

Door middel van vier vragen in een enquête is gemeten hoe de werkplekinrichting van de respondent er uit ziet. De antwoorden op deze vragen variëren van veel tot minder flexibiliteit voor de gebruiker. Om een schaal te hebben voor de analyse zijn aan de antwoorden punten toegekend. Hoe meer punten, hoe hoger de mate van controle die door de instelling op het werkplekbeleid wordt uitgeoefend. Op basis van die puntenverdeling wordt er een score toegekend aan het werkplekbeleid van elke organisatie. De antwoordmogelijkheden en de daarbij horende scores zijn te vinden in tabel 2. Hierbij is bij elke antwoordmogelijkheid in samenspraak met de in hoofdstuk 4 genoemde IT-experts bekeken wat elke keuze betekent voor de mate van controle en/ of flexibiliteit voor de gebruiker. Dat heeft geresulteerd in de scores die in tabel 2 zijn genoemd. Om elke categorie even zwaar mee te laten wegen is er steeds 10 punten te behalen voor de oplossing die de meeste controle met zich meebrengt.

Werkplek	Een vaste PC	10
	Een thin-client	10
	Een laptop	7,5
	Choose Your Own Device	5
	Bring Your Own Device	2,5
Wachtwoord	1 keer per maand	10
	1 keer per kwartaal	7.5
	1 keer per half jaar	5
	1 keer per jaar	2.5
	Ik heb nog nooit mijn wachtwoord hoeven veranderen	0
Thuiswerken	Ja, ik heb een laptop van werk en kan gewoon thuis werken	2,5
	Ja, ik kan op mijn privé computer inloggen met een token of inlogcode	5
	Deels, ik kan wel bij mijn e-mail, maar niet bij mijn bestanden	7,5
	Nee	10
Software	Ja, ik heb volledige rechten om alles te installeren	3,3
	Deels, ik kan uit een vooraf opgestelde lijst software laten installeren	6,6
	Nee, ik heb geen rechten om software te installeren	10

Tabel 2: Antwoordmogelijkheden en scoring werkplekinrichting

Bij vragen 1 en 3 zijn meerdere antwoordmogelijkheden mogelijk en wordt het gemiddelde van de gekozen antwoorden gebruikt om tot een score te komen. Achteraf bleek dat vragen 3 en 4 andersom zijn gesteld dan 1 en 2. Dit is in de toekenning van de score verwerkt. Bovendien is bij vraag 1 de zwaarte van de opties 1 en 2 even hoog in geschat; die krijgen beiden 10 punten toegekend. Door de Mean te berekenen van de scores op de onderliggende vragen wordt een nieuwe variabele berekend: het Totaalcijfer voor werkplekinrichting. Later zal worden bekeken of alle variabelen tot dezelfde schaal kunnen worden gerekend.

5.4.2 Gevaarinschatting

Gevaarinschatting is geoperationaliseerd door middel van het eerder besproken conceptueel model dat is gebaseerd op het Protection Motivation Theory model van Rogers (Rogers, 1983). Omdat binnen zowel het oorspronkelijke PMT-model van Rogers als in het conceptueel model het construct gevaarinschatting is opgebouwd uit zes elementen zijn die elementen ook individueel geoperationaliseerd en uitgevraagd middels dezelfde enquête als waarin werkplekinrichting is uitgevraagd. In het kader van vijf scenario's zijn steeds de zes onderdelen van het conceptueel model uitgevraagd. Deze scenario's zijn gebaseerd op realistische IT-dreigingen binnen een kantoor-setting. Per scenario is dan steeds uitgevraagd hoe de respondent met de situatie om zou gaan en ertegenaan kijkt. Dit is gedaan op basis van de zes elementen van PMT, met gebruik van de volgende stellingen:

Severity	Ik vind dit een ernstige situatie (1)
Vulnerability	De kans dat dit gevolgen gaat hebben op mijn organisatie is groot (2)
Rewards	Door deze situatie te negeren bespaar ik mezelf tijd en moeite (3)
Response Efficacy	Dit probleem kan worden opgelost (4)
Self Efficacy	Ik kan dit zelf oplossen (5)
Costs	De oplossing gaat mij tijd en energie kosten (6)

Tabel 3: Operationalisatie gevaarinschatting

Respondenten moesten aangeven in hoeverre ze het eens zijn met bovenstaande stellingen. De antwoorden bestonden uit een 5-keuze likert schaal met de antwoorden: Zeer mee oneens – Mee oneens – Neutraal – Mee eens – Zeer mee eens. In totaal zijn dit zes vragen per scenario, wat met vijf scenario's gelijk staat aan 30 vragen; 5 per element van het conceptueel model. De scenario's zijn opgesteld op basis van ervaring van de onderzoeker en de gesprekken met de IT-experts. Bij het opstellen van de scenario's werd met drie uitgangspunten rekening gehouden:

1. De scenario's moesten herkenbaar zijn voor de respondenten. Omdat er zoveel variatie zit in de werkplekinrichting van de respondenten zou het heel goed mogelijk zijn dat de scenario's niet 100% aan zouden sluiten op de daadwerkelijke werkplek van de respondent. Het moest dus mogelijk zijn voor

de respondenten om zich elk scenario in ieder geval voldoende te kunnen inbeelden om een goed antwoord te kunnen geven.

2. Het moesten IT-bedreigingen zijn die weliswaar een hoge impact zouden kunnen hebben, maar die ook in de dagelijkse praktijk kunnen voorkomen. Idealiter zijn het op het eerste oog onschuldige situaties die toch een grote impact kunnen hebben. Op die manier zouden de scenario's geschikt zijn voor het testen van de gevaarinschatting. De PMT-theorie gaat om het afwegen van baten en lasten. Zodra een scenario te duidelijk extreem gevaarlijk was, gaat de nuance en het proces van die afweging niet op. Daarom zijn de scenario's zo veel mogelijk bedacht met dit in het achterhoofd.
3. De scenario's konden niet over technische bedreigingen gaan. Vragen over firewall instellingen of backdoors zijn voor een groot deel van de respondenten niet herkenbaar en dat zou dus ook niet tot logische resultaten hebben geleid. Daarom zijn de scenario's situaties die je vooral in het gebruik zal tegenkomen. Op die manier sluiten ze ook meer aan op de principes van werkplekinrichting: het gaat over het dagelijkse gebruik en de beperkingen daarvan.

Met deze criteria in het achterhoofd zijn de volgende vijf stellingen bedacht:

1. *U werkt aan een belangrijk document met vertrouwelijke informatie. Dit document wilt u doorsturen aan een collega, maar bij het versturen kiest u per ongeluk het verkeerde e-mailadres en het bestand wordt als attachment naar iemand buiten uw organisatie verstuurd.*
2. *U heeft vlak voor uw vakantie uw Windows-wachtwoord opgeschreven op een post-it. Bij terugkomst van vakantie is uw bureau opgeruimd en de post-it is nergens meer te vinden. U weet niet zeker of de post-it per ongeluk is weggegooid of door iemand is meegenomen.*
3. *U werkt aan een vertrouwelijk document. U moet even naar het toilet of wilt een kop koffie halen. Bij het weglopen vergrendelt u het beeldscherm niet.*
4. *U werkt met uw team samen met een aantal anderen. Dit gebeurt door het gebruik van Dropbox. Vaak is Dropbox verboden omdat de servers buiten de EU staan en Dropbox daarom niet hoeft te voldoen aan de scherpere privacyregels. In het ergste geval heeft Dropbox inzage in uw gegevens of geeft het dat aan externe partijen.*
5. *In de reglementen van uw werkgever staat dat het verboden is om USB-sticks te gebruiken, met daarbij de uitleg dat dit het systeem kwetsbaar maakt voor virussen. Toch moet uw collega vanwege een samenwerkingsverband regelmatig bestanden uitwisselen die te groot zijn om te e-mailen. Deze collega gebruikt als oplossing regelmatig een USB-stick.*

Het idee voor deze manier van enquêteren is ontstaan bij het lezen van het artikel van Vance et al, *Motivating IS Security Compliance,* waarin ze met behulp van Protection Motivation Theory proberen te verklaren waarom medewerkers wel of niet compliant zijn aan veiligheidsregels (Vance, Siponen, & Pahnila, 2012). Om dit te testen gebruiken ze een vragenlijst die is opgebouwd uit 6 hypothetische scenario's. Per scenario stelden ze daarbij vragen over hoe de respondent tegen die situatie aan kijkt en hoe hij daar mee om zou gaan. Ook bij Vance et al

zijn de scenario's opgesteld na consultatie met experts. Dit onderzoek heeft die aanpak een beetje aangepast, omdat het onderzoek van Vance et al gericht was op één organisatie. De vragen en scenario's waren dan ook specifiek opgesteld voor relevantie binnen die organisatie. Hierdoor voldeden de scenario's niet aan criterium 1, en waren ze niet geschikt voor dit onderzoek. Wel is de manier van uitvragen geschikt voor dit soort onderzoeken, omdat het voorleggen van hypothetische scenario's de respondent in staat stelt om sociaal onwenselijke antwoorden te geven; het gaat immers om situaties die niet echt zijn voorgekomen en daarom is de respondent vrijer in het geven van antwoorden (Hovav & D'Arcy, 2012).

5.5 Corresponderende items per hypothese

Hier volgt een overzicht met daarin duidelijk welke items gebruikt zijn om de hypotheses te operationaliseren.

Hypothese	Element	Items uit de vragenlijst
H1	Severity	S1Q1, S2Q1, S3Q1, S4Q1, S5Q1
H2	Vulnerability	S1Q2, S2Q2, S3Q2, S4Q2, S5Q2
H3	Rewards	S1Q3, S2Q3, S3Q3, S4Q3, S5Q3
H4	Response Efficacy	S1Q4, S2Q4, S3Q4, S4Q4, S5Q4
H5	Self Efficacy	S1Q5, S2Q5, S3Q5, S4Q5, S5Q5
H6	Response Costs	S1Q6, S2Q6, S3Q6, S4Q6, S5Q6

Het begrip Werkplekinrichting is geoperationaliseerd aan de hand van de volgende items: Score_Werkplek, Score_Wachtwoord, Score_Thuiswerken en Score_Software. Dit zijn gemiddelde scores van alle respondenten binnen elke organisatie. Deze scores zijn verkregen door de scores zoals in paragraaf 5.4.1 genoemd te middelen tot een organisatiegemiddelde.

5.6 Dataverzameling

Zoals gezien is de data voor dit onderzoek verzameld door middel van kwantitatieve onderzoeksmethoden. Wel is er een kwalitatief aspect aan het onderzoek geweest, doordat de in de empirische fase uit te vragen elementen zijn bepaald door middel van expertgesprekken en literatuurstudie. De input van deze kwalitatieve fase heeft vormgegeven aan de kwantitatieve fase, die middels een online enquête is uitgevoerd. Hiervoor is gebruik gemaakt van Qualtrics, een online enquête-tool. Om de organisaties te kunnen scheiden en de drempel voor de respondent te verlagen is per organisatie een identieke, maar unieke, link naar de enquête verstuurd. Na sluiting van de enquêtes zijn de resultaten samengevoegd met behoud van inzicht in organisatie.

5.7 Risico's voor de kwaliteit van het onderzoek

Bij elk onderzoek bestaan er meerdere risico's die de validiteit van het onderzoek kunnen verminderen (Bryman & Bell, 2015, pp. 49-51). Naast de algemeen geldende eis van repliceerbaarheid kent dit onderzoek enkele specifieke risico's:

- Dataverzameling:
    - Enquêtes hebben inherent risico's voor de validiteit van onderzoek: zo kan de enquête met een bias zijn ontworpen, kunnen de respondenten door middel van een niet representatieve steekproef zijn geselecteerd en een beperkte diepgang kent ten opzichte van andere methoden, zoals het interview (Verschuren & Doorewaard, 2007, p. 168). Door de enquête uit te zetten onder het gehele medewerkersbestand bestaat er geen risico op een verkeerde steekproef.
    - Doordat de data is verzameld bij verschillende instellingen bestaat is het moeilijk om werkplekinrichting als enige onafhankelijke variabele eruit te halen. Organisatiecultuur, type medewerkers, geschiedenis waar het IT-bedreigingen betreft en het soort werk dat er wordt gedaan kunnen allemaal ook van invloed zijn op het IT-gedrag. In de aanbevelingen zal hierop worden teruggekomen in de vorm van een aanbeveling voor vervolgonderzoek en de vorm waarin dat zal moeten gebeuren.
    - De gekozen scenario's zijn theoretisch van aard. Het is onmogelijk om gezien de diversiteit aan overheidsinstellingen scenario's te kiezen die overal toepasbaar zijn. Om dit te ondervangen is elk scenario uitgelegd en is de respondent gevraagd zich in de situatie te verplaatsen. Uit de antwoorden en toelichtingen blijkt dat respondenten hier gehoor aan hebben gegeven.
- Data-analyse
    - Het risico bestaat dat de gekozen codering van werkplekinrichting niet correct is. Hierdoor kan er een vertekend beeld ontstaan. Als bijvoorbeeld het vereisen van een token in de codering van het onderzoek wordt geïnterpreteerd als zijnde een strenge maatregel, terwijl dat door de respondenten van de enquête niet zo wordt gezien, kan de daaruit volgende conclusie incorrect zijn. Tevens bestaat de kans dat de schalen niet lineair zijn.
    - De enquête is door de onderzoeker zelf opgesteld en als zodoende niet verder gevalideerd. Dat brengt kwetsbaarheden met zich mee. Door te kiezen voor een beperkte set aan vragen en categorieën waar die vragen op scoren, blijft het een relatief simpele enquête en is er afdoende ruimte voor analyse op inhoud, in plaats van de statistiek. Tevens is de respondent middels open vragen gevraagd om toelichting, wat verdere diepte geeft aan de analyse.

6 Resultaten

In dit hoofdstuk zullen de resultaten worden gepresenteerd. Eerst wordt er een overzicht gegeven van de statistieken over de respondenten, daarna zal worden onderzocht of de vragen die gevaarinschatting meten die ook daadwerkelijk doen. Daarna wordt de betrouwbaarheid van de vragenlijst onderzocht door per element van PMT de Cronbach's Alpha uit te rekenen. Uiteindelijk wordt de correlatie tussen werkplekinrichting en gevaarinschatting onderzocht door middel van een correlatiematrix en regressieanalyse.

6.1 Betrouwbaarheid vragenlijst

Om de betrouwbaarheid van de vragenlijst te onderzoeken wordt per element de cronbach's alpha uitgerekend. Dit is mogelijk omdat er in geval van een correlatie tussen items minimaal 2 items nodig zijn (McDonald, 1999). In het geval van werkplekinrichting gaat het om vier items, en in het geval van gevaarinschatting gaat het steeds om 5 items per variabele.

6.1.1 Werkplekinrichting

De vier variabelen die samen werkplekinrichting bepalen zijn Score_Werkplek, Score_Wachtwoord, Score_Thuiswerken en Score_Software. Samen bepalen zij Score_Totaalinrichting op basis van de mean van de onderliggende scores. Om te kijken of deze vier variabelen gelijkmatig bijdragen aan de sub schaal Score_Totaalinrichting wordt cronbach's alpha uitgerekend. De uitkomst van deze score moet hoger zijn dan .5, maar is idealiter hoger dan .6 ((McDonald, 1999). In tabel 4 is te zien wat de uitkomst van deze analyse is.

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.360	.484	4

Tabel 4: Cronbach's Alpha voor Werkplekinrichting

Uit de tabel blijkt dat er een te lage α is om de vier variabelen samen te mogen voegen tot een nieuwe sub schaal. Om te zien of dit geldt voor alle vier de variabelen voeren we een totaalanalyse van α uit. De resultaten daarvan staan in tabel 5.

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Score_Werkplek	19.2100	17.307	.494	.531	.022
Score_Wachtwoord	19.4308	21.943	-.076	.024	.640
Score_Thuiswerken	23.0672	21.942	.323	.297	.240
Score_Software	18.8799	13.896	.273	.377	.183

Tabel 5: Totaananalyse Cronbach's Alpha voor Werkplekinrichting

In de tabel is duidelijk te zien wat het effect is als een variabele niet wordt meegerekend. Zichtbaar is dat Score_Wachtwoord geen samenhang heeft met de andere variabelen en dat het weg laten vallen van deze

variabele zelfs zal leiden tot een α van .640, wat wel een betrouwbare schaal oplevert. In het vormen van de nieuwe sub schaal Score_Totaalinrichting zal het wachtwoord dan ook niet meer worden meegenomen. Een mogelijke verklaring is te vinden in het feit dat gebruikers dagelijks, ook in de privésfeer, worden geconfronteerd met wachtwoordbeleid. De standaarddeviatie op wachtwoordbeleid is over alle respondenten gezien 1.2332, wat betekent dat de scores erg dicht bij elkaar zitten. Dat sluit aan bij het in de theorie benoemde feit dat veelal het wachtwoordbeleid hetzelfde zal zijn. Hierdoor is de situatie ontstaan dat wachtwoordbeleid niet meebeweegt met de andere indicatoren van werkplekinrichting. Als de scores op de overige indicatoren toenemen, doet dat weinig met het wachtwoordbeleid, dat vrij constant blijft. Navraag bij een van de experts geeft aan dat dit geen onverwachte uitkomst is; wachtwoordbeleid zal volgens Cees Lourens door de bank genomen overal vergelijkbaar worden ingericht. Het wel of niet hebben van een BYOD heeft geen effect op bijvoorbeeld het wachtwoord voor de informatiesystemen. Er zit dus geen schaal achter en dat blijkt dan ook uit de lage cronbach's alpha.

6.1.2 Gevaarinschatting

Binnen het onderzoek is er steeds sprake van 5 items die dezelfde construct bepalen. Voor de validiteit en de betrouwbaarheid van de vragenlijst is het belangrijk om te weten of er correlatie bestaat tussen de manier waarop elk element steeds is beantwoord. Om dat te bepalen wordt per element cronbach's alpha uitgerekend. Hierbij is aan te geven dat cronbach's alpha een getal vormt tussen de 0 en de 1 en dat hoe hoger dit getal, hoe betrouwbaarder deze schaal gevormd door de geselecteerde items is. Minimaal moet de waarde 0,5 zijn, maar het beste is een score van 0,6 of hoger.

	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
Severity	.589	.592	5
Vulnerability	.731	.731	5
Rewards	.692	.685	5
Response Efficacy	.452	.449	5
Self Efficacy	.391	.384	5
Response Costs	.435	.468	5

Tabel 6: Cronbach's Alpha voor afhankelijke variabelen

Uit tabel 7 blijkt dat de elementen Severity, Vulnerability en Rewards met respectievelijk een α van 0.589; 0.731 en 0.692 tot dezelfde schaal mogen behoren. Datzelfde is niet te zeggen voor de elementen Response Efficacy, Self Efficacy en Response Costs. Om te zien of deze lage scores te verklaren zijn door specifieke variabelen is gekeken of de α hoger is bij het weglaten van de respons op een bepaald scenario. De resultaten van deze analyse zijn te zien in tabel 8.

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Response Efficacy					
S1Q4	14.9048	5.587	.101	.043	.484
S2Q4	14.8476	3.938	.306	.150	.343
S3Q4	14.9048	4.818	.255	.143	.385
S4Q4	14.8095	4.656	.341	.136	.326
S5Q4	14.6667	5.494	.203	.124	.422
Self-Efficacy					
S1Q5	13.5327	7.742	-.001	.125	.479
S2Q5	13.0093	5.575	.357	.175	.197
S3Q5	12.6449	6.684	.200	.139	.338
S4Q5	13.2056	5.580	.383	.164	.179
S5Q5	13.4019	7.129	.082	.091	.428
Response Costs					
S1Q6	11.9346	6.194	.188	.169	.406
S2Q6	12.2336	5.200	.360	.236	.277
S3Q6	13.1495	6.260	.017	.027	.564
S4Q6	12.2897	5.604	.323	.130	.314
S5Q6	12.3364	5.640	.327	.162	.313

Tabel 7: Cronbach's Alpha totale statistiek

Hieruit blijkt dat op Response Efficacy het weglaten van een variabele geen noemenswaardige invloed heeft. Bij Self Efficacy en met name bij Response Costs is dit wel het geval. Het weglaten van item S1Q5 verhoogt de α van .391 naar .479. Nog altijd geen hoge score, maar wel beduidend beter. In verdere analyses wordt S1Q5 dus niet langer meegerekend. Ditzelfde geldt voor S3Q6, want door het weglaten van dat item stijgt de α van .435 naar .564. Daarmee stijgt de α wel tot een acceptabele waarde. Ook S3Q6 wordt dus niet meegenomen in het analyseren van de resultaten. De uiteindelijke betrouwbaarheid van de vragenlijst is dan weer te geven als in tabel 9. Een mogelijke verklaring voor het feit dat S1Q5 niet goed meetelt aan de schaal van Self Efficacy kan gezocht worden in de aard van het scenario dat werd uitgevraagd. Het ging daarbij om een reeds verzonden e-mail met gevoelige informatie. Het is dus een voldongen feit en dat kan betekenen dat respondenten het niet waarschijnlijk achten daar zelf nog iets aan te kunnen doen. De andere scenario's zijn situaties die on-going zijn en derhalve nog wel zijn op te lossen door de respondent. De overige Q5's vormen daarom een hogere α. Een vergelijkbare verklaring kan worden gegeven voor het wegvallen van S3Q6. S3Q6 gaat over response costs; de moeite die het de respondent zou kosten om de gepresenteerde situatie op te lossen. Scenario drie beschrijft slordig gedrag van een individuele medewerker en niet zoals de andere scenario's een gevaarlijke situatie. Hierdoor zal de inschatting van responskosten misschien anders zijn; gedragsverandering is immers anders van aard dan het aanpassen van een werkproces of het oplossen van een probleem.

	Cronbach's Alpha	N of Items
Severity	.589	5
Vulnerability	.731	5
Rewards	.692	5
Response Efficacy	.452	5
Self Efficacy	.479	5
Response Costs	.564	5

Tabel 8: Cronbach's Alpha na verwijderen items

6.2 Beschrijvende statistieken

De eerste statistieken laten zien hoe de respondenten verdeeld zijn binnen de organisaties. Zoals eerdergenoemd zijn er in totaal 15 organisaties benaderd. In totaal zijn er 110 respondenten, wat een gemiddelde van 7,3 respondent per organisatie oplevert. Dit valt precies binnen de doelstelling van tussen de 5 en 10 respondenten. Hier zijn enkele uitschieters, zoals de Gemeente Alkmaar (n=15), PBLQ (n=14), maar ook het Ministerie van Buitenlandse Zaken (n=3).

	Frequentie	Procent
CIBG	8	7.3
Gemeente Alkmaar	15	13.6
Gemeente Amsterdam	4	3.6
GGZ-NHN	6	5.5
Inspectie SZW	5	4.5
KNAW	10	9.1
Ministerie van Buitenlandse Zaken	3	2.7
Ministerie van OCW	6	5.5
Openbaar Ministerie	7	6.4
PBLQ	14	12.7
ROC Horizon College	6	5.5
Stadsarchief Amsterdam	8	7.3
Universiteit van Amsterdam	6	5.5
UWV Alkmaar	7	6.4
UWV Amsterdam	5	4.5
Totaal	110	100.0

Tabel 9: Respondenten per organisatie

Het volgende overzicht is een overzicht van de scores op de vier vragen die tezamen de werkplekinrichting bepalen. Hier valt te verwachten dat medewerkers op de hoogte zijn van het beleid rondom werkplekinrichting en dat er dus een eenduidig antwoord gegeven is op alle categorieën. Om dit te bepalen is naast het gemiddelde ook de standaarddeviatie opgenomen. Deze standaarddeviatie laat zien of de antwoorden inderdaad geclusterd

zijn. Over de gehele linie is te zien dat de standaarddeviaties laag zijn, wat betekent dat de respondenten binnen elke organisatie redelijk uniform de vragen hebben beantwoord. Een grote uitschieter hier is de Gemeente Alkmaar, waar kennelijk onduidelijkheid bestaat over de mogelijkheid tot het installeren van eigen software (S.D.: 3,3). Dit is deels te verklaren door de manier waarop de contactpersoon de enquête heeft verspreid onder de medewerkers van de gemeente. Waar bij de andere enquêtes een contactpersoon enkel teamleden heeft aangeschreven is bij de gemeente Alkmaar de enquête middels intranet verspreid. Het is onbekend wie er allemaal toegang hebben tot intranet, maar het is duidelijk dat de enquête daar team overstijgend is ingevuld. Mogelijk heeft de gemeente Alkmaar een werkplekinrichting die per afdeling of locatie verschillend is. Een vergelijkbaar effect is te veronderstellen voor het UWV Alkmaar, waar de contactpersoon eveneens buiten het team de enquête heeft uitgezet. Dat heeft in dit geval gezorgd voor een S.D. van 2.53 op Software.

Organisatie		Werkplekkeuze (0-10)	Thuiswerken (0-10)	Softwarekeuze (0-10)	Totaal (0-10)
CIBG	Mean	7.6563	3.4375	9.5750	6.8896
	Std. Deviation	.44194	.88388	1.20208	.63208
Gemeente Alkmaar	Mean	5.8000	3.0833	6.2000	5.0278
	Std. Deviation	1.26844	.64550	3.31749	1.36848
Gemeente Amsterdam	Mean	8.1250	4.6875	10.0000	7.6042
	Std. Deviation	2.16506	.62500	.00000	.85898
GGZ-NHN	Mean	10.0000	4.7917	9.4333	8.0750
	Std. Deviation	.00000	.51031	1.38804	.63278
Inspectie SZW	Mean	7.4167	4.5000	10.0000	7.3056
	Std. Deviation	.85391	.68465	.00000	.18634
KNAW	Mean	8.5000	3.6250	8.6400	6.9217
	Std. Deviation	.52705	1.09449	1.75575	.66272
Ministerie van Buitenlandse Za	Mean	8.3333	2.5000	10.0000	6.9444
	Std. Deviation	.72169	.00000	.00000	.24056
Ministerie van OCW	Mean	7.2917	3.1250	10.0000	6.8056
	Std. Deviation	1.22899	.68465	.00000	.56928
Openbaar Ministerie	Mean	8.9881	4.4643	10.0000	7.8175
	Std. Deviation	1.19937	.98349	.00000	.62994
PBLQ	Mean	5.0000	2.5000	3.3000	3.6000
	Std. Deviation	.00000	.00000	.00000	.00000
ROC Horizon College	Mean	9.3750	5.0000	8.3000	7.5583
	Std. Deviation	.68465	.00000	1.86226	.84897
Stadsarchief Amsterdam	Mean	8.7240	4.5313	9.1500	7.4684
	Std. Deviation	1.49585	.93003	1.57389	1.07189
Universiteit van Amsterdam	Mean	8.3333	6.2500	5.5000	6.6944
	Std. Deviation	.64550	1.36931	1.70411	.56230
UWV Alkmaar	Mean	8.5714	3.9286	9.0429	7.1810

	Std. Deviation	.86258	1.82981	2.53236	.60057
UWV Amsterdam	Mean	8.2500	2.7500	10.0000	7.0000
	Std. Deviation	.68465	.55902	.00000	.34861
Total	Mean	7.6527	3.7955	7.9827	6.4769
	Std. Deviation	1.74141	1.28870	2.80821	1.56145

Tabel 10: Scores op Werkplekinrichting

Net als bij werkplekinrichting moet ook op het gebied van de zes elementen uit het PMT-model de standaarddeviatie worden berekend om te zien of er grote uitschieters zijn. Deze scores zijn te zien in tabel 12.

Organisatie		Severity	Vulnerability	Rewards	Response Efficacy	Self Efficacy	Response Costs
CIBG	Mean	3.8750	3.3500	2.4750	3.2750	3.3438	3.6875
	Std. Deviation	.52304	.63019	.43997	.39911	.70632	.37201
Gemeente Alkmaar	Mean	4.0667	3.6667	2.6533	3.5778	3.7000	3.3444
	Std. Deviation	.63095	.56904	.61629	.45175	.86706	.82908
Gemeente Amsterdam	Mean	3.8500	3.3500	2.9000	3.5000	3.3750	3.5000
	Std. Deviation	.86987	.59722	.20000	.52915	.47871	.35355
GGZ-NHN	Mean	3.6667	3.4000	2.8667	3.1333	3.0417	2.9583
	Std. Deviation	.24221	.30984	.56095	.46762	.79713	.84286
Inspectie SZW	Mean	4.0800	3.8800	2.2000	3.6800	4.0500	3.5500
	Std. Deviation	.33466	.54037	.64807	.33466	.37081	.54199
KNAW	Mean	3.2800	2.9400	2.7200	3.4600	3.6000	3.2000
	Std. Deviation	.40222	.59666	.44422	.25033	.35746	.38730
Ministerie van BUA	Mean	3.5333	2.8667	2.3000	3.5167	3.9722	2.6667
	Std. Deviation	.30551	.41633	.43589	.44814	.45896	.38188
Ministerie van OCW	Mean	3.2000	3.2000	2.6000	3.6333	3.7500	3.5833
	Std. Deviation	.25298	.52154	.41952	.23381	.44721	.37639
Openbaar Ministerie	Mean	3.9714	3.7429	2.6857	3.5143	3.6071	3.6071
	Std. Deviation	.46803	.45774	.53984	.27946	.51755	.31810
PBLQ	Mean	3.4714	2.7286	2.9000	3.2000	2.9464	3.0179
	Std. Deviation	.28937	.31968	.44893	.45742	.58160	.50444
Horizon College	Mean	3.9667	2.6000	3.2333	3.1667	2.7500	3.7500
	Std. Deviation	.48028	.25298	.29439	.42740	.59161	.35355
Stadsarchief Amsterdam	Mean	3.8750	3.6750	2.7000	3.5250	3.3750	3.9063
	Std. Deviation	.62278	.78513	.59522	.31960	.75593	.61146
UvA	Mean	3.6000	2.0667	3.1000	3.2667	2.9167	2.5417
	Std. Deviation	.37947	.24221	.50200	.24221	.20412	.53424
UWV Alkmaar	Mean	3.6286	3.3857	2.5357	3.2571	3.0357	2.9643
	Std. Deviation	.58228	.45617	.33506	.22254	.46611	.44320
UWV Amsterdam	Mean	3.7600	3.5200	2.3600	3.8400	3.7500	3.0000
	Std. Deviation	.96333	.64187	.35777	.32863	.75000	.46771

Total	Mean	3.7218	3.2300	2.7059	3.4202	3.3833	3.2992
	Std. Deviation	.55527	.67695	.51899	.40148	.68757	.63166

Tabel 11: Standaarddeviaties op gevaarinschatting

Hier zijn geen opvallende uitschieters te vinden. Gezien de lage hoeveelheid respondenten per organisatie kan de standaarddeviatie wat groot zijn. Dit geldt ook voor de standaarddeviaties bij werkplekinrichting. Maar door de bank genomen zijn er geen uitschieters die binnen de organisatie zelf een hogere standaarddeviatie hebben dan op het totaalniveau.

7 Analyse van de resultaten

In dit hoofdstuk zal per opgestelde hypothese worden gekeken of die aangenomen of verworpen kan worden. Uiteindelijk zorgen deze analyses voor input voor de discussie en de beantwoording van de empirische deelvraag.

7.1 Correlatiematrix

Om direct inzichtelijk te maken wat de correlatie is tussen de variabelen is hier gebruik gemaakt van een correlatiematrix.

			Score_Totaalinrichting	Severity_MEAN	Vulnerability_MEAN	Rewards_MEAN	Response_Eff_MEAN	Self_Eff_MEAN	Response_Costs_MEAN
Spearman's rho	Score_Totaalinrichting	Correlation Coefficient	1.000	.032	.186	.012	.029	.066	.113
		Sig. (2-tailed)	.	.742	.052	.901	.761	.492	.242
	Severity_MEAN	Correlation Coefficient	.032	1.000	.579**	-.266**	-.018	-.025	.147
		Sig. (2-tailed)	.742	.	.000	.005	.852	.793	.126
	Vulnerability_MEAN	Correlation Coefficient	.186	.579**	1.000	-.361**	.091	.179	.220*
		Sig. (2-tailed)	.052	.000	.	.000	.347	.061	.021
	Rewards_MEAN	Correlation Coefficient	.012	-.266**	-.361**	1.000	-.368**	-.239*	-.010
		Sig. (2-tailed)	.901	.005	.000	.	.000	.012	.919
	Response_Eff_MEAN	Correlation Coefficient	.029	-.018	.091	-.368**	1.000	.297**	.132
		Sig. (2-tailed)	.761	.852	.347	.000	.	.002	.168
	Self_Eff_MEAN	Correlation Coefficient	.066	-.025	.179	-.239*	.297**	1.000	-.058
		Sig. (2-tailed)	.492	.793	.061	.012	.002	.	.549
	Response_Costs_MEAN	Correlation Coefficient	.113	.147	.220*	-.010	.132	-.058	1.000
		Sig. (2-tailed)	.242	.126	.021	.919	.168	.549	.

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Tabel 12: Correlatiematrix

7.2 Hypotheses

7.3 Hypothese 1: Severity

H1	Een hogere score op werkplekinrichting gaat samen met een hogere score op Severity

Om H1 te kunnen aannemen moet er een significante correlatie zijn tussen variabelen Score_Totaalinrichting (onafhankelijk) en Severity_MEAN (afhankelijk). Zoals in de correlatiematrix is te zien is er een correlatiecoëfficiënt van 0.032, wat betekent dat er geen significante correlatie is. Daarnaast laat de T-waarde van .742 zien dat er een 75% kans is dat er geen relatie is tussen de twee variabelen. Hiernaar kijkende kan worden geconcludeerd dat er geen verband is tussen de score op werkplekbeleid en de variabele severity van gevaarinschatting.

7.4 Hypothese 2: Vulnerability

H2	Een hogere score op werkplekinrichting gaat samen met een lagere score op Vulnerability

Om H2 te kunnen aannemen moet er een significante correlatie zijn tussen variabelen Score_Totaalinrichting (onafhankelijk) en Vulnerability_MEAN (afhankelijk). Zoals in de correlatiematrix is te zien is er een correlatiecoëfficiënt van 0.186, wat betekent dat er geen significante correlatie is. De T-waarde van 0.05 betekent dat er 5% kans is dat de verschillen op toeval berusten. Hiernaar kijkende kan worden geconcludeerd dat er weliswaar geen significante correlatie bestaat tussen de twee variabelen, maar dat er wel degelijk correlatie is. Het feit dat de correlatie niet significant is komt doordat er niet voldoende *power* is behaald. De n= van de enquête was simpelweg te klein om representatief te zijn. Ondanks dit zal de hypothese worden verworpen omdat er geen significante correlatie is gevonden.

7.5 Hypothese 3: Rewards

H3	Een hogere score op werkplekinrichting gaat samen met een hogere score op Rewards

Om H3 te kunnen aannemen moet er een significante correlatie zijn tussen variabelen Score_Totaalinrichting (onafhankelijk) en Rewards_MEAN (afhankelijk). Zoals in de correlatiematrix is te zien is er een correlatiecoëfficiënt van 0.012, wat betekent dat er dat er geen significante correlatie is. Daarnaast laat de T-waarde van 0,901 zien dat 90% zeker is dat er geen relatie is tussen de variabelen. Hiermee kan onomstotelijk worden gezegd dat de hypothese is verworpen. Er is geen correlatie.

7.6 Hypothese 4: Response Efficacy

H4	Een hogere score op werkplekinrichting gaat samen met een hogere score op Response Efficacy

Om H4 te kunnen aannemen moet er een significante correlatie zijn tussen variabelen Score_Totaalinrichting (onafhankelijk) en Response_Eff_MEAN (afhankelijk). Zoals in de correlatiematrix is te zien is er een correlatiecoëfficiënt van 0.029, wat betekent dat er dat er geen significante correlatie is. Daarnaast laat de T-waarde van 0,761 zien dat 76% zeker is dat er geen relatie is tussen de variabelen. Hiermee kan onomstotelijk worden gezegd dat de hypothese is verworpen. Er is geen correlatie.

7.7 Hypothese 5: Self Efficacy

H5	Een hogere score op werkplekinrichting gaat samen met een lagere score op Self Efficacy

Om H5 te kunnen aannemen moet er een significante correlatie zijn tussen variabelen Score_Totaalinrichting (onafhankelijk) en Self_Eff_MEAN (afhankelijk). Zoals in de correlatiematrix is te zien is er een correlatiecoëfficiënt van 0.066, wat betekent dat er dat er geen significante correlatie is. Daarnaast laat de T-waarde van 0,492 zien dat 49% zeker is dat er geen relatie is tussen de variabelen. Hiermee kan onomstotelijk worden gezegd dat de hypothese is verworpen. Er is geen correlatie gevonden.

7.8 Hypothese 6: Response Costs

H6	Een hogere score op werkplekinrichting gaat samen met tot een hogere score op Response Costs

Om H5 te kunnen aannemen moet er een significante correlatie zijn tussen variabelen Score_Totaalinrichting (onafhankelijk) en Response_Costs_MEAN (afhankelijk). Zoals in de correlatiematrix is te zien is er een correlatiecoëfficiënt van 0.113, wat betekent dat er dat er geen significante correlatie is. Daarnaast laat de T-waarde van 0,242 zien dat 24% zeker is dat er geen relatie is tussen de variabelen. Er is dus wel sprake van een correlatie, maar deze is niet significant. Met een grotere steekproef kan er wellicht een ander oordeel worden geveld.

7.9 Beantwoording deelvraag

De empirische deelvraag van dit onderzoek kan aan de hand van de literatuur en de empirische resultaten worden beantwoord. De vraag is als volgt:

Welk verband tussen werkplekinrichting en gevaarinschatting kan worden gevonden aan de hand van de resultaten van de dataverzameling?

Door de hypothesen aan te nemen of te verwerpen kan een duidelijk beeld worden gegeven of er een verband te vinden is. Uit paragraaf 8.2 is te herleiden dat er aan de hand van dit onderzoek geen relatie is te ontdekken tussen werkplekinrichting en gevaarinschatting van medewerkers. Er zijn geen significante correlaties te vinden. Kort gezegd is het antwoord op basis van deze resultaten als volgt: Er is geen verband tussen werkplekinrichting en gevaarinschatting. Om dit nog op te sommen volgt een overzicht van de hypothesen en de aanname of verwerping daarvan:

H1	VERWORPEN
H2	VERWORPEN
H3	VERWORPEN
H4	VERWORPEN
H5	VERWORPEN
H6	VERWORPEN

Tabel 13: Conclusie Hypotheses

8 Discussie

In de discussie zal verder worden gekeken naar verklaringen voor de gevonden resultaten. Hierbij wordt ook gekeken naar verbeteringen in methodologie en onderzoeksontwerp.

8.1 Werkplekinrichting

Uit de betrouwbaarheidsanalyse is gebleken dat de gekozen variabelen (behalve het weggelaten wachtwoordbeleid) samen een nieuwe sub schaal kunnen vormen om zo een totaalbeeld voor werkplekinrichting. Er bleek binnen de diverse organisaties voldoende eenduidigheid te zijn, met een paar uitschieters. De verklaring voor die afwijkende resultaten zijn al gegeven, maar de oorzaak ervan was te vinden in de verspreiding van de enquête. Het blijkt echter dat er geen relatie bestaat tussen werkplekinrichting en gevaarinschatting van medewerkers. Dit kan deels worden verklaard doordat er tussen de organisaties simpelweg niet genoeg variatie mogelijk was op het gebied van werkplekinrichting. Door de variabelen middels een enquête uit te vragen zijn de resulterende waarden veelal gecentreerd in het midden. Het gebrek aan variatie, gekoppeld aan een te lage hoeveelheid respondenten hebben niet genoeg variantie opgeleverd om de correlatie (als die er al was) aan te tonen. Het wegvallen van wachtwoordbeleid is daarbij ook een tegenvaller; hierdoor is de schaal nog kleiner geworden

Vervolgonderzoek moet dan ook kritisch kijken naar de manier waarop werkplekinrichting moet worden uitgevraagd. De gesprekken met experts bleken eenduidig en waren als zodanig een goede input voor de te kiezen variabelen. Een alternatief voor de enquête kan, samen met een hoger aantal respondenten binnen de organisaties voor een duidelijker beeld zorgen. Er zijn namelijk wel degelijk correlaties te vinden, maar die zijn niet significant genoeg omdat er onvoldoende respondenten waren. Daarnaast is het de vraag of de gekozen indicatoren voor werkplekinrichting wel representatief genoeg waren voor een nieuwe schaal om werkplekinrichting mee te meten. Hier had betere validatie en het vooraf testen van de vragenlijst antwoord op kunnen geven. Wel kan gezegd worden dat de antwoorden binnen elke organisatie eenduidig waren en dus niet random waren ingevoerd. Ze zeggen dus wel degelijk wat over de individuele variabelen voor werkplekinrichting, maar het is de vraag of ze gecombineerd kunnen worden. De cronbach's alpha was laag, maar dat kan te verklaren zijn door het lage aantal respondenten.

8.2 Gevaarinschatting

Zoals uit paragraaf 8.2 en 8.3 is gebleken lijkt er op basis van de uit de empirie verkregen gegevens geen relatie te zijn tussen werkplekinrichting en gevaarinschatting. Evenals bij werkplekinrichting lijkt op het eerste oog de betrouwbaarheid van de data voldoende te zijn. Het lijkt erop dat de vragen die per scenario over elk van de variabelen gesteld werden konden worden samengevoegd tot een nieuwe schaal per element van PMT (na het verwijderen van twee vragen). De scores op cronbach's alpha waren echter niet hoog genoeg om dit definitief vast te kunnen stellen. Ook hier is dat omdat er niet genoeg respondenten waren om goed gebruik van

cronbach's alpha te kunnen maken. Ondanks dat er geen relatie is aangetoond tussen werkplekinrichting en gevaarinschatting is het wel interessant om te zien dat er binnen gevaarinschatting wel degelijk significante correlaties bestaan. Zo is er een significante correlatie (.579) tussen Severity en Vulnerability. Hoe hoger de Severity van een bedreiging, hoe hoger Vulnerability scoort. Dit is ook te verwachten uit de theorie en het conceptueel model. Daaruit kan je ook verwachten dat Rewards dan negatief correleert met Severity en dat blijkt ook zo te zijn: -.266 ten opzichte van Severity en -.361 ten opzichte van Vulnerability. Aan de kant van de *coping appraisal* is een positieve correlatie te verwachten tussen Response Efficacy en Self Efficacy. De gegevens wijzen dit ook uit: .297. Er lijkt op basis van deze gegevens echter geen correlatie te zijn tussen de variabelen van Efficacy en Response Costs. Op zich is dit niet raar, want het vertrouwen in het kunnen bieden van een oplossing hoeft geen invloed te hebben op de tijd en moeite die die oplossing zou kosten. Dat daar dus ook geen correlatie tussen bestaat is niet opvallend. Alle correlaties die hierboven worden genoemd zijn significant op het 0.01 niveau.

Het feit dat deze correlaties bestaan, significant zijn en bovendien overeenkomen met het conceptueel model en de theorie geeft aan dat PMT zoals verwacht ook goed toepasbaar is op het veld van informatiebeveiliging. In verder onderzoek kan het echter wel helpen om middels meer vragen de variabelen uit te vragen. Binnen dit onderzoek is steeds 1 vraag per variabele per scenario gesteld, maar dit geeft meer waarde als dat aantal wordt uitgebreid. Vance et al hebben dit ook gedaan: zij stelden drie vragen per variabele per scenario. Zij hadden 6 scenario's en dit resulteert dan in 18 vragen over elk element van PMT, tegenover 5 in dit onderzoek.

9 Conclusie

In dit hoofdstuk wordt een antwoord gegeven op de hoofdvraag en de deelvragen. Daarnaast wordt er gekeken naar aanbevelingen op het gebied van vervolgonderzoek.

9.1 Beantwoording hoofdvraag

De hoofdvraag van het onderzoek was als volgt:

Hoe is werkplekinrichting van invloed op gevaarinschatting van IT-risico's van medewerkers bij overheidsinstellingen?

Deze vraag is beantwoord middels de volgende deelvragen:

Welke relevante verschillen zijn er te herkennen op het gebied van werkplekinrichting?

Hoe schatten medewerkers gevaren rondom IT-risico's in?

Welk verband tussen werkplekinrichting en gevaarinschatting kan worden gevonden aan de hand van de resultaten van de dataverzameling?

9.1.1 Deelvraag 1

Het bleek dat er zeer veel verschillen te herkennen zijn op het gebied van werkplekinrichting. De richtlijn waar overheidsorganisaties zich aan moeten houden (de BIR) is weliswaar erg gedetailleerd en rechtlijnig in *wat* de overheidsinstellingen moeten doen om compliant te zijn, maar niet *hoe* ze dat moeten doen. Er is gebleken dat er dan ook enorm veel keuzes zijn voor IT-managers bij het inrichten van de werkplek. De verschillen tussen organisaties zijn in potentie dan ook heel erg groot. Het gekozen detailniveau van de vergelijking is daarvoor echter wel bepalend, want als er gevraagd wordt naar de vier belangrijkste keuzes (die bovendien zichtbaar zijn voor de gebruiker), komen alle geïnterviewde IT-experts met dezelfde vier keuzes waar verschillend op besloten kan worden. Het antwoord van de vraag welke *relevante* categorieën er zijn te herkennen is voor dit onderzoek dan ook:

- Keuze in werkplek
- Rechten om software te installeren
- Mogelijkheden tot thuiswerken
- Wachtwoordbeleid

De nadruk ligt hier echter wel op het feit dat dit de verschillen zijn die *voor dit onderzoek* relevant zijn. Het bredere antwoord op de vraag is dat er zeer veel verschillende mogelijkheden zijn om de werkplek in te richten, met name als het detailniveau groter wordt.

9.1.2 Deelvraag 2

Voor dit onderzoek is gekozen om de term gevaarinschatting te operationaliseren middels het PMT-model. Dit model, oorspronkelijk ontwikkeld voor de medische wereld, laat zien hoe de afweging van respondenten verloopt. Het model bestaat uit zes elementen: Severity, Vulnerability, Rewards, Response Efficacy, Self Efficacy, Response Costs. De inschatting van gevaren bestaat uit een aantal stappen waarbij de hevigheid, de kwetsbaarheid, het vertrouwen in een oplossing en het zelfvertrouwen ten opzichte van het kunnen geven van een oplossing worden afgewogen. De uitkomst van die optelsom wordt vervolgens verwerkt met de beloning die de instandhouding van de dreiging en de kosten/ moeite van een eventuele oplossing met zich meebrengen. Uit de empirie is gebleken dat dit model geldig is in het kader van de voorgelegde scenario's. Het proces werkt inderdaad zoals beschreven in de theorie.

9.1.3 Deelvraag 3

Uit de empirie is gebleken dat er geen relatie lijkt te bestaan tussen werkplekinrichting en gevaarinschatting. Geen van de elementen van gevaarinschatting (de elementen uit het PMT-model) correleert met werkplekinrichting.

9.1.4 Hoofdvraag

Om aan de richtlijnen van de BIR te voldoen moeten er een aantal zaken geregeld zijn waar het de werkplekinrichting betreft. Dat neemt niet weg dat er heel veel opties zijn om daarvoor te zorgen. De grote hoeveelheid aan variatie binnen de mogelijke werkplekinrichting bij overheidsinstellingen zorgt ervoor dat het merendeel van die afwegingen niet eens opvalt voor de gebruikers. De elementen die wel opvallen – de uitkomst van deelvraag 1 – zorgen er gezien de resultaten van deelvraag 3 niet voor dat het proces van gevaarinschatting anders verloopt bij verschillende vormen van werkplekinrichting. Uit de data die in dit onderzoek is verzameld is niet aan te tonen dat er een relatie bestaat.

9.2 Aanbevelingen voor verder onderzoek

Hoewel binnen dit onderzoek er niet in is geslaagd een relatie aan te tonen tussen werkplekinrichting en gevaarinschatting betekent dat niet dat de relatie er niet is. Vervolgonderzoek zou de lessen uit dit onderzoek moeten meenemen om tot een beter proces en methode te komen. Het belangrijkste waar de aandacht op gevestigd moet worden is een ander onderzoeksontwerp. De gekozen methode waarbij onder zo veel mogelijk willekeurige organisaties tussen de 5 en 10 respondenten werden bevraagd heeft ervoor gezorgd dat met name de onafhankelijke variabele (werkplekinrichting) onvoldoende variatie kent. Door de willekeur van het selectieproces, zowel bij het selecteren van de organisaties als het binnen die organisaties selecteren van respondenten, is de representativiteit niet gewaarborgd. Het zou kunnen dat de gekozen manier van verspreiden ervoor heeft gezorgd dat de organisaties een relatief vergelijkbare werkplekinrichting kennen en dat de respondenten van zeer verschillende teams zijn. Zo is bijvoorbeeld bekend dat bij één van de organisaties

het ging om leden van het team voor cybersecurity, terwijl het bij een andere organisatie ging om een team van beleidsmedewerkers die niet gewend zijn om met dit soort scenario's om te gaan. Daarnaast wordt er niet afdoende gekeken naar de verschillen in organisatiecultuur. De invloed hiervan is geen onderdeel van het onderzoek en daardoor is het onduidelijk of de antwoorden op werkplekinrichting én gevaarinschatting niet door andere factoren wordt bepaald. Medewerkers van ministeries kunnen immers anders omgaan met IT dan medewerkers van een mbo-school.

Naast het selecteren van de respondenten en de meegenomen factoren van invloed is er ook verbetering mogelijk op het gebied van de operationalisatie. Het vrijelijk aanpassen van het operationalisatie-model van Vance et al (zie de operationalisatie) is niet zonder risico's. Het model dat zij gebruikten is gevalideerd en getest onder een grote groep expertgebruikers. Doordat er verschil zat in het onderzoeksontwerp kon die vragenlijst niet letterlijk worden overgenomen en is de vragenlijst aangepast om zo meer algemeen toepasbaar te zijn. Dat heeft er echter voor gezorgd dat de vragenlijst niet langer gevalideerd is. Daardoor is het mogelijk dat de uitgevraagde constructen niet daadwerkelijk representatief waren voor werkplekinrichting of gevaarinschatting.

Om deze kwetsbaarheden te verwerken kan er beter worden gekozen voor een multiple case study. Daarbij is het belangrijk om twee vergelijkbare organisaties te selecteren die gekozen hebben voor een verschillende inrichting van de werkplek. Dit *most similar* ontwerp moet ervoor zorgen twee cases te vinden die zoveel mogelijk hetzelfde zijn, maar die verschillen in de onafhankelijke variabele. Met andere woorden: er moeten twee instellingen gevonden worden die qua cultuur en soort werk zoveel mogelijk hetzelfde zijn, maar die een zo verschillend mogelijke werkplekinrichting hebben. Een goed voorbeeld daarvan zou het bekijken van twee mbo-instellingen zijn. Waar het werk betreft doen de medewerkers daar veelal hetzelfde en zijn het zo veel mogelijk hetzelfde type medewerkers. Toch bestaat daar veel variatie in hoe de werkplek is ingericht. Als dat wordt gecombineerd met een veel grotere steekproef, dan zijn de resultaten waarschijnlijk meer representatief en kan er een betere conclusie getrokken worden. Belangrijk daarbij is dat er ook mee wordt genomen welke afdeling de respondenten werken, zodat ook dat als factor kan worden geanalyseerd.

Waar het de operationalisatie van de vragenlijst betreft, moet de vragenlijst beter worden gevalideerd. De keuze om de scenario's zo algemeen mogelijk te operationaliseren heeft er wellicht voor gezorgd dat de scenario's niet langer aansloten bij de beleving van de respondenten. Om dat te voorkomen (en dat kan makkelijker bij het voorgestelde ontwerp) kan er worden gekozen voor specifieke scenario's die met de IT-verantwoordelijken van de cases worden vastgesteld. Deze scenario's zouden meer moeten aansluiten op hun dagelijkse werk en zo meer representatieve antwoorden geven. Bovendien kan de operationalisatie van werkplekinrichting bij een casestudy door middel van interviews worden gedaan, om op die manier zo veel mogelijk variatie weg te nemen. Deze aanbevelingen zorgen voor een hogere validiteit en daarmee meer krachtige uitspraken over de relatie tussen werkplekinrichting en gevaarinschatting. Dit onderzoek heeft geen

krachtige uitspraken kunnen doen over die relatie, en dat betekent dat vervolgonderzoek nodig is. De maatschappelijke relevantie is daarbij misschien nog belangrijker dan de wetenschappelijke relevantie, aangezien de impact van IT-bedreigingen groot kan zijn en alles wat die bedreigingen kan verminderen moet worden aangegrepen om systemen veilig te houden.

10 Reflectie

Gedurende het gehele scriptietraject is de opzet van dit onderzoek meermaals veranderd. Het uiteindelijke product is dan ook een compromis tussen de initiële bedoeling en de uiteindelijke mogelijkheden en beperkingen. In principe zou het onderzoek een casestudy zijn, vergelijkbaar met de voorgestelde opzet uit de aanbevelingen voor vervolgonderzoek. De beperkingen bestonden uit drie categorieën: toegang tot respondenten, beperkte kennis van sociaalwetenschappelijk onderzoek en verkeerde planning. Om te beginnen met de eerste categorie: de eerste aanname was dat er gemakkelijk toegang zou zijn tot zowel respondenten als IT-experts bij twee mbo-instellingen: het Horizon College en het NOVA College. Naarmate de tijd vorderde bleek echter dat er wel toegang was tot de IT-experts (hun expertise is ook gebruikt bij de operationalisatie van werkplekinrichting), maar dat er geen bereidheid was om de enquêtes onder hun medewerkers te verspreiden. Dit had te maken met een timing, er was namelijk net een groot IT-awareness traject begonnen en het 'geduld' van de medewerkers waar het IT en voorlichting betrof begon op te raken. Hierdoor is besloten geen medewerking te verlenen aan het onderzoek. Dit gaf een probleem, want hoe kom je anders aan een vergelijkbare populatie aan respondenten? Om te voldoen aan de casestudy-eisen moesten ze immers zo veel mogelijk gelijk zijn aan elkaar, behalve op het gebied van werkplekinrichting. Uiteindelijk bleek dit niet te gaan lukken. Er zijn nog pogingen gedaan om via saMBO-ICT (een sectoraal IT-platform voor MBO's) inzicht te krijgen in werkplekinrichting bij de scholen, maar ook hier was de bereidheid nihil. Uiteindelijk is tijdens een van de scriptiecirkels de mogelijkheid geopperd om dan maar onder meerdere overheidsorganisaties enquêtes te verspreiden om zo een multiple casestudy te krijgen. De suggestie was dat vijf organisaties met elk 5 respondenten genoeg zou zijn. Uiteindelijk is dat uitgekomen op 110 respondenten bij 15 (semi-) overheidsorganisaties. De contactpersonen bij deze organisaties zijn actief benaderd of hebben gereageerd op een oproep op LinkedIn. Hierbij viel het mij bijzonder op dat er veel bereidheid is onder mensen om mee te helpen met een dergelijk onderzoek. De conclusie is dat er weliswaar veel meer mensen zijn aangeschreven dan in de scriptiecirkel als suggestie werd gegeven, maar dat er veel minder respondenten zijn gebruikt dan initieel de bedoeling was geweest. Daar kwam nog bij dat er ineens ook veel complexere statistiek nodig zou zijn dan in het begin gedacht. Gezien het gebrek aan kennis over statistiek (komende vanuit een academische achtergrond in geschiedenis) was dit aan het einde van het scriptietraject een vertragende factor: het gebrek aan ervaring met sociaalwetenschappelijk onderwijs.

De laatste beperkende factor was dan ook de planning. Ik ben gewend om dicht tegen deadlines aan te werken. Ik zit lang met stukken in mijn hoofd, waar ik alles op orde breng om het tot slot in een gigantische eindsprint op papier te krijgen. Dat heeft altijd gewerkt en ik had verwacht dat dat nu ook weer zou werken. Dat sloot alleen niet aan op de planning en het tempo van de begeleiding. Daar heb ik niet voldoende rekening mee gehouden en ik heb ook niet tijdig genoeg bijgeschakeld toen ik in de gaten kreeg dat dat een probleem kon

worden. Dit resulteerde in een conceptversie die op papier niet veel verder was dan een onderzoeksopzet. Het was dan ook begrijpelijk dat de begeleiders er weinig zinnigs over konden zeggen. Het gebrek aan tijd heeft uiteindelijk ook gezorgd dat ik niet de vooraf bedachte multilevel analyse heb kunnen uitvoeren. Ik heb twee dagen besteed aan het leren en begrijpen van wat de analyse doet en met succes: ik begreep wat het was, wat de meerwaarde was en wat de gedachte erachter was. Ik kreeg het echter niet voor elkaar om het goed toe te passen op mijn data. Ik begreep steeds niet wat er in de (overigens zeer beperkte) documentatie stond en wat mijn resultaten van de analyse precies vertelden. Om die reden is de multilevel analyse dan ook niet opgenomen in mijn onderzoek. Had ik langer gehad, was daar wellicht een andere uitkomst geweest en had de analyse wel in het stuk gezeten. Het neemt echter niet weg dat vier jaar academisch statistiek onderwijs simpelweg niet in drie weken zelfstudie kan worden gestopt.

Wat had ik achteraf anders gedaan? Nu blijkt dat ik in drie weken een scriptie heb geschreven had ik dat dus in augustus al gedaan kunnen hebben. Dan had ik enorm veel mogelijkheden gehad tot feedback en verfijning van het werk. Nu is daar geen tijd en geen mogelijkheid toe geweest. Dat is jammer en dat is onnodig geweest. Tegelijkertijd was het een leertraject waarbij ik weliswaar veel steken heb laten vallen, maar ook aan mezelf heb laten zien in korte tijd tot veel in staat te zijn. Dat is een positieve opsteker en daar komt bij dat ik uiteindelijk het doen van de analyses en de statistiek erg leuk ben gaan vinden. Dat zijn voor mij de positieve kanttekeningen van een lastig scriptietraject. Jammer genoeg kwamen er met deze opzet en deze respondenten geen significante correlaties uit het onderzoek. Ik blijf nog altijd erg betrokken bij het vraagstuk en ben ervan overtuigd dat eventueel vervolgonderzoek, mits goed ontworpen, wel een uitkomst geeft. Die uitkomst is oprecht belangrijk voor de veiligheid van de werkplek en hopelijk komen die resultaten er ooit nog eens.

11 Bibliografie

Abed, J., & Weistroffer, H. (2016). Understanding Deterrence Theory in Security Compliance Behaviour: A Quantitative Meta-Analysis Approach. *Proceedings of the Southern Association for Information Systems Conference* (pp. 1-6). St. Augustine, Florida: SAIS.

Alomari, R., & Thorpe, J. (2019). On password behaviours and attitudes in different populations. *Journal of Information Security and Applications*, 79-89.

Bada, M., Nurse, J., & Sasse, A. (2015). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*, (pp. 118-131). Londen.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, 191-215.

Blythe, J., Coventry, L., & Little, L. (2015). Unpacking Security Policy Compliance: The Motivators and Barriers of Employees' Security Behaviors. *Symposium on Usable Privacy and Security*. Ottawa.

Bryman, A., & Bell, E. (2015). *Business Research Methods.* Oxford: Oxford University Press.

Chiasson, S., & Van Oorschot, P. (2015). Quantifying the security advantage of password expiration policies. *Designs, Codes and Cryptography*, 401-408.

Choong, Y., & Theofanos, M. (2015). What 4,500+ people can tell you–employees' attitudes toward organizational password policy do matter. *International Conference on Human Aspects of Information Security, Privacy, and Trust*, (pp. 299-310).

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of disparate findings. *European Journal of Information Systems, 20*, 643-658.

Dolan, P., Hallsworth, M., Halpern, D., King, D., & Vlaev, I. (2010). *MINDSPACE. Influencing behaviour through public policy*. Londen: Institute for Government, Cabinet Office UK.

Fenwick, T. (2017). *Standardisation, Innovation and Learning in the Workspace: Missions in Complexity Reduction.* Toronto: University of British Columbia.

Floyd, D., Prentice-Dunn, S., & Rogers, R. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology.*, 407-429.

Ghosh, A., Gajar, P., & Rai, S. (2013). Bring Your Own Device (BYOD): Security Risks and mitigating strategies. . *Journal of Global Research in Computer Science*, 62-70.

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the U.S. and South Korea. *Information & Management*, 99-110.

Kotulic, A., & Clark, J. (2004). Why there aren't more information security research studies. *Information & Management*, 597-607.

Lourens, C. (2018, November 16). Interview betreffende werkplekinrichting. (W. d. Graaf, Interviewer)

McAfee. (2018). *Economic Impact of Cybercrime.* Opgehaald van https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf

McDonald, R. (1999). *Test theory: A unified approach.* Mahwah, NJ: Lawrence Erlbaum.

Ministerie van Algemene Zaken. (2018, 03 13). *DPC BIR Documentatie.* Opgehaald van https://www.communicatierijk.nl/vakkennis/r/rijkswebsites/documenten/publicaties/2018/mrt/13/dpc-bir-documenten-tbv-externen

Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. *Network Security*, 5-8.

Norman, P., & Seydel, E. (2005). Protection Motivation Theory. In M. Connor, & P. Norman, *Predicting Health Behaviour: Research and Practice with Social Cognition Models* (pp. 81-126). Chicago: Open University Press.

Olalere, M., Taufik Abdullah, M., Mahmod, R., & Abdullah, A. (2015). A Review of Bring Your Own Device on Security Issues. *SAGE Open*.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. *Proceedings of the 40th Hawaii International Conference on System Sciences.*

Paquette, S., Jaeger, P., & Wilson, S. (2010). Identifying the security risks associated with governmental use of cloud computing. *Government information quarterly*, 245-253.

Prentice-Dunn, S., McMath, B., & Cramer, R. (2009). Protection motivation theory and stages of change in sun protective behavior. *Journal of Health Psychology*, 14.

Rijksoverheid. (2017). *Baseline Informatiebeveiliging Rijksdienst.* Opgehaald van Rijksoverheid.nl: https://www.communicatierijk.nl/vakkennis/r/rijkswebsites/verplichte-richtlijnen/baseline-informatiebeveiliging-rijksdienst

Rogers, R. (1983). Cognitive and physiological processes in fear appeals and attitude change: A Revised theory of protection motivation. In J. Cacioppo, & R. Petty, *Social Psychophysiology* (pp. 136-171). New York: Guilford Press.

Siponen, V., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Systems Security Policy Violations. *MIS Quarterly*, 487-502.

Statista. (2019). Opgehaald van https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, 190-198.

Verschuren, P., & Doorewaard, H. (2007). *Het ontwerpen van een onderzoek.* Amsterdam: Boom Lemma Uitgevers.

Woon, I., Tan, G., & Low, R. (2005). A protection motivation theory approach to home wireless security. *International Conference on Information Systems (ICIS)*, (pp. 367-380).

Yin, R. (2014). *Case Study Research. Design and Methods.* Londen: Sage.

12 Tabellen en figuren

13 Bijlagen

Toegevoegd als bijlage is de vragenlijst zoals via het internet verstuurd. Deze is niet opgenomen in de scriptie zelf, maar als bijlage digitaal verzonden.