Compliance informatieveiligheidsbeleid bij Nederlandse gemeenten

Resultaten van een vignettestudie naar de naleving van informatiebeveiligingsbeleid onder beleidsmedewerkers van Nederlandse gemeenten.

Door: Jeroen Kokje

Studentnummer: 381085

Faculteit: Faculteit der Sociale Wetenschappen, Erasmus Universiteit Rotterdam

Opleiding: Bestuurskunde, Publiek Management

Begeleider: Vincent Homburg

Aantal woorden: 14.583

Stagebedrijf: PBLQ

Stagebegeleider: Henk de Jong

Datum: 29 juni 2020

Voorwoord

Voor u ligt de scriptie ‘Compliance informatieveiligheid bij Nederlandse gemeenten’. Het onderzoek is uitgevoerd bij zeven middelgrote gemeenten in Nederland. De scriptie is geschreven in het kader van de opleiding Publiek Management aan de Erasmus Universiteit Rotterdam. Daarnaast is deze scriptie geschreven in samenwerking met het stagebedrijf PBLQ, waar ik van februari tot juli 2019 stage heb gelopen. In deze tijd is deze scriptie ook geschreven, waarbij deze is afgemaakt van februari tot juni 2020.

Tijdens de stage bij PBLQ heb ik ontzettend veel geleerd. Hiervoor wil ik met name Henk de Jong en Willy Krieger bedanken. Zij hebben mij de mogelijkheid gegeven om binnen te kijken bij deze mooie organisatie. Samen met Henk de Jong heb ik gekozen voor het onderwerp van deze scriptie en hij heeft mij ook geholpen met het in contact komen met respondenten.

Bij dezen wil ik graag ook mijn begeleider vanuit de universiteit, Vincent Homburg, bedanken voor de fijne begeleiding en zijn ondersteuning tijdens dit traject. Het is een langere weg geweest dan gepland, maar uiteindelijk heeft hij het geduld kunnen bewaren en mij door het traject heen getrokken. Ook wil ik alle respondenten bedanken die mee hebben gewerkt aan dit onderzoek. Zonder hun medewerking had ik dit onderzoek nooit kunnen voltooien.

Het hele proces rondom deze scriptie heeft door persoonlijke omstandigheden langer geduurd dan verwacht en gepland. Toch ben ik ontzettend blij dat ik mijn studie en schoolcarrière met dit eindresultaat kan afsluiten. Ik heb erg veel geleerd en ben mezelf tijdens het schrijven van de scriptie meerdere keren tegen gekomen. Hierbij wil ik dan ook mijn ouders bedanken voor de mentale steun tijdens het hele proces.

Ik wens u veel leesplezier toe.

Jeroen Kokje

Samenvatting

Tijdens deze scriptie wordt onderzoek gedaan naar de naleving van voorschriften op het gebied informatiebeveiliging bij Nederlandse gemeenten. Hierbij wordt gekeken naar het perspectief van de werknemer en deze worden daarbij bevraagd met behulp van een survey. Het doel van dit onderzoek is het toetsen van theorieën over naleving van informatieveiligheidsvoorschriften bij Nederlandse gemeenten door hypothesen uit informatieveiligheidsliteratuur te confronteren met een survey onder beleidsmedewerkers van gemeenten. De hoofdvraag van dit onderzoek is als volgt: *Hoe kan de naleving van voorschriften op het gebied van informatieveiligheid door beleidsmedewerkers van Nederlandse gemeenten worden verklaard en welke factoren spelen hierbij een rol?*

De conclusie van dit onderzoek is dat de naleving van voorschriften op het gebied van informatieveiligheid door medewerkers van Nederlandse gemeenten verklaard kan worden met behulp van bewustzijn. Hoe meer bewustzijn er is onder de medewerkers, hoe meer men zich houdt aan de richtlijnen en voorschriften op het gebied van informatieveiligheid. De uitkomsten laten zien dat de andere variabelen die in dit onderzoek zijn meegenomen geen significant verband aantonen. Sancties, leiderschap en risicoaversie hebben volgens dit onderzoek geen verband met de naleving van voorschriften op het gebied van informatieveiligheid.

Dit is tot stand gekomen door een model dat is afgeleid uit eerder onderzoek. Op basis van verschillende theoretische onderzoeken en eerdere onderzoeken naar naleving van informatieveiligheidsbeleid is er een keuze gemaakt welke variabelen in dit onderzoek zijn meegenomen. Met name het onderzoek van Moody et al. (2018) is hierbij een richtlijn geweest. Vervolgens is er een digitale vragenlijst opgesteld, die uitgezet is onder respondenten. Deze vragenlijst bestaat uit vragen over de verschillende variabelen. Daarnaast zijn er drie vignetten toegevoegd over het onderwerp informatieveiligheid. Vignetten zijn scenarioschetsen die meer context geven dan een gewone surveyvraag, zodat de gevoeligheid van het onderwerp enigszins weggenomen kan worden en de respondent zo eerlijk mogelijk kan antwoorden. Er is eveneens een keuze gemaakt over de respondenten. Het onderzoek is gericht op beleidsmedewerkers bij Nederlandse gemeenten. Er is contact opgenomen met meerdere gemeenten, die de vragenlijst hebben uitgezet onder hun beleidsmedewerkers.

De resultaten van de survey zijn vervolgens geanalyseerd met behulp van een multiple regressieanalyse via SPSS, een statistiek programma. Empirische data die zijn verzameld door middel van een vignetonderzoek naar de antwoorden van gemeentelijke overheidsmedewerkers, wijzen erop dat er weinig steun is voor de hypothesen die in deel twee worden gepresenteerd; in twee van de drie vignetten is er steun voor het idee dat bewustzijn de naleving beïnvloedt. Het is duidelijk dat percepties van sancties, managementstijl en risicoaversie geen significante impact hebben op de naleving van het informatiebeveiligingsbeleid en de richtlijnen.

Inhoudsopgave

1. Inleiding

1.1 Aanleiding

Op 3 mei 2019 kwam het bericht naar buiten dat er een datalek ontstaan is bij het UWV. Ongeveer 117.000 CV's zijn illegaal gedownload bij de uitkeringsinstantie. Men vermoedt dat phishing of spam de oorzaak van het lek is. Het account van een medewerker is op die manier waarschijnlijk gehackt en misbruikt (NOS, 2019). Informatiebeveiliging, ook wel cybersecurity genoemd, dient ervoor te zorgen dat deze risico's worden uitgesloten. In het geval van het UWV is er iets misgegaan en heeft een medewerker op één of andere manier een risico genomen. Phishing en spam zijn voorbeelden van cybercrime waarmee criminelen proberen om in de systemen van een organisatie te komen. Ook malware of andere manieren van hacken zijn populair. Overheden beschikken over veel data, wat hen een interessant slachtoffer maakt voor hackers en cybercriminelen. Dit vereist dat overheden goed up-to-date moeten zijn op het gebied van informatiebeveiliging.

In oktober 2018 stelde minister Bijleveld van Defensie dat Rusland en Nederland in een cyberoorlog verkeren: "In april werden vier Russische militaire agenten het land uitgezet, omdat ze het wifi-netwerk van de OPCW in Den Haag wilden hacken" (Nu.nl, 2018). De MIVD waarschuwt al jaren voor cyberspionage, met name door Rusland en China. Defensie investeert onder andere hierdoor extra in haar cyber capaciteit en inlichtingendienst. Hoe Nederland zich het beste kan verdedigen tegen digitale dreigingen staat beschreven in de Defensie Cyber Strategie 2018. Hierbij is het doel om digitaal weerbaar te blijven en de controle te houden over de eigen IT en wapensystemen (NOS, 2018). Ook de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) waarschuwt voor ontwrichting van de maatschappij door toedoen van cybercrime: "De digitale dreiging voor de nationale veiligheid is permanent. Vrijwel alle vitale processen en systemen in Nederland zijn deels of volledig gedigitaliseerd waarbij er nauwelijks terugvalopties of analoge alternatieven zijn. Deze factoren gecombineerd met het achterblijven van de weerbaarheid, maken Nederland kwetsbaar voor digitale aanvallen" (NCTV, 2019).

Informatiebeveiliging is niet alleen nationaal van belang, maar ook lokaal cruciaal. Gemeenten en andere overheden beschikken over een bulk aan data, wat hen een interessant doelwit maakt. Dat overheden bezig zijn met de ontwikkeling van de veiligheid rondom informatie blijkt uit de invoering van de Baseline Informatiebeveiliging Overheid (BIO). De VNG (2019) zegt hierover het volgende: “informatieveiligheid is een randvoorwaarde voor een professionele gemeente. We werken steeds meer samen in een netwerkende overheidsomgeving. Daarbij moeten we impliciet kunnen vertrouwen op een adequaat beveiligingsniveau van ketenpartners. Gemeente, Rijk, waterschappen en provincies gaan daarom over op één uniform normenkader voor informatiebeveiliging.” Deze Baseline is een voorbeeld waaruit blijkt dat overheden in Nederland bezig zijn met de ontwikkeling rondom informatiebeveiliging. Hierbij is een trend te zien, waarbij de focus niet alleen ligt bij het technische aspect. Bijna elke organisatie beschikt tegenwoordig over een Chief Information Security Officer (CISO) en over een informatiebeveiligingsbeleid met richtlijnen omtrent informatiebeveiliging. Dit geeft aan dat veel organisaties het probleem rondom cybercrime en informatieveiligheid serieus nemen. Met name het openbaar bestuur is hierbij bijzonder, aangezien ieder issue bij de overheid groot gemaakt wordt in de media. Dit tast vervolgens het vertrouwen van de burger in het openbaar bestuur aan. Ook de Tweede Kamer merkt dit, aangezien zij een parlementair onderzoek begint naar hoe de politiek zijn greep op de digitalisering kan vergroten (NOS, 2019). Hierbij wordt bijvoorbeeld de mogelijkheid voor een minister van digitalisering en informatieveiligheid geopperd.

1.2 Probleemanalyse

Tegenwoordig zijn risico's met betrekking tot informatiebeveiliging dus een grote uitdaging. Dit geldt voor zowel publieke als private organisaties, omdat deze risico's ernstige gevolgen kunnen hebben zoals imagoschade en financiele schade. Zorgen voor informatiebeveiliging wordt een van de topprioriteiten van het management in veel organisaties. Hierbij ligt de focus vaak op de technische kant van informatieveiligheid en hoewel dit soort oplossingen helpen de informatiebeveiliging te verbeteren (Straub 1990), een beroep op hen uitsluitend is zelden genoeg om het risico te elimineren (Siponen, 2005). Zelfs nu organisaties meer investeren in op technologie gebaseerde oplossingen, blijven incidenten op dit gebied toenemen.

Informatiebeveiliging bestaat dus niet alleen uit ICT, systemen of software; informatiebeveiliging is mensenwerk. Het belang van een structurele bestuurlijke aandacht voor dit thema is hierbij zeer groot. Wanneer alle technische aspecten op orde zijn, kunnen alsnog menselijke handelingen lekken van data al dan niet opzettelijk veroorzaken. Oorspronkelijk probeerden organisaties dit op te vangen door checklists, handleidingen en logische beveiligingsmaatregelen (Dhillon & Backhouse, 2001). Enkel het voldoen aan de beveiligingschecklist sluiten menselijke fouten niet uit. Menselijke fouten treden vooral op door onbewust gedrag of doordat handelingen op de automatische piloot worden uitgevoerd (De Bruijn et al., 2010). D'Arcy en Hovav (2008) stellen dat het begrijpen van de factoren die invloed hebben op de effectiviteit van beveiligingsmaatregelen een consistent thema is in de literatuur over informatiebeveiliging. Kortweg wordt informatiebeveiliging conventioneel beschreven als het beschermen van informatievoorzieningen tegen kwaadwillige gebruikers (Pieters, 2011, p. 326).

In de wetenschappelijke literatuur gaat het met name over waarom het belangrijk is om te werken aan het informatiebeveiligingsbewustzijn. Gedragsmaatregelen worden effectiever geacht dan organisatorische en technische maatregelen (Hagen et al., 2008). Het gedrag van medewerkers speelt namelijk een grote rol bij de effectiviteit van de implementatie van technische en organisatorische (procedurele) maatregelen, omdat medewerkers deze maatregelen vaak eenvoudig kunnen omzeilen. Het niet naleven van procedures door medewerkers is een grote zorg voor elke organisatie (Siponen & Karjalainen, 2011).

De focus op de publieke sector is hier van belang en relevant, aangezien Perry (Perry, 1996) betoogde dat werknemers in de publieke sector worden gemotiveerd door de wens om het algemeen belang te dienen, een niveau dat typisch de individuele motivaties of zelfs organisatiedoelen overtreft. De studie van de naleving van het informatiebeveiligingsbeleid bij werknemers in de publieke sector biedt interessante mogelijkheden om te onderzoeken hoe naleving (of het gebrek daaraan) van het informatiebeveiligingsbeleid plaatsvindt bij professionals met een hoger niveau van motivatie voor de openbare dienst (en dus ruime mogelijkheden om naar een hogere orde te verwijzen) normen ter rechtvaardiging van het niet naleven van beveiligingsbeleid en -richtlijnen). In dit onderzoek gaan we in op de vraag welke factoren van invloed zijn op de naleving van het informatiebeveiligingsbeleid in Nederlandse gemeenten. Blijkbaar gaat er nog genoeg mis op het gebied van informatiebeveiliging, maar de vraag is waar het precies mis gaat en waarom.

De focus ligt hierbij op de naleving van informatiebeveiligingsbeleid, die in relatie staat tot de gedragingen van mensen.

1.3 Probleemstelling

De naleving van informatiebeveiligingsbeleid en -voorschriften in de publieke sector staat centraal in dit onderzoek. Hierbij is gekozen voor een large-n, deductief onderzoek, op basis van eerdere onderzoeken. Het doel van dit onderzoek is het toetsen van theorieën over naleving van informatieveiligheidsvoorschriften bij Nederlandse gemeenten door hypothesen uit informatieveiligheidsliteratuur te confronteren met een survey onder beleidsmedewerkers van gemeenten.

De hoofdvraag van dit onderzoek is als volgt:
Hoe kan de naleving van voorschriften op het gebied van informatieveiligheid door beleidsmedewerkers van Nederlandse gemeenten worden verklaard en welke factoren spelen hierbij een rol?

Deze hoofdvraag wordt beantwoord met behulp van twee deelvragen:
Welke hypothesen met betrekking tot informatieveiligheidsvoorschriften kunnen uit de literatuur worden afgeleid?
W*elke uitspraken kunnen worden gedaan na confrontatie van die hypothesen met data uit de survey onder beleidsmedewerkers van Nederlandse gemeenten?*

1.4 Onderzoeksmethode

Dit onderzoek is large-n, deductief en toetsend van aard. Hier is voor gekozen, omdat er al een groot aantal onderzoeken is gedaan naar handhaving van informatiebeveiligingsbeleid, zoals Moody et al. (2018), Siponen & Vance (2010) en Bulgurcu et al. (2010). Dit onderzoek wordt echter uitgevoerd in een andere context, waarbij de vraag is of dezelfde resultaten naar voren zullen komen. In dit onderzoek is gekozen voor een survey onder beleidsmedewerkers van Nederlandse gemeenten, omdat op die manier een grote hoeveelheid data kan worden onderzocht en zo de opgestelde hypothesen kunnen worden getoetst. De survey is uitgezet bij verschillende grote en middelgrote gemeenten. De respondenten zijn beleidsmedewerkers, verspreid over verschillende beleidsdomeinen om zo een algemeen beeld te krijgen.

Hierbij is kennis van ICT geen vereiste, werken met een digitale werkplek wel. Met behulp van verschillende analyses, waaronder de regressieanalyse, kunnen vervolgens conclusies worden getrokken.

De scriptie start met een literatuurreview, waarin een aantal grond theorieën over de naleving van richtlijnen omtrent informatiebeveiliging wordt opgesteld. Hier komen de gebruikte variabelen uit voort, dat zijn er in dit onderzoek vijf. In een conceptueel onderzoeksmodel zijn de verschillende hypothesen opgesteld, die worden getoetst met behulp van een regressieanalyse. De uitkomsten hiervan bepalen of de hypothesen worden verworpen of worden aangenomen.

1.5 Maatschappelijke en wetenschappelijke relevantie

Zoals eerdergenoemde voorbeelden laten zien, wordt informatiebeveiliging een steeds belangrijker onderwerp. Iedereen krijgt hiermee te maken; bedrijven, overheden en individuen. De digitalisering van de samenleving neemt steeds verder toe, wat zorgt voor een groter belang van de veiligheid van data en gegevens. Overheden beschikken over een grote hoeveelheid data en gegevens van de burger. Hierbij is het erg belangrijk dat deze goed beschermd worden en niet zomaar ingezien kunnen worden door iedereen. Dit onderzoek neemt een kijkje in de manier waarop de medewerkers van deze overheden, in dit geval gemeenten, omgaan met informatiebeveiliging en richtlijnen op dit gebied. Hierbij draait het niet alleen om de stand van zaken, maar kan ook worden gezocht naar oorzaken.

Er bestaan eerdere onderzoeken naar de naleving van richtlijnen op het gebied van informatiebeveiliging, zoals Moody et al. (2018), Siponen & Vance (2010) en Bulgurcu et al. (2010). Deze onderzoeken kennen echter een andere context, wat dit onderzoek extra interessant maakt. De vraag die opkomt is namelijk of de resultaten van onderzoeken in een andere context overeenkomen met de resultaten van dit onderzoek in de Nederlandse context.

1.6 Leeswijzer

Deze scriptie is opgebouwd uit verschillende hoofdstukken, die gezamenlijk het onderzoek vormen. Allereerst worden de methoden en technieken die worden gebruikt uiteengezet, waarbij ook de betrouwbaarheid en validiteit van het onderzoek worden behandeld. Hierop volgt de literatuurreview in hoofdstuk 3. In de literatuurreview worden verschillende concepten die in dit onderzoek worden gebruikt uiteengezet met behulp van wetenschappelijke theorieën. In hoofdstuk 4 worden de resultaten van de survey en de analyse van de data besproken.

Vervolgens worden in datzelfde hoofdstuk de deelvragen en de hoofdvraag van het onderzoek beantwoord, waarbij conclusies kunnen worden getrokken. Tot slot worden aanbevelingen gedaan en worden beperkingen besproken bij de discussie. De vragenlijst en geanalyseerde documenten zijn terug te vinden in de bijlagen.

2. Literatuurreview

2.1 Inleiding

In de literatuurreview worden verschillende wetenschappelijke theorieën uiteengezet. Theorieën over informatiebeveiliging hebben achtergronden in criminologie, sociologie en gedragswetenschap. Deze theorieën leiden zijn de basis voor de variabelen die in dit onderzoek worden meegenomen. In dit hoofdstuk wordt de eerste deelvraag van dit onderzoek beantwoord: welke hypothesen met betrekking tot informatieveiligheidsvoorschriften kunnen uit de literatuur worden afgeleid?

2.2 Informatiebeveiligingsbeleid

Beleid en richtlijnen rondom informatiebeveiliging worden in de theorie vaak Information Security Policy (ISP), oftewel informatiebeveiligingsbeleid genoemd. Zoals bij de probleemanalyse is besproken, draait informatiebeveiliging niet meer alleen om de technische kant. Het informatiebeveiligingsbeleid van een organisatie richt zich dan ook met name op individuele en organisatorische perspectieven, waarbij de naleving door medewerkers vaak naar voren komt als een belangrijke socio-organisatorische hulpbron (Boss and Kirsch 2007; Siponen et al. 2007).

Informatiebeveiligingsbeleid bestaat uit richtlijnen, die ervoor moeten zorgen dat medewerkers hun werk zowel goed als veilig kunnen uitvoeren. Een informatiebeveiligingsbeleid is in het algemeen gericht op een divers publiek van medewerkers voor wie informatiebeveiliging een vreemd en nieuw concept kan zijn. Het is daarom van cruciaal belang dat het beleid een korte en begrijpelijke definitie van informatiebeveiliging bevat om een uniform begrip van het concept in de hele organisatie te waarborgen (Höne & Eloff, 2002). De principes voor informatiebeveiliging beschrijven de algemene regels met betrekking tot informatiebeveiliging binnen een organisatie. Deze principes proberen de gebruikers uit te leggen wat het juiste en onjuiste gedrag in de organisatie is met betrekking tot verschillende onderwerpen en concepten. Sommige van deze principes zullen nauw verbonden zijn met de cultuur van een organisatie of met wettelijke vereisten voor de sector waarin de organisatie functioneert. Andere zullen echter van toepassing zijn op alle organisaties en worden aangetroffen in elk informatiebeveiligingsbeleid, zoals virusbescherming en gebruikersbewustzijn en -onderwijs. De Bruijn & Janssen (2017) zeggen het volgende over informatiebeveiliging: “Cybersecurity is een wereldwijd fenomeen dat een complexe sociaal-technische uitdaging vormt voor overheden, maar waarbij de betrokkenheid van individuen vereist is” (p.1).

Werknemers worden vaak de zwakste link in informatiebeveiliging genoemd volgens De Bruijn & Janssen (2017). Organisaties maken informatiebeveiligingsbeleid om werknemers te voorzien van richtlijn over hoe zij veilig hun baan kunnen uitvoeren en alle systemen kunnen gebruiken. Dit beleid is een belangrijk beginpunt, maar hier houdt informatiebeveiliging niet op. De naleving van het informatiebeveiligingsbeleid is nog vele malen belangrijker. Naleving of compliance houdt in dat de medewerker de regels en voorschriften die in het informatiebeveiligingsbeleid staan volgt. Handhaving houdt in dat de organisatie ervoor zorgt dat de medewerkers ook daadwerkelijk compliance vertonen en dat er wordt ingegrepen indien nodig. Onder andere Bulgurcu et al. (2010) onderzoeken verschillende factoren die medewerkers motiveren om zich aan het informatiebeveiligingsbeleid van de organisatie te houden. Dit is dan ook een van de onderzoeken waarop in dit onderzoek wordt voortgeborduurd. Hierbij worden verschillende theorieën uiteengezet waarom medewerkers zich niet houden aan informatiebeveiligingsbeleid, waaronder de Theory of Planned Behaviour en de Theory of Reasoned Action.

2.3 Behavioural theory

Gedragstheorieën zijn met name van toepassing op onbewuste, niet-opzettelijke overtredingen. Deze theorieën gaan namelijk over waarom mensen zich gedragen zoals ze doen en wat gedrag stimuleert. In dit onderzoek wordt de Theory of Planned Behaviour (TPB) (Ajzen & Sheikh, 2013) gezien als belangrijkste gedragstheorie. Deze theorie vormt de basis voor een onderzoek naar de relatie tussen houding, intentie en gedrag. Pahnila et al., 2007 gebruikt deze theorie als basis in onderzoek in de compliance-context van het beveiligingsbeleid. De Theory of Planned Behaviour focust op attitudes, subjectieve normen en gedragscontrole (Ajzen & Sheikh, 2013). Attitudes bestaan uit de verwachte uitkomsten van vertoond gedrag van de persoon en de evaluatie van deze uitkomsten. Hierbij bedenkt iemand van tevoren wat het resultaat zal zijn van zijn of haar gedrag en evalueert diegene of dit wenselijk of onwenselijk is (Ajzen & Sheikh, 2013) Subjectieve normen zijn de normatieve opvattingen van een persoon en de motivatie om aan deze norm te willen voldoen. Hierbij is de sociale norm en de sociale invloed van groot belang (Ajzen & Sheikh, 2013). Gedragscontrole doelt op de mate waarin iemand denkt het gedrag ook daadwerkelijk uit te kunnen voeren (Ajzen & Sheikh, 2013).

Informatiebeveiligingsbewustzijn doelt op de bereidheid van een medewerker om regels te volgen, doordat zij zich bewust zijn van de risico's en gevaren het met zich meebrengt als zij dit niet doen. Hoewel beloningen en straffen externe motivaties bieden, bieden de intrinsieke verlangens van een werknemer de interne motivatie om regels en voorschriften te volgen (Tyler & Blader 2005). Informatiebeveiligingsbewustzijn wordt gedefinieerd als de kennis en het begrip van een werknemer van de richtlijnen die zijn voorgeschreven in het informatiebeveiligingsbeleid van de organisatie. Deze definitie is in overeenstemming met de opvatting dat veiligheidsbewustzijn een situatie is waarin werknemers zich bewust zijn van en zich optimaal inzetten voor de veiligheidsdoelstellingen van hun organisaties (Siponen, 2000). Iemands bewustzijn van informatiebeveiliging kan worden opgebouwd uit directe levenservaringen, zoals eens schade te hebben geleden door een virusaanval of zijn gestraft wegens het niet naleven van beveiligingsrichtlijnen. Ook een interne cursus kan informatiebeveiligingsbewustzijn stimuleren (Bulgurcu et al., 2010).

Bulgurcu et al. (2010) hebben een onderzoek gedaan naar bewustzijn op het gebied van informatieveiligheidsbewustzijn, waarin wordt aangegeven dat er een gebrek is aan onderzoeken waarin informatiebeveiliging bewustzijn centraal staat. Siponen (2000) heeft in zijn onderzoek verschillende methoden voorgesteld om het bewustzijn te vergroten op basis van verschillende theoretische perspectieven. Andere studies zoals Furnell et al. (2002) en Hentea (2005) benadrukken het belang van educatie en training. D'Arcy et al. (2009) suggereerde op basis van onderzoek dat de focus met name moet liggen op bewustzijn, onder meer met behulp van campagnes, training en educatie. Ook De Bruijn & Janssen (2017) benoemen dat een gebrek aan bewustzijn op het gebied van informatiebeveiliging een groot probleem vormt in de cybersecurity. De urgentie en het gedrag van mensen laten zien dat er nog geen sprake is van een groot bewustzijn in organisaties.

De Theory of Planned Behaviour laat net als eerdere onderzoeken zien dat bewustzijn invloed kan hebben op het handelen van medewerkers op het gebied van informatiebeveiliging. Hierbij wordt de eerste hypothese van dit onderzoek opgesteld. Deze hypothese is te zien in tabel 1.

Theory of planned behavior	
Variabelen	Bewustzijn
Bronnen	(Ajzen, Sheikh, 2013; D'Arcy et al., 2009, Bulgurcu et al., 2010)
Hypothese 1	Naarmate er meer sprake is van informatiebeveiligingsbewustzijn, zal er meer handhaving van richtlijnen van informatieveiligheidsbeleid door medewerker van Nederlandse gemeenten zijn.

Tabel 1: Theory of Planned Behaviour

2.4 Rational Choice Theory

De Rational Choice Theory (RCT) wordt als een basistheorie gezien in onderzoeken naar motiverende factoren onder medewerkers. Deze theorie is gebaseerd op de afschrikkingstheorie, die stelt dat overtredingen kunnen worden beperkt door sancties op te leggen. Hoewel RCT vaak wordt toegepast om crimineel gedrag te verklaren, is het bedoeld om 'voldoende algemeen te zijn om alle schendingen te behandelen' (Becker, 1968, blz. 170) en is daarom ook van toepassing op de studie van schendingen van informatiebeveiligingsbeleid. Volgens de RCT maken individuen een afweging tussen overtreding en sanctie, om vervolgens te kiezen wat voor hen het beste is. Hoewel sommigen kritiek hebben geuit op RCT voor het aannemen van een volledig rationele misdadiger (Cornish & Clarke, 1986), zijn voorstanders van RCT van mening dat de beslissingen van daders om overtredingen te plegen subjectieve beoordelingen zijn en "vaak objectief verkeerd zijn, vanwege individuele begrensde rationaliteit" (Becker & Mehlkop, 2006, blz. 197). Bulgurcu (2010) benoemt dat “gepercipieerde voordelen, morele overtuigingen en informele sancties een aanzienlijke invloed hebben op de intenties van werknemers om informatiebeveiligingsbeleid te schenden”. In datzelfde onderzoek wordt benoemd dat formele sancties niet significant effectief worden bewezen, wat suggereert dat de context van computermisbruik enerzijds en opzettelijke schendingen van het IS-beveiligingsbeleid anderzijds aanzienlijk kunnen verschillen (Siponen & Vance, 2012). Hierbij is van belang dat het bij de RCT gaat om een bewuste, afgewogen en opzettelijke overtreding. Fouten of onbewuste, niet-opzettelijke overtredingen worden hierbij niet benoemd.

Siponen & Vance (2012) benoemen dat er een afschrikkingseffect gekoppeld moet zijn aan sancties, om deze effectief te maken. Losstaande sancties zijn in hun onderzoek niet gekoppeld aan meer handhaving van voorschriften op het gebied van informatiebeveiliging. Zij zeggen dat monitoring en controle-inspanningen weinig invloed lijken te hebben op de vraag of individuen kunnen worden gemotiveerd door afschrikmechanismen, tenzij er voorbeelden zijn waarbij mensen betrapt en gestraft worden. Als er geen voorbeelden zijn van straffen, wordt het effect van afschrikmiddelen marginaal genoemd (Siponen & Vance, 2012). D'Arcy & Hovav (2004) hebben een theoretisch model gemaakt op het gebied van sancties en Peace et al. hebben sancties in een publieke context onderzocht. Herath & Rao (2009) hebben sancties op het gebied van informatiebeveiliging in de publieke sector onderzocht, maar hier kwamen gemengde resultaten uit.

Op basis van de Rational Choice Theory is gekozen om sancties te identificeren als onafhankelijke variabele. Bij het opstellen van de sanctie zal de organisatie moeten beseffen dat deze zodanig zwaar of streng is, dat een werknemer geen voordeel meer ziet. Hierbij is van belang dat sancties per gemeente kunnen verschillen. Sancties kunnen hierbij zowel monetair als non-monetair zijn. Het gaat hier dus om een straf, die aan de medewerker wordt uitgedeeld als gevolg van een overtreding van de richtlijnen van informatiebeveiliging. Sancties is de tweede variabele van dit onderzoek en deze lijdt tot een tweede hypothese. Hypothese 2 is te vinden in tabel 2.

Rational choice theory	
Variabelen	Sancties
Bronnen	(Bulgurcu et al., 2010; Siponen & Vance, 2010;)
Hypothese 2	Naarmate er meer sancties in de organisatie zijn voor overtredingen op het gebied van informatiebeveiliging, zal er meer handhaving van richtlijnen van informatieveiligheidsbeleid plaatsvinden.

Tabel 2: Rational Choice Theory

2.5 Sociale omgevingstheorie

De sociale omgeving van een medewerker kan invloed hebben op zijn of haar gedrag. Het gaat hierbij om de directe sociale omgeving die al dan niet het gedrag van individuen beïnvloedt. Moody (Moody et al., 2018) verwijst naar Triandis (1977) Theory of Interpersonal Behavior om te beweren dat groepsdruk of sociale invloed het gedrag en de beslissingen van individuen beïnvloedt om zich op een bepaalde manier te gedragen. Hierbij is de kerngedachte dat organisatieleden niet in een vacuüm opereren, maar functioneren in een sociale omgeving bestaande uit peers, superieuren, opdrachtgevers et cetera. Door interactie met deze leeftijdsgenoten worden specifieke normen (zoals gewenst gedrag dat wordt geïmpliceerd door informatiebeveiligingsbeleid) verspreid in groepen individuen. De meer generieke literatuur over adoptie en verspreiding van technologieën verwijst ook naar groepsdruk en sociale invloed als componenten van een verklaring voor de acceptatie van technologieën.

Herath & Rao (2009) benoemen social influence nadrukkelijk in hun onderzoek, waarbij zij aangeven “dat normatieve overtuigingen gerelateerd aan verwachtingen van relevante anderen een significante impact hebben op gedrag van werknemers” (Herath & Rao, 2009; p.118). Dit laat volgens hen zien dat werknemers hun gedrag aanpassen, omdat zij druk voelen door de verwachtingen van anderen, zoals leidinggevenden, collega’s en IT-personeel.

Ondanks wisselend succes van het concept sociale norm, is in dit onderzoek gekozen om de sociale invloed mee te nemen als onafhankelijke variabele. Meerdere theoretische onderzoeken benadrukken het belang van sociale aspecten van technologiegebruik inclusief sociale invloed (Fulk et al., 1987), waardoor ook in de Nederlandse context gekeken moet worden of dit van invloed is op de handhaving van richtlijnen van informatiebeveiligingsbeleid. Dit heeft geleid tot de derde hypothese, die te vinden is in tabel 3.

Sociale omgevingstheorie	
Variabelen	Social influence
Bronnen	(Moody et al., 2018, Herath & Rao, 2009, Triandis, 1977)
Hypothese 3	Naarmate er meer sprake is van social influence, zal er meer handhaving van richtlijnen van informatieveiligheidsbeleid door medewerker van Nederlandse gemeenten zijn.

Tabel 3: Sociale omgevingstheorie

2.6 Leadership theory

Transformationele leiders beïnvloeden de organisatiebetrokkenheid van volgers door volgelingen aan te moedigen kritisch te denken door nieuwe benaderingen te gebruiken, volgelingen bij besluitvormingsprocessen te betrekken, loyaliteit te inspireren, en tegelijkertijd de verschillende behoeften van elke volger te erkennen en te waarderen om zijn of haar persoonlijk potentieel te ontwikkelen (Bass & Avolio, 1994). Door volgelingen aan te moedigen nieuwe manieren te zoeken om problemen en uitdagingen te benaderen en te identificeren met de behoeften van volgers, kunnen transformationele leiders hun volgers motiveren om meer betrokken te raken bij hun werk, wat resulteert in hogere niveaus van organisatorische betrokkenheid (Walumbwa & Lawler, 2003). Deze visie wordt ondersteund door onderzoek dat aantoont dat de betrokkenheid van de organisatie hoger was voor werknemers van wie de leiders deelname aan de besluitvorming aanmoedigen (Jermier & Berkes, 1979; Rhodes & Steers, 1981), de overwegingen benadrukten (Bycio, Hackett, & Allen, 1995), en waren ondersteunend en bezorgd over de ontwikkeling van hun volgelingen (Allen & Meyer, 1996). Er is echter weinig onderzoek gedaan naar de directe link tussen leiderschap en organisatiebetrokkenheid.

Ook over de invloed van leidinggevenden hebben Herath & Rao (2009) uitspraken gedaan op basis van hun onderzoek. Zo benoemen zij dat leidinggevenden beveiligingsnaleving kunnen verbeteren door het creëren of verbeteren van het beveiligingsklimaat in hun organisatie (Herath & Rao, 2009; p.188). Humaidi & Balakrishnan (2015) geven aan dat zowel transactioneel als transformationeel leiderschap invloed hebben op naleving op het gebied van informatiebeveiliging bij medewerkers.

Leiderschap wordt in dit onderzoek meegenomen als onafhankelijke variabele, aangezien het een goede voorspeller lijkt te zijn op basis van eerder onderzoek. In dit onderzoek wordt de term consideration, oftewel coaching, gebruikt. Leiderschap zelf is een lastig te onderzoeken concept, omdat leiderschap verschillende onderdelen en concepten omvat. Consideration is een van die concepten en is in dit onderzoek gebruikt als vorm van leiderschap. Hierbij gaat het om ondersteunen en coaching van de medewerker, zodat deze de richtlijnen van informatiebeveiliging naleeft. De hypothese die bij de variabele leiderschap hoort, is te vinden in tabel 4.

Leiderschapstheorie: transformationeel leiderschap	
Variabalen	Consideration
Bronnen	(Aviolo & Bass, 1990; Herath & Rao, 2009; Humaidi & Balakrishnan, 2015)
Hypothese 4	Naarmate er meer sprake is van coachend leiderschap (consideration), zal er meer handhaving van richtlijnen van informatieveiligheidsbeleid door medewerker van Nederlandse gemeenten zijn.

Tabel 4: Leiderschapstheorie

2.7 Persoonlijkheidstheorie

Naast de variabelen bewustzijn, sancties, social influence en coachend leiderschap, wordt in dit onderzoek ook het effect van risicoaversie op de mate van handhaving van richtlijnen van informatiebeveiliging onderzocht. Deze term komt uit de psychologische literatuur over persoonlijkheidskenmerken, die ook wordt onderzocht in de criminologische literatuur. Risicoaversie is het tegenovergestelde van risicobereidheid. Risicobereidheid is gedefinieerd als de neiging van een persoon om risico's te nemen of risico's te vermijden (Nicholson et al., 2005). Hoewel risicoperceptie van situatie tot situatie verschilt, blijft de houding van een individu ten aanzien van waargenomen risico relatief stabiel (Weber & Milliman, 1997).

Onzekerheidsvermijding beschrijft 'de mate waarin mensen zich bedreigd voelen door dubbelzinnige of onbekende situaties' (Hofstede 2001; p. 161). Hoe hoger deze vermijding is, hoe meer behoefte een persoon heeft aan voorspelbaarheid, geschreven expliciete regels en gestructureerde situaties. Een lagere onzekerheidsvermijding leidt tot meer neiging om risico's te nemen (Hofstede 2001). Mensen die een laag onzekerheidsvermijdingsniveau hebben, zijn volgens Sharma (2010) minder emotioneel en nemen risico's. Ze hebben een grotere behoefte om de omgeving, gebeurtenissen en situaties in hun persoonlijke leven te beheersen (Sharma, 2010). De persoonlijkheidstheorie is in eerdere onderzoeken op het gebied van handhaving van informatiebeveiligingsvoorschriften niet meegenomen. Toch lijkt risicoaversie een voorspeller te zijn voor handelen van mensen, ook op het gebied van informatieveiligheid. Dit is de reden dat deze variabelen wel is meegenomen in dit onderzoek, terwijl deze in eerdere onderzoeken dus niet mee werd genomen.

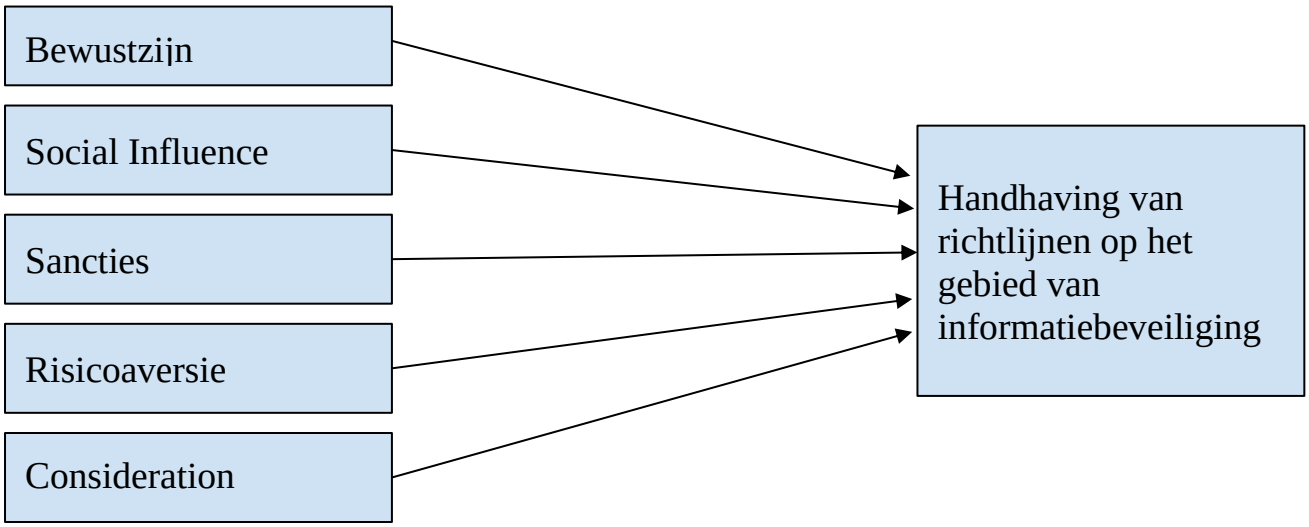
In dit specifieke onderzoek richten we ons op de individuele eigenschap van risicoaversie en veronderstellen we dat risicoaversie een voorspeller is van compliance. Meer in het bijzonder veronderstellen we dat individuen die meer risicomijdend zijn, minder geneigd zijn om te voldoen aan het informatiebeveiligingsbeleid, gezien de neutralisatie plaatsvindt, dan individuen die minder risicomijdend zijn. Dit brengt ons bij de laatste hypothese van dit onderzoek, die te vinden is in tabel 5.

Risicoaversie	
Variabalen	Risicoaversie
Bronnen	(Nicholson et al., 2005; Hofstede, 2001; Sharma, 2010)
Hypothese 5	Naarmate er meer sprake is van risicoaversie op het gebied van informatiebeveiliging, zal er meer handhaving van richtlijnen van informatieveiligheidsbeleid door medewerker van Nederlandse gemeenten zijn.

Tabel 5: Risicoaversie

2.8 Tussenconclusie en conceptueel model

De verschillende theorieen van dit onderzoek zorgen voor meerdere variabelen. Deze variabelen worden meegenomen in dit onderzoek met behulp van hypothesen, die getoetst worden. De theory of planned behaviour leidt tot de variabele bewustzijn, de rational choice theory tot de variabele sancties, de sociale omgevingstheorie tot de variabele social influence, de leiderschapstheorie tot de variabele consideration en de persoonlijkheidstheorie tot de variabele risicoaversie. Met het opstellen van de hypothesen en bijbehorend conceptueel model, te zien in tabel 6, is de eerste deelvraag van dit onderzoek beantwoord. In het vervolg van dit onderzoek wordt gekeken of deze variabelen en hypothesen daadwerkelijk verband houden met de handhaving van richtlijnen op het gebied van informatiebeveiliging. Het conceptueel model van dit onderzoek is dan als volgt:



Tabel 6: Conceptueel model

Er zijn vijf hypothesen afgeleid:

H1: Naarmate er meer sprake is van informatiebeveiligingsbewustzijn, zal er meer handhaving van richtlijnen van informatieveiligheidsbeleid door medewerker van Nederlandse gemeenten zijn.

H2: Naarmate er meer sancties in de organisatie zijn voor overtredingen op het gebied van informatiebeveiliging, zal er meer handhaving van richtlijnen van informatieveiligheidsbeleid plaatsvinden.

H3: Naarmate er meer sprake is van social influence, zal er meer handhaving van richtlijnen van informatieveiligheidsbeleid door medewerker van Nederlandse gemeenten zijn.

H4: Naarmate er meer sprake is van coachend leiderschap (consideration), zal er meer handhaving van richtlijnen van informatieveiligheidsbeleid door medewerker van Nederlandse gemeenten zijn.

H5: Naarmate er meer sprake is van risicoaversie op het gebied van informatiebeveiliging, zal er meer handhaving van richtlijnen van informatieveiligheidsbeleid door medewerker van Nederlandse gemeenten zijn.

3. Methodologie

3.1 Inleiding

In dit hoofdstuk worden de gemaakte keuzes in dit onderzoek uitgelegd en onderbouwd. Hierbij wordt allereerst ingegaan op de gekozen onderzoeksmethode, vervolgens op de gekozen respondenten en op de analysemethode. In de operationalisering worden de in dit onderzoek gebruikte variabelen uiteengezet.

3.2 Onderzoeksmethode

Bij dit onderzoek is gekozen voor een large-n, toetsend onderzoek. Hiervoor is gekozen, omdat er al vele onderzoeken zijn op het gebied van informatiebeveiliging en handhaving van richtlijnen, maar door de grote aantallen verschillende onderzoeken is de consistentie uit het oog verloren. Daarnaast is de context een cruciaal onderdeel, waarbij niet zeker is of de uitkomsten van eerdere onderzoeken ook in de context van Nederlandse gemeenten gelden. Ook is dit onderzoek gericht op de medewerkers, die gebruik dienen te maken van het informatiebeveiligingsbeleid. Een experiment is in dit geval een goede oplossing, maar helaas is dit niet haalbaar in de situatie van dit onderzoek. Een surveyonderzoek is dus de meest haalbare en best passende methode, waarbij eerdere onderzoeken in een andere context zijn gebruikt bij het samenstellen van deze survey.

De survey, in dit geval een elektronische vragenlijst, is dus de hoofdmethode van dit onderzoek. Aan de hand van de literatuurreview is een aantal onafhankelijke variabelen gekozen, die volgens deze literatuur het meest een verband hebben met de afhankelijke variabele. Bij elk van deze variabelen is een hypothese opgesteld en die hypothesen zijn door middel van empirisch onderzoek, in de vorm van een survey getoetst. De keuze voor een survey is onder andere gemaakt door de grote hoeveelheid van onderzoekseenheden en de hoeveelheid gegevens die daarmee gepaard gaan. Een dergelijke grootschaligheid en hoge mate van standaardisatie van de verzameling van gegevens maakt deze onderzoeksmethodiek efficiënt en zorgt er tevens voor dat er sprake is van generaliseerbaarheid en hoge externe validiteit van dit onderzoek (Van Thiel, 2010). Daarom is ook vanuit praktisch oogpunt gekozen voor deze kwantitatieve onderzoeksmethode.

Wel moet worden benadrukt dat het uitvoeren van een surveyonderzoek een aantal nadelen met zich meebrengt. Door het gestandaardiseerde karakter van het onderzoek kan eventuele oppervlakkigheid van de verzamelde informatie optreden. Doordat het onderzoek een toetsend karakter heeft en geen verklarend karakter mist vaak de 'informatie achter de informatie' bij het verzamelen van de gegevens door middel van een survey. Ook kan de mogelijkheid zich voordoen dat bij het invullen van de vragen er door de respondenten niet altijd een eerlijk antwoord wordt gegeven of dat het antwoord voor de respondent niet volledig dekkend is (Van Thiel, 2010).

3.3 Respondenten

Er is in dit onderzoek gekozen voor grote en middelgrote gemeenten als respondenten. Hierbij is gekozen voor verspreiding van de respondenten over meerdere gemeenten, om de generaliseerbaarheid van dit onderzoek te verhogen en om zo de last voor de onderzochte organisaties te verminderen. Binnen deze gemeenten is gekozen voor beleidsmedewerkers als respondenten, omdat dit de mensen zijn die daadwerkelijk met de gegevens van burgers en bedrijven omgaan. De menselijke kant van informatiebeveiliging begint dus bij hen. Het is dan ook juist interessant als de respondent geen of weinig kennis heeft van informatiebeveiliging of ICT. Een belangrijk onderdeel is dat een respondent veel werkt via zijn of haar device. Iemand die niet of nauwelijks werkt met ICT, krijgt immers niet veel te maken met informatiebeveiliging. Echter, tegenwoordig werkt eigenlijk iedereen veel met de digitale werkplek.

In dit onderzoek worden medewerkers van het openbaar bestuur, in dit geval gemeenten, ondervraagd met behulp van een aantal stellingen en scenario's. Deze stellingen en scenario's zijn gebaseerd op 5 variabelen, waarbij een simplistisch model is opgesteld. De vereiste sample size van dit onderzoek is minimaal 150 respondenten. Vanvoorhis & Morgan (2007) benoemen dat er voor een onderzoek gericht op het onderzoeken van onderlinge relaties altijd minstens 50 respondenten dienen te zijn. Daarnaast wordt door hen geconstateerd dat het aantal respondenten bij een regressieanalyse minstens tien keer het aantal variabelen moet zijn. Toch wordt een analyse en daarmee een onderzoek sterker op het moment dat er minstens 30 respondenten zijn per gekozen variabele (Van Voris & Morgan, 2007). In dit onderzoek zijn er 5 variabelen, waardoor er een vereiste van minstens 150 respondenten is volgens de literatuur.

De respondenten zijn benaderd na contact en goedkeuring van de CEO van de gemeente. Uiteindelijk hebben zeven verschillende gemeenten de vragenlijst uitgezet bij hun werknemers. Deze dataverzameling vond tussen mei 2019 en juli 2019 plaats. Er is hierbij gebruik gemaakt van Qualtrics. Dit is een online enquête-tool, met een eenvoudige manier om de verkregen data te exporteren naar SPSS, het programma waarmee de analyse wordt uitgevoerd.

3.4 Operationalisering & constructie vragenlijst

De vragenlijst is geconstrueerd met behulp van de literatuurreview. Hierin zijn verschillende theorieën besproken, die vervolgens zijn gespecificeerd in variabelen. Voor deze variabelen zijn gekozen op basis van deze literatuur en eerdere onderzoeken naar de handhaving van richtlijnen van informatiebeveiliging.

De vragenlijst is zo geconstrueerd dat de verschillende variabelen eerst worden onderzocht aan de hand van een aantal stellingen. De respondent wordt per stelling gevraagd naar zijn of haar positie ten opzichte van deze stelling. Hierbij is gekozen om minimaal 3 stellingen per variabele op te nemen, zodat de concepten goed geanalyseerd kunnen worden. Immers, mocht een stelling niet aansluiten dan kan deze alsnog weggelaten worden. Daarnaast is gekozen voor een 5-punts Likert-schaal. Hierbij lopen de antwoorden van ‘zeer oneens’ tot ‘zeer eens’, waarbij ook een mogelijkheid is om neutraal te kiezen. Deze manier van ondervragen is gebaseerd op andere, soortgelijke onderzoeken, zoals Moody, Siponen & Pahnila (2018) en Siponen & Vance (2010). Die ook de 5-punts Likert-schaal gebruikt hebben. Na de stellingen worden drie situatieschetsen, oftewel vignetten, uiteengezet. Deze bestaan uit vijf stellingen per vignet, waarbij de afhankelijke variabelen en het realisme van de situatieschets worden gemeten. Ook hier is gebruik gemaakt van de 5-punts Likert-schaal. Deze vignettescenario’s zijn gebaseerd op eerdere onderzoeken op het gebied van compliance, zoals Moody, Siponen & Pahnila (2018) en Siponen & Vance, 2010. Hierbij is gekozen voor de naam Marijn, die door zowel mannen als vrouwen kan worden gedragen.

Tot slot zijn er enkele items in de vragenlijst opgenomen die de controlevariabelen van dit onderzoek vormen. De controlevariabelen zijn in dit onderzoek geslacht, geboortejaar, opleidingsniveau en percentage van de tijd dat de respondent achter het computerscherm werkt. Hieronder zijn de verschillende stellingen (items) per variabele te zien.

3.5 Variabelen

Bewustzijn is gemeten aan de hand van vijf items. Bulgurcu *et al.* (2010). Deze items zijn geformuleerd als volgt:

Bewustzijn	**Item**
BWZ1	Ik begrijp de bezorgdheid over informatiebeveiliging en de risico's die ze in het algemeen vormen.
BWZ2	Ik ben me bewust van de mogelijke risico's die er zijn als ik mij niet aan het informatiebeveiligingsbeleid houd.
BWZ3	Mijn collega's zijn op de hoogte van het informatiebeveiligingsbeleid van mijn werkgever.
BWZ4	Ik heb een cursus gevolgd op het gebied van informatiebeveiliging.
BWZ5	Ik ken mijn verantwoordelijkheden zoals voorgeschreven in het informatiebeveiligingsbeleid om de informatiebeveiliging van mijn organisatie te verbeteren.

Tabel 7: Vragenlijst Bewustzijn

Ook de tweede variabele, sancties, is gemeten met behulp van vijf items. Bulgurcu *et al.* (2010). De items zijn als volgt:

Sancties	**Item**
SNC1	Ik zal waarschijnlijk worden gestraft als ik niet voldoe aan de vereisten van het informatiebeveiligingsbeleid.
SNC2	Ik moet consequenties ondergaan als ik niet voldoe aan de vereisten van de informatiebeveiligingsbeleid.
SNC3	Ik zal monetaire of niet-geldelijke boetes oplopen als ik niet voldoe aan de vereisten van het informatiebeveiligingsbeleid.
SNC4	Opgelegde sancties houden verband met of ik voldoe aan de vereisten van de informatiebeveiligingsbeleid.
SNC5	Als ik mij niet houd aan de richtlijnen voor informatiebeveiliging, heeft dat consequenties.

Tabel 8: Vragenlijst Sancties

Social influence is aanvankelijk gemeten met behulp van vier items, waarbij het vierde item niet consistent genoeg was en dus is weggelaten uit dit onderzoek. De items zijn samengesteld aan de hand van Moody et al, (2018). Dit zijn de items:

Social Influence	**Item**
SIN1	Directe collega's vinden dat ik me aan het informatiebeveiligingsbeleid moet houden.
SIN2	Mensen die mijn gedrag beïnvloeden, vinden dat ik me aan het informatiebeveiligingsbeleid moet houden.
SIN3	Mijn leidinggevende vindt dat ik me aan het informatiebeveiligingsbeleid moet houden.

Tabel 9: Vragenlijst Social Influence

De vierde variabele, consideration, telt vier items. Voor deze variabele en de bijbehorende items is het onderzoek van Bass (1990) de basis.

Consideration	**Item**
CSR1	Mijn leidinggevende besteedt aandacht aan iedereen afzonderlijk.
CSR2	Mijn leidinggevende bevestigt mijn sterke punten.
CSR3	Mijn leidinggevende helpt me om mijn competenties te ontwikkelen.
CSR4	Mijn leidinggevende maakt een onderscheid tussen zijn werknemers.

Tabel 10: Vragenlijst Consideration

Risicoaversie is de vijfde en laatste variabele, die wordt gemeten aan de hand van vijf items. Deze items zijn gebaseerd op de onzekerheidsvermijdingsschaal, ontwikkeld door Hofstede en aangepast door (Sharma, 2010).

Risicoaversie	**Item**
RAV1	Ik ben zelden de eerste persoon die iets nieuws probeert.
RAV2	Ik zou mezelf niet omschrijven als iemand die graag risico's neemt.
RAV3	Ik geef de voorkeur aan een routinematige manier van leven ten faveure van een onvoorspelbaar leven vol verandering.
RAV4	Ik volg protocollen en beleid strikt en neem niet graag risico's.

Tabel 11: Vragenlijst Risicoaversie

3.6 Vignetten

Vignetten zijn scenarioschetsen; korte verhalen met een fictief personage in bepaalde omstandigheden. Een vignette geeft meer context en informatie, zodat de respondent de situatie beter kan inschatten. Hierbij moet niet zodanig veel informatie gegeven worden dat het antwoord van de respondent in een bepaalde richting wordt gestuurd (Braun & Clarke, 2013). Dit is een gevaar bij het gebruik van vignetten. De scenario's moeten voor de respondent duidelijk en herkenbaar zijn, maar er mag geen sprake zijn van een sturende vraag. Op het moment dat een respondent het scenario niet snapt of het niet realistisch vindt, kunnen de vragen verkeerd worden geïnterpreteerd en kunnen de antwoorden niet verklaren wat ze lijken te verklaren. Om dit te voorkomen is er vooraf overlegd met een aantal mensen uit het werkveld. Met behulp van hun kennis en ervaring zijn drie scenario's uitgekozen om in dit onderzoek te gebruiken.

Voordelen van het gebruik van vignetten is het tegengaan van sociaalwenselijke antwoorden. Deze methode kan een moreel of praktisch dilemma aankaarten, zonder dat dit als bedreigend wordt ervaren door de respondenten (Braun & Clarke, 2013). Het fictieve personage zorgt ervoor dat respondenten zich minder aangevallen zullen voelen. Zij denken in deze situatie namelijk niet dat dit over henzelf gaat, waardoor men eerlijker zal antwoorden. De respondent kan zich juist verplaatsen in het fictief personage. Hierdoor is de vignettensurvey een goede methode bij een onderzoek naar gevoelige onderwerpen, zoals informatiebeveiliging. Een ander voordeel is dat er meer controle voor de onderzoeker, aangezien de vraag in een bepaalde context en situatie wordt gesteld. Deze vignetten zijn gebaseerd op eerder onderzoek op het gebied van compliance door Moody, Siponen en Pahnila (2018).

Vignette 1:

Marijn heeft net gevoelige klantgegevens voor zijn werkgever verzameld en hij wil die gegevens mee naar huis nemen om zijn werk voort te zetten. Hij weet dat zijn werkgever vereist dat hij een wachtwoord aanvraagt dat wordt uitgegeven en wordt toegepast op alle gegevens voordat het op een USB-station het kantoor verlaat, zodat het niet kan worden bezocht door een onbevoegde persoon. Marijn heeft de procedure voor het aanvragen van een wachtwoord eerder voltooid, dus hij is ervan overtuigd dat hij het gemakkelijk opnieuw kan doen. Marijn gelooft dat het zonder het wachtwoord waarschijnlijk is dat ongeautoriseerde mensen de gegevens zullen zien, maar als ze dat doen, gebeurt er niets slechts.

Marijn is van mening dat de wachtwoordprocedure niet effectief is en niet voorkomt dat onbevoegde personen de gegevens kunnen zien. Hoe dan ook, de wachtwoordprocedure duurt enkele minuten en hij moet nu vertrekken, dus hij slaat de procedure over. Marijn gelooft dat zijn kansen om gepakt te worden laag zijn, maar als hij wordt betrapt, zouden de consequenties minimaal zijn.

De variabele handhaving bestaat uit drie items bij deze vignette, gebaseerd op Moody et al. (2018). Daarnaast is getoetst of het scenario realistisch is volgens de respondenten, met behulp van twee items.

HHV1.1	Ik zou in deze situatie hetzelfde handelen als Marijn.
RSC1.1	Het bovenstaande scenario is realistisch.
HHV2.1	Als ik Marijn was, had ik de procedure ook overgeslagen.
RSC2.1	Ik kan me voorstellen dat een soortgelijk scenario op mijn werk plaatsvindt.
HHV3.1	Ik denk dat ik zou doen wat Marijn deed als mij dit overkwam

Tabel 12: Vragenlijst Vignette 1

Vignette 2:

Marijn is aan het werk op zijn digitale werkplek. Tijdens het werk wordt hij gevraagd om even mee te kijken met een collega. Marijn accepteert dit en loopt met de collega mee. Hij verlaat zijn digitale werkplek, zonder deze te vergrendelen. Vervolgens ontstaat een discussie over de werkzaamheden, die langer duurt dan Marijn vooraf inschatte. De digitale werkplek van Marijn blijft hierdoor een tiental minuten onbewaakt en ontgrendeld. Als Marijn terugkomt bij zijn werkplek ziet hij dat deze nog steeds ontgrendeld is en hij bedenkt zich dat hij een fout heeft gemaakt door deze niet te vergrendelen bij het verlaten van zijn werkplek. Hij gelooft dat zijn kansen om hiermee geconfronteerd te worden erg laag zijn en eventuele consequenties ook minimaal zullen zijn.

Ook bij vignette 2 is de variabele handhaving getest met drie items. Het realisme van het scenario is getoetst met dezelfde twee items als bij vignette 1.

HHV1.2	Ik zou in deze situatie hetzelfde handelen als Marijn.
RSC1.2	Het bovenstaande scenario is realistisch.
HHV2.2	Als ik Marijn was, had ik de digitale werkplek ook niet vergrendeld.
RSC2.2	Ik kan me voorstellen dat een soortgelijk scenario op mijn werk plaatsvindt.
HHV3.2	Ik denk dat ik zou doen wat Marijn deed als mij dit overkwam

Tabel 13: Vragenlijst Vignette 2

Vignette 3:

Marijn heeft zojuist belangrijke informatie over een project verzameld en opgeslagen op een USB-stick. Eenmaal aangekomen op zijn werkplek wil hij de informatie overzetten naar zijn digitale werkplek, maar er komt iets tussen. Een collega vraagt om hulp en Marijn wil graag meedenken met deze collega. Hij laat de USB-stick achter op zijn bureau, om deze later te verwerken. Tijdens het gesprek met de collega verliest Marijn de tijd uit het oog en gaat hij door naar de volgende afspraak. De USB-stick ligt nog steeds op het bureau, maar dit kan volgens Marijn geen kwaad. Hij verwacht dat hij niet gepakt zal worden en dat de eventuele consequenties minimaal zullen zijn.

Handhaving is ook bij de derde vignette getoetst met behulp van drie items, wederom gebaseerd op Moody et al. (2018). Het realisme van het scenario is wederom getoetst met dezelfde twee items als bij de andere vignetten.

HHV1.3	Ik zou in deze situatie hetzelfde handelen als Marijn.
RSC1.3	Het bovenstaande scenario is realistisch.
HHV2.3	Als ik Marijn was, had ik de USB-stick ook laten liggen.
RSC2.3	Ik kan me voorstellen dat een soortgelijk scenario op mijn werk plaatsvindt.
HHV3.3	Ik denk dat ik zou doen wat Marijn deed als mij dit overkwam

Tabel 14: Vragenlijst Vignette 3

3.7 Analysemethode

De analyse van dit onderzoek wordt gedaan met behulp van het statistiekprogramma SPSS. Hierbij wordt de data geanalyseerd op verschillende manieren. De data, afkomstig uit Qualtrics, moet eerst worden opgeschoond om de juiste data te gebruiken bij de analyses. Hierbij moeten verschillende keuzes worden gemaakt. De opschoning van de data is de eerste stap van de analyse. Hierbij is het belangrijk om actie te ondernemen bij missing values. Er kwamen meerdere missing values voor bij de opgehaalde data. Zo werd een aantal keer '1900' ingevuld bij geboortejaar, werd bij geslacht 'neutraal' als antwoord gegeven en werden sommige vragenlijsten niet afgemaakt. Ik heb ervoor gekozen om alle rijen data met missing values te verwijderen om zo de data op te schonen.

Vanwege de aard van dit onderzoek, large-n en toetsend, is gekozen voor een multiple lineaire regressieanalyse. Vanwege het feit dat er in dit onderzoek één afhankelijke variabele en meerdere onafhankelijke variabelen zijn, is er gekozen voor deze analysemethode. Alle items voor alle variabelen zijn geaggregeerd tot een schaal per variabele, waarbij de Cronbach Alpha minstens 0.7 dient te zijn als controle voor de interne consistentie. Vervolgens is de beschrijvende statistiek getoetst, om inzicht te krijgen in de data. Het realisme van de drie scenario's zijn in een tabel weergegeven, met wederom een Cronbach Alpha van 0.7. Vervolgens zijn ook de beschrijvende statistiek van alle variabelen, inclusief de controlevariabelen leeftijd en geslacht, berekend en in een tabel weergegeven. Naast de beschrijvende statistiek is ook de onderlinge correlatie tussen de variabelen berekend.

Na het voltooien van deze stappen, werden de modelassumpties voor de lineaire regressieanalyse gecheckt. Om deze analyse uit te kunnen voeren, moest voldaan worden aan vier modelassumpties, te zien in tabel 15. De uitwerking van deze modelassumpties wordt gedaan in hoofdstuk 4: resultaten.

Modelassumptie 1	De relaties tussen de onafhankelijke variabelen en de afhankelijke variabele zijn lineair
Modelassumptie 2	Er is geen sprake van multicollineariteit tussen de onafhankelijke variabelen
Modelassumptie 3	De standaardfout geproduceerd door het model is normaal verdeeld
Modelassumptie 4	Er is homoskedasticiteit in het model (geen "fanning out" van standaardfout)

Tabel 15: Modelassumpties van de lineaire regressieanalyse

4. Resultaten

4.1 Inleiding

In dit hoofdstuk worden de resultaten van het onderzoek getoond en onderbouwd. De uit de survey verkregen data zijn opgeschoond en getoetst. Vervolgens is er met behulp van de een regressieanalyse onderzocht welke verbanden kunnen worden aangetoond op basis van significantie. Het hoofdstuk bestaat allereerst uit de beschrijvende statistieken van de data. Vervolgens worden de criteria voor de regressieanalyse besproken. Ook worden de resultaten van de regressieanalyse uiteengezet. Ten slotte wordt in dit hoofdstuk antwoord gegeven op de tweede deelvraag van dit onderzoek: Welke uitspraken kunnen worden gedaan na confrontatie van die hypothesen met data uit de survey onder beleidsmedewerkers van Nederlandse gemeenten?

4.2 Beschrijvende statistiek

Om een inzicht te krijgen in de losse variabelen van dit onderzoek, worden de beschrijvende statistieken weergegeven in tabel 16 en tabel 17. In tabel 16 zijn de Cronbach's Alpha, het gemiddelde, de standaardafwijking en de minimale en maximale scores van de drie verschillende vignettenscenario's weergegeven. Hierbij gaat het over hoe realistisch het scenario is volgens de respondenten.

De Cronbach's Alpha van elk van de drie scenario's ligt rond de 0.7, waardoor de samenhang tussen de verschillende items voor deze variabelen kan worden geconstateerd. Het gemiddelde van vignette 2 ligt hierbij iets lager dan van de andere scenario's. Dit kan komen doordat respondenten zich niet in dit scenario kunnen verplaatsen. De scores bij elke van de drie scenario's worden als hoog genoeg ervaren om de hypotheses verder te kunnen testen.

	Cronbach 's Alpha (# Items)	***Mean (SD)***	***Min.***	***Max.***
Vignette 1	0.677 (2)	2.44 (0.79)	1.00	5.00
Vignette 2	0.746 (2)	1.87 (0.77)	1.00	4.50
Vignette 3	0.720 (2)	2.13 (0.78)	1.00	5.00

Tabel 16: Consistentie en beschrijvinsstatistiek van de score op realisme

Tabel 17 toont de Cronbach's Alpha, het gemiddelde en de minimale en maximale scores van alle variabelen. Hierbij zijn leeftijd en geslacht de controlevariabelen die bestaan uit één vraag, waardoor hier geen Cronbach's Alpha te berekenen is. Cronbach's Alpha van de variabelen dient minimaal 0.7 te zijn, welke aangeeft dat de verschillende items per variabelen intern consistent zijn. De variabele social influence is niet meegenomen in de verdere analyse, omdat de interne consistentie niet gewaarborgd is. De Cronbach's Alpha was bij deze variabele 0.562, waardoor de schaal niet geconstrueerd kon worden. Hierbij is geprobeerd om items één voor één weg te laten bij het construeren van de schaal, maar de Cronbach's Alpha bleef onder de 0.7. De variabele social influence viel dus helaas niet meer te redden. In het geval van consideration is er gekozen om wel een schaal te creëren, gezien het kleine verschil tussen deze Cronbach's Alpha (0.693) en de vereiste 0.7.

Aan het einde van de tabel zijn ook de correlaties tussen de variabelen te vinden, uitgedrukt in VIF-score. Deze geeft aan of er een verband is tussen de verschillende onafhankelijk variabelen. De VIf-score dient lager te zijn dan 5 om multicollineariteit uit te sluiten. Het ontbreken van multicollineariteit is een van de vereisten om de regressieanalyse uit te kunnen voeren. Hier wordt in de volgende alinea verder op ingegaan.

	Cronbach's Alpha (# Items)	*Mean (SD)*	*Min.*	*Max.*	*Bewust-zijn*	*Sancties*	*Con-sideration*	*Risico-aversie*	*VIF-score*
Geslacht	-	1.42 (0.47)	1.00	2.00					
Leeftijd	-	44.68 (11.23)	25.00	65.00					
Bewustzijn	0.766 (5)	3.48 (0.70)	2.00	5.00	1				1.079
Sancties	0.789 (5)	3.15 (0.67)	1.20	5.00	0.265**	1			1.194
Consideration	0.693 (3)	3.67 (0.70)	2.00	5.00	0.140	0.321**	1		1.121
Risicoaversie	0.736 (4)	2.93 (0.70)	1.75	4.75	0.029	0.133	0.082	1	1.020
Handhaving Wachtwoord	0.871 (3)	3.87 (0.83)	1.67	5.00					
Handhaving Werkplek	0.847 (3)	3.48 (1.01)	1.00	5.00					
Handhaving USB-stick	0.877 (3)	3.73 (0.95)	1.00	5.00					

Tabel 17: Beschrijvende statistiek variabelen, correlaties tussen variabelen (= significant bij 0.05, ** significant bij 0.01, *** significant bij 0.001) en VIF-waarde per variabele.*

4.3 Modelassumpties regressieanalyse

Voordat de regressieanalyse uitgevoerd kan worden en voordat het model opgesteld wordt, dient voldaan te worden aan de modelassumpties. Deze modelassumpties bestaan uit vier criteria. Het eerste criterium houdt in dat de relaties tussen onafhankelijke variabelen en de afhankelijke variabele lineair zijn. Een lineair verband houdt in dat de invloed voor zowel de hoge als de lage waarden van de verklarende variabele gelijk is. Dit criterium kan getest worden met behulp van de scatterplots. In de scatterplots moet een rechte lijn door de puntenwolk kunnen worden getrokken. Als dit het geval is, is er sprake van een lineair verband. De scatterplots zijn toegevoegd in bijlage 2. Hier is te zien dat er in dit onderzoek sprake is van lineaire verbanden.

Het tweede criterium richt zich op multicollineariteit. Multicollineariteit houdt in dat er een lineair verband is tussen de onafhankelijke variabelen. Dit kan ervoor zorgen dat de verkregen data uit de regressieanalyse verkeerd wordt geïnterpreteerd. Bij multicollineariteit voorspellen de verklarende variabelen elkaar in plaats van de afhankelijke variabele, terwijl dit het verband is dat wordt onderzocht. Er dient dus geen multicollineariteit te zijn. Dit kan getest worden met behulp van de VIF-waarde, een score die met behulp van SPSS berekend kan worden. De VIF-scores van alle onafhankelijke variabelen is toegevoegd in tabel 17. Hierbij is te zien dat deze scores niet hoger zijn dan 1.121. Als de VIF-score onder de 5 is, is er geen sprake van multicollineariteit. Ook aan het tweede criterium wordt in dit onderzoek voldaan.

Het derde criterium is dat de standaardfout geproduceerd door het model normaal verdeeld is. Via SPSS kan de normaalverdeling worden aangegeven met behulp van een Q-Q-plot. In dit onderzoek is er sprake van een normaalverdeling, waardoor ook aan het derde criterium voldaan wordt.

Het vierde en laatste criterium is dat er geen sprake is van homoscedaticiteit. Homoscedaticiteit houdt in dat de variantie van een variabele gelijk is voor meerdere groepen of dat de variantie van de foutterm gelijk is. Bij regressie moet de variantie van de foutterm gelijk zijn voor alle waarden van de verklarende variabele. Er mag dus niet meer of minder spreiding in de foutterm zijn voor grotere of lagere waarden van de verklarende variabele. Dit wordt ook wel “fanning out” genoemd en kan gecontroleerd worden met behulp van scatterplots. Bij heteroscedaticiteit is de significantie onbetrouwbaar, waardoor het mogelijk is dat de onderzoeker de verkeerde conclusie trekt op basis van de uitkomsten. De scatterplots, bijgevoegd in bijlage 2, laten geen homoscedaticiteit zien.

Ook aan de laatste modelassumptie wordt voldaan, waardoor de regressieanalyse kan worden uitgevoerd en het model kan worden opgesteld.

4.4 Regressieanalyse

De uitvoering van de regressieanalyse is gedaan door middel van het bouwen van een model, waarvan de uitkomsten te zien zijn in tabel 18. In dit model is per scenario twee keer een regressieanalyse uitgevoerd, waarbij de eerste keer enkel de controlevariabelen zijn meegenomen en de tweede keer alle variabelen worden getoetst. De Beta's en significantielevels zijn voor elke variabele weergegeven in tabel 18.

	Vignette 1		**Vignette 2**		**Vignette 3**	
	Model 1	**Model 2**	**Model 1**	**Model 2**	**Model 1**	**Model 2**
Leeftijd	.065	.045	-.111	-.115	.067	.041
Geslacht	-.089	-.060	-.072	-.046	-.083	-.056
Bewustzijn		.198*		.246**		.141
Sancties		.167		.055		.154
Leiderschap		.115		.060		.081
Risicoaversie		.077		.007		.124
R^2	.013	.140	.017	.097	.012	.107

Tabel 18: Regressie resultaten (= significant bij 0,05; ** significant bij 0,01; *** significant bij 0,001)*

4.5 Tussenconclusie

De resultaten van de regressieanalyse, zoals weergegeven in tabel 19, laten zien dat de verondersteld invloed van bewustzijn op handhaving in vignette 1 en vignette 2 wordt ondersteund, maar in vignette 3 niet. Alle andere variabelen zijn niet significant bevonden, waardoor de bijbehorende hypothesen worden verworpen.

Hypothese	Handhaving Wachtwoord	Handhaving Werkplek	Handhaving USB-Stick
Naarmate er meer sprake is van informatiebeveiligingsbewustzijn, zal er meer handhaving van richtlijnen van informatieveiligheidsbeleid door medewerker van Nederlandse gemeenten zijn.	Aangenomen	Aangenomen	Verworpen
Naarmate er meer sancties in de organisatie zijn voor overtredingen op het gebied van informatiebeveiliging, zal er meer handhaving van richtlijnen van informatieveiligheidsbeleid plaatsvinden.	Verworpen	Verworpen	Verworpen
Naarmate er meer sprake is van coachend leiderschap (consideration), zal er meer handhaving van richtlijnen van informatieveiligheidsbeleid door medewerker van Nederlandse gemeenten zijn.	Verworpen	Verworpen	Verworpen
Naarmate er meer sprake is van risicoaversie op het gebied van informatiebeveiliging, zal er meer handhaving van richtlijnen van informatieveiligheidsbeleid door medewerker van Nederlandse gemeenten zijn.	Verworpen	Verworpen	Verworpen

Tabel 19: Resultaten van de toetsing van de hypothesen.

4.6 Resultaten versus theorie

De resultaten laten zien dat bewustzijn invloed heeft op de handhaving van voorschriften op het gebied van informatiebeveiliging bij Nederlandse gemeenten, maar dat de andere variabelen geen significant verband laten zien. Dit is ontzettend interessant, aangezien op basis van andere onderzoeken verwacht werd dat de meeste variabelen verbanden tussen de variabelen en handhaving van voorschriften op het gebied van informatiebeveiliging zouden laten zien.

Bewustzijn wordt in veel onderzoeken over informatiebeveiliging genoemd als belangrijk onderwerp. Bulgurcu et al. (2010), Siponen (2000), D'Arcy (2009) en De Bruijn & Janssen (2017) geven allen aan dat het belang van bewustzijn voorop staat als het gaat om informatiebeveiliging. De Theory of Planned Behaviour (Ajzen & Sheikh, 2013) geeft aan dat mensen hun gedrag baseren

Sancties zijn hebben volgens de resultaten van dit onderzoek geen significante relatie tot de naleving van informatiebeveiliging. Vance & Siponen (2012) gaven in hun onderoek ook al aan dat formele straffen niet per se afschrikkend zijn, tenzij iedereen weet dat de straffen er zijn en dat er actief wordt gecontroleerd op naleving van de voorschriften. Voorbeelden van mensen die gepakt zijn en daarvoor bestraft worden, zorgen ervoor dat werknemers zich meer bewust worden van het feit dat ze strafbaar bezig zijn als zij de voorschriften op het gebied van informatiebeveiliging niet naleven. (Siponen & Vance, 2012)

Leiderschap is volgens dit onderzoek minder van invloed op de naleving van informatieveiligheidsbeleid dan verwacht. Eerdere onderzoeken geven een significant verband aan, maar in deze context blijkt dit niet zo te zijn. Wel is leiderschap van belang om het bewustzijn te vergroten en een omgeving te creëren waarin naleving op het gebied van informatiebeveiliging als normaal wordt gezien. Hierbij is ook het concept Social Influence betrokken. Ondanks het feit dat deze variabele niet is meegenomen in dit onderzoek, heeft ook Social Influence invloed op het bewustzijn van medewerkers op het gebied van informatiebeveiliging.

5. Conclusie en discussie

5.1 Inleiding

Het laatste hoofdstuk van dit onderzoek bestaat uit de conclusies in de vorm van de beantwoording van de deelvragen en de hoofdvraag. Onder het kopje discussie wordt daarnaast gereflecteerd op de gemaakte keuzes in dit onderzoek, de implicatie van de praktijk en op de wetenschappelijke theorie rondom het onderwerp van het onderzoek. Tot slot wordt ook gereflecteerd op mijn eigen rol als onderzoeker, waarbij mijn mening over het gehele proces wordt uiteengezet.

5.2 Beantwoording deelvragen en hoofdvraag

In dit onderzoek is gezocht naar een antwoord op de vraag: '*Hoe kan de naleving van voorschriften op het gebied van informatieveiligheid door beleidsmedewerkers van Nederlandse gemeenten worden verklaard en welke factoren spelen hierbij een rol?*' Hiervoor is een kwantitatief onderzoek uitgevoerd naar informatiebeveiligingsbeleid.

De hoofdvraag van het onderzoek kan beantwoord worden met behulp van de twee deelvragen. De eerste deelvraag: 'Welke hypothesen met betrekking tot informatieveiligheidsvoorschriften kunnen uit de literatuur worden afgeleid?' Er zijn in dit onderzoek vijf hypothesen opgesteld; één hypothese per variabele. De hypothesen zijn als volgt: H1: Naarmate er meer sprake is van informatiebeveiligingsbewustzijn, zal er meer handhaving van richtlijnen van informatieveiligheidsbeleid door medewerker van Nederlandse gemeenten zijn. H2: Naarmate er meer sancties in de organisatie zijn voor overtredingen op het gebied van informatiebeveiliging, zal er meer handhaving van richtlijnen van informatieveiligheidsbeleid plaatsvinden. H3: Naarmate er meer sprake is van social influence, zal er meer handhaving van richtlijnen van informatieveiligheidsbeleid door medewerker van Nederlandse gemeenten zijn. H4: Naarmate er meer sprake is van coachend leiderschap, zal er meer handhaving van richtlijnen van informatieveiligheidsbeleid door medewerker van Nederlandse gemeenten zijn. H5: Naarmate er meer sprake is van risicoaversie op het gebied van informatiebeveiliging, zal er meer handhaving van richtlijnen van informatieveiligheidsbeleid door medewerker van Nederlandse gemeenten zijn.

De tweede deelvraag van dit onderzoek is als volgt: ‘Welke uitspraken kunnen worden gedaan na confrontatie van die hypothesen met data uit de survey onder beleidsmedewerkers van Nederlandse gemeenten?’ Met behulp van de statistische analyse kunnen er uitspraken gedaan worden over de naleving van richtlijnen op het gebied van informatiebeveiliging door beleidsmedewerkers van Nederlandse gemeenten. De regressieanalyse heeft aangetoond dat er geen significant verband is tussen sancties en naleving. Hypothese 2 kan dus worden verworpen. Er is ook geen significant verband aangetroffen tussen leiderschap en naleving, waardoor hypothese 4 ook verworpen kan worden. Daarnaast kan hypothese 5 eveneens worden verworpen, aangezien er in dit onderzoek geen significant verband is tussen risicoaversie en naleving.

De onderzoeksvragen die in dit artikel aan de orde kwamen, waren welke factoren van invloed zijn op de naleving van het informatiebeveiligingsbeleid in Nederlandse gemeenten. Empirisch bewijs dat is verzameld door middel van een vignetonderzoek naar de antwoorden van gemeentelijke overheidsmedewerkers, wijst erop dat er weinig steun is voor de hypothesen die in deel twee worden gepresenteerd; in twee van de drie vignetten is er steun voor het idee dat bewustzijn de naleving beïnvloedt. Het is duidelijk dat percepties van sancties, managementstijl en risicoaversie geen significante impact hebben op de naleving van het informatiebeveiligingsbeleid en de richtlijnen. De enige hypothese die dus kan worden aangenomen is hypothese 1, wat betekent dat er in dit onderzoek een verband is tussen het bewustzijn van medewerkers en de naleving van richtlijnen op het gebied van informatieveiligheid.

5.3 Aanbevelingen

Uit de resultaten van dit onderzoek blijkt dat sancties, leiderschap en risicoaversie geen directe invloed hebben op de naleving van voorschriften op het gebied van informatiebeveiliging door medewerkers. Op die gebieden heb ik dan ook geen aanbevelingen, aangezien er geen significante verbanden zijn gevonden. Aan gemeenten en andere belanghebbenden zou ik dan ook graag willen meegeven dat men specifiek moet werken aan het creëren bewustzijn bij de medewerkers. Zorg ervoor dat de mensen zich ervan bewust worden wat voor risico een organisatie loopt bij een eventueel datalek of als het systeem wordt gehackt. Een organisatiesfeer waarbij het normaal is om veilig om te gaan met internet en informatie en dus de veiligheidsrichtlijnen na te leven, is hierbij een vereiste. De organisatietop en managers zijn hierbij van belang, omdat zij deze organisatiesfeer kunnen creëren. Educatie en training spelen kunnen hier een grote rol bij spelen. Betrek de

medewerker hierbij en laat men actief meedenken over hoe een organisatie beter bewust kan worden van en de veiligheidsvoorschriften beter kan naleven.

Zoals eerder in dit onderzoek aangegeven, benadrukken andere studies ook het belang van educatie en training om het bewustzijn te verhogen. Met name D'Arcy et al. (2009), Furnell et al. (2002) en Hentea (2005) benoemen dit specifiek. D'Arcy et al. (2009) noemen hierbij SETA-programma's. De basis van een SETA-programma is het informatieveiligheidsbeleid. Het programma biedt vervolgens de mogelijkheid om werknemers bewust te maken van hun verantwoordelijkheden met betrekking tot verkregen informatie en de veiligheid daarvan, om kennis over informatierisico's in de organisatie over te brengen en om recente acties tegen werknemers te benadrukken wegens schendingen van het beveiligingsbeleid (D'Arcy et al., 2009).

Binnen de gemeentelijke organisatie is de CISO de persoon die de leiding moet nemen op het gebied van informatieveiligheid. Deze persoon is verantwoordelijk voor alles wat er gebeurt rondom informatieveiligheid en deze persoon is dan ook degene die ervoor moet zorgen dat de informatieveiligheid toeneemt binnen de organisatie. Mijn advies is om twee momenten in het jaar te wijden aan het onderwerp informatieveiligheid. Bied hierbij een bewustzijnscursus aan of organiseer een dag in het teken van informatieveiligheidsbewustzijn. Daarnaast is mijn advies om nieuwe werknemers direct bij binnenkomst een cursus of andere educatievorm te laten doen, zodat zij direct op de hoogte zijn van de voorschriften en bewuster zullen omgaan met informatieveiligheid.

5.4 Discussie

Tijdens dit onderzoek zijn er veel keuzes gemaakt. De gekozen variabelen, de onderzoeksmethode, de respondenten, de vignetten, de operationalisering van de variabelen. Al deze keuzes hebben hun onderbouwing. Echter kan elke keuze anders uitgelegd worden. De variabelen van dit onderzoek (bewustzijn, sancties, social influence, leiderschap en risicoaversie) zijn gekozen op basis van theoretische invalshoeken en eerdere onderzoeken. Echter is bekend dat er meer factoren en variabelen van invloed zijn op de naleving van informatieveiligheidsbeleid dan de vijf gekozen variabelen. De lage R^2 in dit onderzoek laat bijvoorbeeld zien dat de gekozen variabelen slechts voor een deel de voorspellers zijn voor de naleving van informatieveiligheidsvoorschriften; er zijn nog ontzettend veel andere variabelen die ook invloed hebben op de naleving. Dit laat zien dat de gekozen variabelen niet per se de juiste zijn of dat er meer variabelen meegenomen hadden moeten worden. Hierdoor kunnen de resultaten afwijken van eerdere onderzoeken.

Daarnaast is er in dit onderzoek gekozen voor een bepaalde groep respondenten, namelijk beleidsmedewerkers bij gemeenten. De keuze voor deze respondenten is anders dan in de eerdere onderzoeken naar naleving van informatieveiligheidsbeleid. Zo koos Moody et al. (2018) voor ICT-personeel, terwijl in dit onderzoek algemene beleidsmedewerkers worden ondervraagd. Dit kan wederom zorgen voor een verschil in resultaten.

Een derde discussiepunt in dit onderzoek is de herkenbaarheid van de vignetten. De realismescores, berekend via SPSS zijn onder de 3. Dit is een relatief lage score, die kan verklaren dat de respondenten zich niet goed genoeg herkennen in de beschreven situaties van de vignetten. Dit kan leiden tot andere resultaten dan vooraf verwacht.

Het vierde en laatste discussiepunt richt zich op de operationalisering. Hier zijn wederom vele keuzes gemaakt, met name over het aantal items per variabele en over hoe deze items moeten worden geformuleerd. De keuze is hierbij gevallen op het hergebruiken van items uit eerdere onderzoeken, waarbij bij met name leiderschap en risicoaversie geen link is gemaakt met informatieveiligheidsbeleid. Daarnaast de variabele leiderschap vrij simplistisch gemeten met behulp van vier items. In sommige andere onderzoeken wordt de variabele leiderschap gemeten met behulp van meer dan veertig items. Het ontbreken van de link met het onderwerp naleving van informatieveiligheidsbeleid en de simplistische meting van leiderschap en risicoaversie kan ervoor zorgen dat respondenten andere antwoorden geven. Dit kan er vervolgens voor zorgen dat er andere resultaten uitkomen dan verwacht en dan in eerdere onderzoeken over dit onderwerp.

5.5 Suggesties voor vervolgonderzoek

In vervolgonderzoek kan gekeken worden naar andere variabelen in dezelfde context als dit onderzoek, waarbij er wellicht andere variabelen meer invloed hebben dan vooraf verwacht. Zo blijkt achteraf dat gekozen variabelen als social influence en leiderschap een sterk verband hebben met het bewustzijn van medewerkers.

De respondenten in dit onderzoek bestaat uit beleidsmedewerkers bij Nederlandse gemeenten. Over het algemeen zijn dit mensen die op kantoor werken in een veilige omgeving. De buitenpost, de mensen die er juist op uit trekken en buiten kantoor werken, zijn over het algemeen een grotere risicogroep. Deze mensen zijn in dit onderzoek niet meegenomen, terwijl echte veiligheidsrisico’s juist in deze groep vallen. In een vervolgonderzoek kan gekozen worden voor een andere doelgroep, zoals mensen in de buitendienst.

Een andere keuze in dit onderzoek is het gebruik van vignetten. Zoals eerder is uitgelegd vergroot een vignette de kans op een antwoord van een respondent op een gevoelig onderwerp, zonder dat sociaalwenselijke antwoorden worden gegeven. Echter is het gevaar dat een vignette niet herkenbaar genoeg is voor de respondent. De realismescores van de vignetten zijn in dit onderzoek aan de lage kant. Dit laat zien dat de respondent zich niet altijd kan verplaatsen in het scenario. Dit kan ertoe leiden dat een respondent een ander antwoord geeft, bijvoorbeeld een sociaalwenselijk antwoord. In eventueel vervolgonderzoek kunnen andere vignetten worden gekozen, waarin de respondent zich beter kan verplaatsen.

Een vierde en laatste suggestie voor vervolgonderzoek richt zich op de operationalisering van de variabelen in dit onderzoek. Er zijn veel keuze gemaakt over welke vragen gesteld moeten worden bij welke variabele. Hierbij zijn de items gebaseerd op eerder onderzoek, zoals Moody et al. (2018). Ook hier kunnen andere keuzes gemaakt worden, die kunnen zorgen voor andere antwoorden. Bijvoorbeeld door de context van informatiebeveiliging meer toe te passen, terwijl in dit onderzoek met name algemene vragen zijn gesteld over bijvoorbeeld risicoaversie en leiderschap.

5.6 Reflectie op eigen ervaringen

Als ik terugkijk naar het hele traject van deze scriptie, heb ik met name veel over mezelf geleerd. Het gehele traject heeft langer geduurd dan gebruikelijk door een avontuur in Amerika eind 2019 en een zware knieblessure begin 2020, maar uiteindelijk ben ik blij dat dit het resultaat is. Het belangrijkste wat ik heb geleerd, is dat het maken van keuzes cruciaal is bij het doen van wetenschappelijk onderzoek. Hierbij is het niet erg om een verkeerde keuze te maken, want dit maakt het juist interessant. De kennisopbrengst zit hem niet altijd in de aansluiting op eerdere onderzoeken of wetenschappelijke theorieën. De kennisopbrengst zit hem juist in het verwerpen van deze onderzoeken en in het aanbrengen van verschillende nuances. Tijdens mijn bachelor heb ik geleerd om vast te houden aan eerdere onderzoeken en wetenschappelijke theorieën, maar soms is het zelfs interessanter om dit niet te doen. Hierbij is het natuurlijk wel van belang dat de gemaakte keuzes worden onderbouwd.

Het doen van kwantitatief onderzoek is mij daarnaast redelijk tegen gevallen. Bepalen welke variabelen worden meegenomen, bepalen voor welke groep respondenten wordt gekozen, het verzamelen van de gegevens, het verwerken van de gegevens, het analyseren van de data. Al deze stappen kosten ontzettend veel tijd en moeite. Met name de gegevensverzameling is hierbij een lastige fase, aangezien je als onderzoeker eigenlijk alleen

kunt wachten tot er genoeg respondenten zijn. Dit is een moeilijke fase, waarin je eigenlijk meer kunt doen dan je denkt.

Tot slot de vignetten. Deze scenarioschetsen zijn moeilijker in gebruik dan vooraf verwacht. Met name het geringe gebruik in andere onderzoeken zorgt voor problemen, aangezien je goed moet uitleggen en verklaren waarom jij als onderzoeker de keuze maakt om dat in dit onderzoek juist wel te gebruiken. Daarnaast moeten de vignetten representatief en herkenbaar zijn, maar vooral niet te sturend. Dit is een balans die zeker in ogenschouw moet worden genomen. Ik heb hier wel veel van geleerd, aangezien een context een bepaalde nuance kan aanbrengen in een vraagstelling. Wel is het belangrijk om vooraf te weten waarom je deze keuze maakt.

Dit brengt mij bij een aantal tips voor studenten die aan hun scriptie gaan beginnen. De belangrijkste tip is eigenlijk dat alles mogelijk is, als er maar een goede onderbouwing voor is. Maak keuzes, leg uit waarom eerder onderzoek dit ook of juist niet heeft gedaan en blijf achter de keuze staan. Zoals ik al aangaf, is het wel belangrijk voor jezelf om te weten waar de kennisopbrengst zit. Dus een verworpen hypothese is ook een uitkomst, die het onderzoek vaak interessanter maakt dan een aangenomen hypothese.

Een tweede tip heeft te maken met de planning. Kies vooral je eigen tempo, waarbij het belangrijk is dat je niet stil komt te vallen. Op het moment dat de scriptie stil komt te staan, is het dubbel zo moeilijk om weer op te starten. Een voorbeeld hiervan is tijdens de gegevensverzameling. Zet op momenten dat de scriptie stilligt de volgende stappen alvast uit en houd actief contact met de persoon die de survey heeft uitgezet bij je respondenten. Hierdoor blijf je aansluiting houden en blijf je in de flow. Deze flow is voor mij cruciaal geweest. Het is belangrijk om leuke dingen te blijven doen naast je scriptie en om jezelf vooral niet de hele dag op te sluiten achter je laptop. Schrijf de scriptie stap voor stap, met elke dag maximaal 4 uur aan schrijfwerk. Dit heeft mij uiteindelijk gered. De laatste tip heeft te maken met de literatuurlijst. Ik heb deze niet vanaf het begin bijgehouden, waardoor ik uiteindelijk een dag mee bezig ben geweest met alleen het goed neerzetten van de literatuurlijst. Doe dit vanaf het begin en gebruik hierbij de citaatknop in Google Scholar. Zo staat de hele bron direct goed vermeld en dit scheelt uiteindelijk heel veel tijd.

Literatuurlijst

Ajzen, I., & Sheikh, S. (2013). Action versus inaction: Anticipated affect in the theory of planned behavior. *Journal of Applied Social Psychology*, *43*(1), 155-162.

Allen, N.J., & Meyer. J.P. (1996). "Affective, continuance, and normative commitment to the organization: An examination of construct validity." *Journal of vocational behavior* 49.3: 252-276.

Bass, B. M., & Avolio, B. J. (Eds.). (1994). *Improving organizational effectiveness through transformational leadership*. Sage.

Bass, B.M. (1990), "From transactional to transformational leadership: Learning to share the vision", *Organizational dynamics,* vol. 18, no. 3, pp. 19-31.

Braun, V., & Clarke, V. (2013). *Successful qualitative research: A practical guide for beginners*. sage.

De Bruijn, H. & Janssen, M. (2017), "Building Cybersecurity Awarsheness: The need for evidence-based framing strategies."

De Bruijn, W., Spruit, M. R., & Van Den Heuvel, M. (2010). Identifying the cost of security. *Journal of Information Assurance and Security*, *5*(2010), 074-083.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010), "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly: Management Information Systems,* vol. 34, no. SPEC. ISSUE 3, pp. 523-548.

Bycio, P., Hackett, R.D., & Allen, J.S., (1995). "Further assessments of Bass's (1985) conceptualization of transactional and transformational leadership." *Journal of applied psychology* 80.4: 468.

D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of business ethics*, *89*(1), 59.

D'Arcy, J., Hovav, A. & Galletta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach", *Information Systems Research,* vol. 20, no. 1, pp. 79-98.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information systems journal*, *11*(2), 127-153.

Fulk, J., Steinfield, C. W., Schmitz, J., & Power, J. G. (1987). A social information processing model of media use in organizations. *Communication research*, *14*(5), 529-552.

Furnell, S. M., Gennatou, M., & Dowland, P. S. (2002). A prototype tool for information security awareness and training. *Logistics Information Management*.

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*.

Hentea, M. (2005). A Perspective on Achieving Information Security Awareness. *Issues in Informing Science & Information Technology*, *2*.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125.

Hofstede, G. (2001). *Culture's consequences: Comparing values, behaviors, institutions and organizations across nations*. Sage publications.

Höne, K., & Eloff, J. H. P. (2002). Information security policy—what do international information security standards say?. *Computers & security*, *21*(5), 402-409.

Hovav, A., & D'Arcy, J. (2004). The impact of virus attack announcements on the market value of firms. Information Systems Security, 13(3), 32-40.

Humaidi, N., & Balakrishnan, V. (2015). Leadership styles and information security compliance behavior: The mediator effect of information security awareness. *International Journal of Information and Education Technology*, *5*(4), 311.

Jermier, J.M. & Berkes, L.J. (1979). "Leader behavior in a police command bureaucracy: A closer look at the quasi-military model." *Administrative science quarterly*: 1-23.

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, *12*(8), 3.

Kirsch, L., & Boss, S. (2007). The last line of defense: motivating employees to follow corporate security guidelines. *ICIS 2007 proceedings*, 103.

Moody, G.D., Siponen, M. & Pahnila, S. (2018). "Toward a unified model of information security policy compliance", *MIS Quarterly: Management Information Systems*, vol. 42, no. 1, pp. 285-311.

NCTV (2019). *Ontwrichting van de maatschappij ligt op de loer.* Geraadpleegd via: [https://nctv.nl/actueel/nieuws/2019/csbn-2019-ontwrichting-maatschappij-ligt-op-de-loer.aspx]

N. Nicholson, E. Soane, M. Fenton-O'Creevy, P. Willman (2005). *Personality and domain-specific risk taking.* Journal of Risk Research, 8 (2), pp. 157-176

NOS (2019a). *Ruim 100.000 CV's illegaal gedownload bij UWV.* Geraadpleegd via [https://nos.nl/artikel/2283117-ruim-100-000-cv-s-illegaal-gedownload-bij-uwv.html]

NOS (2018). *Nederland gaat brutaler terugslaan bij cyberaanval.* Geraadpleegd via [https://nos.nl/nieuwsuur/artikel/2259078-nederland-gaat-brutaler-terugslaan-bij-cyberaanvallen.html]

NOS (2019b). *Tweede Kamer wil meer greep op digitalisering en onderzoekt hoe dat moet.* Geraadpleegd via: [https://nos.nl/artikel/2287568-tweede-kamer-wil-meer-greep-op-digitalisering-en-onderzoekt-hoe-dat-moet.html]

Nu.nl (2018). *Minister Bijleveld: 'Nederland in cyberoorlog met Rusland.'* Geraadpleegd via: [https://www.nu.nl/internet/5513204/minister-bijleveld-nederland-in-cyberoorlog-met-rusland-.html]

Pahnila, S., Siponen, M., & Mahmood, A. (2007, January). Employees' behavior towards IS security policy compliance. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)* (pp. 156b-156b). IEEE.

Peace, A.G., Galletta, D., & Thong, J. (2003). "Software Piracy in the Workplace: A Model and Empirical Test." *Journal of Management Information Systems, 20 (1).*

Perry, J.L. (1996), "Measuring public service motivation: An assessment of construct reliability and validity", *Journal of Public Administration Research and Theory*, vol. 6, no. 1, pp. 5-22.

Pieters, W. (2011). The (social) construction of information security. *The Information Society*, *27*(5), 326-335.

Rhodes, S. & Steers, R.(1981). "A systematic approach to diagnosing employee absenteeism." *Employee Relations*.

Sharma, P. (2010). "Measuring personal cultural orientations: Scale development and validation", *Journal of the Academy of Marketing Science*, vol. 38, no. 6, pp. 787-806.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*.

Siponen, M., (2005). "Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods". Information and Organization, Volume 15, Issue 4, pp. 336 -375.

Siponen, M. & Vance, A. (2010) "Neutralization: New insights into the problem of employee information systems security policy violations", *MIS Quarterly: Management Information Systems*, vol. 34, no. SPEC. ISSUE 3, pp. 487-502.

Straub Jr, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276.

Thiel, S. V. (2010). Bestuurskundig onderzoek: een methodologische inleiding.

Tyler, T. R., & Blader, S. L. (2005). Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. *Academy of Management Journal*, *48*(6), 1143-1158.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198.

VNG (2019). *Standaardverklaring Baseline Informatiebeveiliging Overheid.* Geraadpleegd via: [https://vng-nl.eur.idm.oclc.org/files/vng/brieven/2019/20190107_ledenbrief_standaardverklaring-baseline-informatiebeveiliging-overheid.pdf]

Walumbwa, F. O. & Lawler, J.J. (2003). "Building effective organizations: Transformational leadership, collectivist orientation, work-related attitudes and withdrawal behaviours in three emerging economies." *International journal of human resource management* 14.7: 1083-1101.

Weber, E. U., & Milliman, R. A. (1997). Perceived risk attitudes: Relating risk perception to risky choice. *Management science*, *43*(2), 123-144.

Wilson, C. R; Van Voorhis; Morgan, B, L.(2007). *Understanding power and rules of thumb for determing sample sizes. Tutorials in Quant. Meth. for Psychology*, *3*(2), 43-50.

Bijlage 1: Survey vragenlijst

Beste deelnemer,

Bij voorbaat hartelijk bedankt voor je deelname. Deze vragenlijst is onderdeel van de masterscriptie van de studie Publiek Management aan de Erasmus Universiteit Rotterdam. Hierbij onderzoek ik de handhaving van richtlijnen op het gebied van informatiebeveiliging bij Nederlandse gemeenten. De focus ligt hierbij op de beleving en mening van de medewerker, waarbij er geen goede of foute antwoorden zijn.

Het invullen van de vragenlijst duurt ongeveer 10 tot 15 minuten. Je deelname aan dit onderzoek is anoniem en je gegevens worden vertrouwelijk behandeld. Dit betekent dat de ingevulde enquêtes alleen worden gebruikt voor dit onderzoek. Dit onderzoek is puur wetenschappelijk van aard en wordt niet voor commerciële doeleinden gebruikt. Succes!

Hieronder worden enkele stellingen gegeven.

	Volledig oneens (1)	Oneens (2)	Neutraal (3)	Eens (4)	Volledig eens (5)
Als ik mij niet houd aan de richtlijnen voor informatiebeveiliging, heeft dat consequenties. (1)	○	○	○	○	○
Directe collega's vinden dat ik me aan het informatiebeveiligingsbeleid moet houden. (2)	○	○	○	○	○
Er volgen sancties als ik niet voldoe aan de vereisten van het informatiebeveiligingsbeleid. (3)	○	○	○	○	○
Ik ben me bewust van de mogelijke risico's die er zijn als ik mij niet aan het informatiebeveiligingsbeleid houd. (4)	○	○	○	○	○
Ik ben zelden de eerste persoon die iets nieuws probeert. (5)	○	○	○	○	○
Ik begrijp de bezorgdheid over informatiebeveiliging en de risico's die ze in het algemeen vormen. (6)	○	○	○	○	○

Ik heb een cursus op het gebied van informatiebeveiligingsbeleid gevolgd. (7)	○	○	○	○	○
Ik ken mijn verantwoordelijkheden zoals voorgeschreven in het informatiebeveiligingsbeleid om de informatiebeveiliging van mijn organisatie te verbeteren. (8)	○	○	○	○	○
Ik zal waarschijnlijk worden gestraft als ik niet voldoe aan de vereisten van de informatiebeveiligingsbeleid. (9)	○	○	○	○	○
Ik zal monetaire of niet-geldelijke sancties oplopen als ik niet voldoe aan de vereisten van het informatiebeveiligingsbeleid. (10)	○	○	○	○	○
Ik zou mezelf niet omschrijven als iemand die graag risico's neemt. (11)	○	○	○	○	○
Ik geef de voorkeur aan een routinematige manier van leven ten faveure van een onvoorspelbaar leven vol verandering. (12)	○	○	○	○	○

Ik volg protocollen en beleid strikt en neem niet graag risico's. (13)	○	○	○	○	○
Mensen die mijn gedrag beïnvloeden, vinden dat ik me aan het informatiebeveiligingsbeleid moet houden. (14)	○	○	○	○	○
Mijn collega's zijn op de hoogte van het informatiebeveiligingsbeleid van mijn werkgever. (15)	○	○	○	○	○
Mijn leidinggevende besteedt aandacht aan iedereen afzonderlijk. (16)	○	○	○	○	○
Mijn leidinggevende bevestigt mijn sterke punten. (17)	○	○	○	○	○
Mijn leidinggevende helpt me om mijn competenties te ontwikkelen. (18)	○	○	○	○	○
Mijn leidinggevende maakt een onderscheid tussen zijn werknemers. (19)	○	○	○	○	○

Mijn leidinggevende vindt dat ik me aan het informatiebeveiligingsbeleid moet houden. (20)	○	○	○	○	○
Opgelegde sancties houden verband met of ik voldoe aan de vereisten van het informatiebeveiligingsbeleid. (21)	○	○	○	○	○

Vignette 1: Marijn heeft net gevoelige klantgegevens voor zijn werkgever verzameld en hij wil die gegevens mee naar huis nemen om zijn werk voort te zetten. Hij weet dat zijn werkgever vereist dat hij een wachtwoord aanvraagt dat wordt uitgegeven en wordt toegepast op alle gegevens voordat het op een USB-station het kantoor verlaat, zodat het niet kan worden bezocht door een onbevoegde persoon. Marijn heeft de procedure voor het aanvragen van een wachtwoord eerder voltooid, dus hij is ervan overtuigd dat hij het gemakkelijk opnieuw kan doen. Marijn gelooft dat het zonder het wachtwoord waarschijnlijk is dat ongeautoriseerde mensen de gegevens zullen zien, maar als ze dat doen, gebeurt er niets slechts. Marijn is van mening dat de wachtwoordprocedure niet effectief is en niet voorkomt dat onbevoegde personen de gegevens kunnen zien. Hoe dan ook, de wachtwoordprocedure duurt enkele minuten en hij moet nu vertrekken, dus hij slaat de procedure over. Marijn gelooft dat zijn kansen om gepakt te worden laag zijn, maar als hij wordt betrapt, zouden de consequenties minimaal zijn.

	Volledig oneens (1)	Oneens (2)	Neutraal (3)	Eens (4)	Volledig eens (5)
Ik zou in deze situatie hetzelfde handelen als Marijn. (1)	○	○	○	○	○
Het bovenstaande scenario is realistisch. (2)	○	○	○	○	○
Als ik Marijn was, had ik de procedure ook overgeslagen. (3)	○	○	○	○	○
Ik kan me voorstellen dat een soortgelijk scenario op mijn werk plaatsvindt. (4)	○	○	○	○	○
Ik denk dat ik zou doen wat Marijn deed als mij dit overkwam. (5)	○	○	○	○	○

Vignette 2: Marijn is aan het werk op zijn digitale werkplek. Tijdens het werk wordt hij gevraagd om even mee te kijken met een collega. Marijn accepteert dit en loopt met de collega mee. Hij verlaat zijn digitale werkplek, zonder deze te vergrendelen. Vervolgens ontstaat een discussie over de werkzaamheden, die langer duurt dan Marijn vooraf inschatte. De digitale werkplek van Marijn blijft hierdoor een tiental minuten onbewaakt en ontgrendeld. Als Marijn terugkomt bij zijn werkplek ziet hij dat deze nog steeds ontgrendeld is en hij bedenkt zich dat hij een fout heeft gemaakt door deze niet te vergrendelen bij het verlaten van zijn werkplek. Hij gelooft dat zijn kansen om hiermee geconfronteerd te worden erg laag zijn en eventuele consequenties ook minimaal zullen zijn.

	Volledig oneens (1)	Oneens (2)	Neutraal (3)	Eens (4)	Volledig eens (5)
Ik zou in deze situatie hetzelfde handelen als Marijn. (1)	○	○	○	○	○
Het bovenstaande scenario is realistisch. (2)	○	○	○	○	○
Als ik Marijn was, had ik de digitale werkplek ook niet vergrendeld. (3)	○	○	○	○	○
Ik kan me voorstellen dat een soortgelijk scenario op mijn werk plaatsvindt. (4)	○	○	○	○	○
Ik denk dat ik zou doen wat Marijn deed als mij dit overkwam. (5)	○	○	○	○	○

Vignette 3: Marijn heeft zojuist belangrijke informatie over een project verzameld en opgeslagen op een USB-stick. Eenmaal aangekomen op zijn werkplek wil hij de informatie overzetten naar zijn digitale werkplek, maar er komt iets tussen. Een collega vraagt om hulp en Marijn wil graag meedenken met deze collega. Hij laat de USB-stick achter op zijn bureau, om deze later te verwerken. Tijdens het gesprek met de collega verliest Marijn de tijd uit het oog en gaat hij door naar de volgende afspraak. De USB-stick ligt nog steeds op het bureau, maar dit kan volgens Marijn geen kwaad. Hij verwacht dat hij niet gepakt zal worden en dat de eventuele consequenties minimaal zullen zijn.

	Volledig oneens (1)	Oneens (2)	Neutraal (3)	Eens (4)	Volledig eens (5)
Ik zou in deze situatie hetzelfde handelen als Marijn. (1)	○	○	○	○	○
Het bovenstaande scenario is realistisch. (2)	○	○	○	○	○
Als ik Marijn was, had ik de USB-stick ook laten liggen. (3)	○	○	○	○	○
Ik kan me voorstellen dat een soortgelijk scenario op mijn werk plaatsvindt. (4)	○	○	○	○	○
Ik denk dat ik zou doen wat Marijn deed als mij dit overkwam. (5)	○	○	○	○	○

Ik ben een

- Man (1)
- Vrouw (2)
- Neutraal (3)

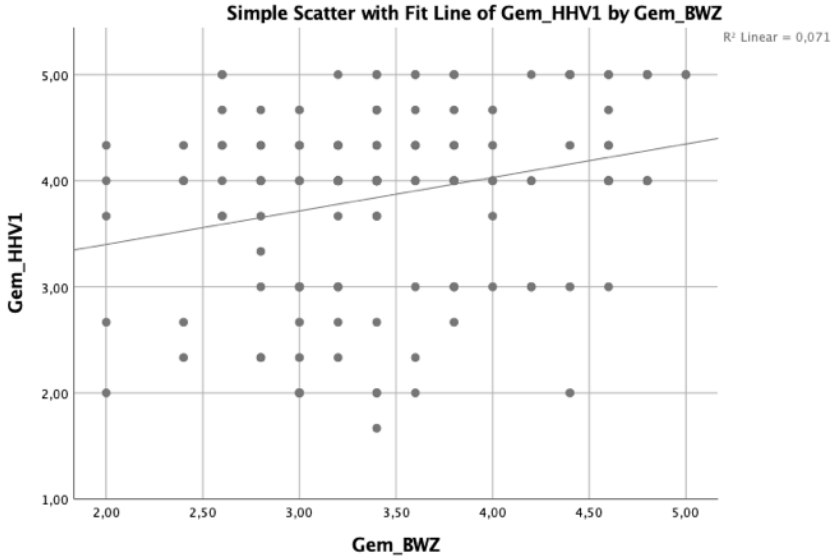
Wat is uw geboortejaar?

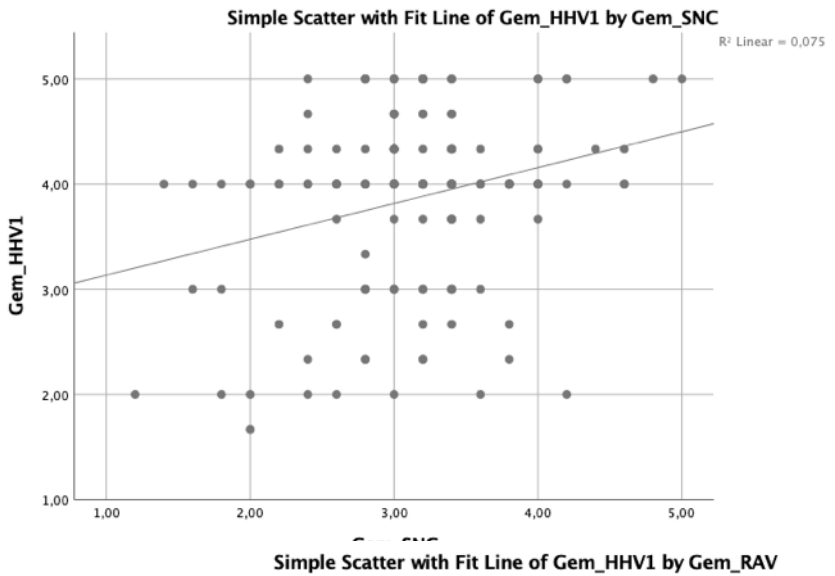
Wat is uw hoogst afgeronde opleiding?

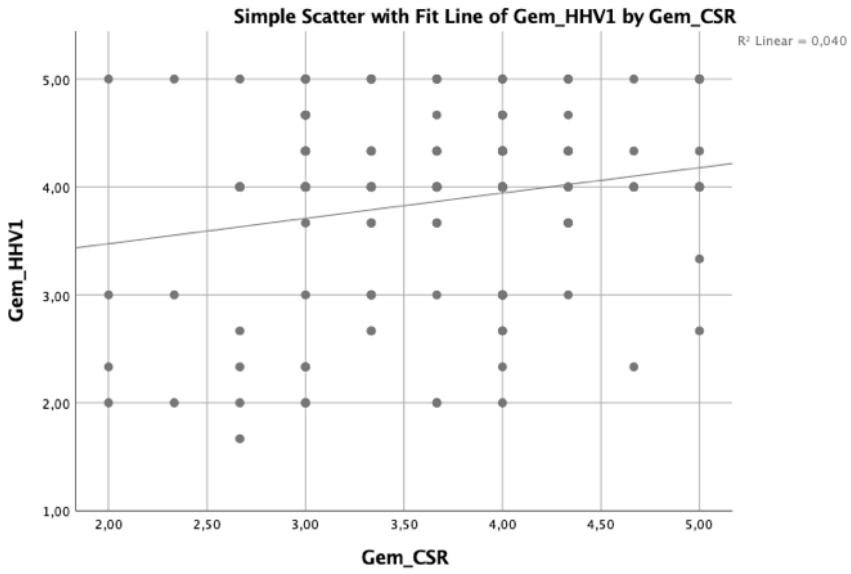
- ○ Basisonderwijs / Lager onderwijs (1)
- ○ MAVO (2)
- ○ HAVO (3)
- ○ VWO (4)
- ○ MBO (5)
- ○ HBO (6)
- ○ Universitair Bachelor (7)
- ○ Universitair Master (8)
- ○ PhD (9)
- ○ Wil ik niet zeggen (10)

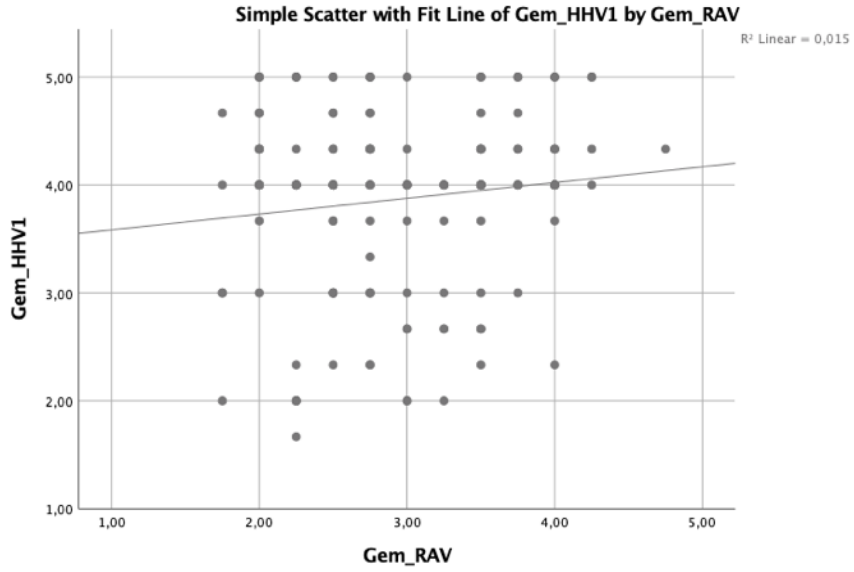
Bijlage 2: Scatterplots

Handhaving 1

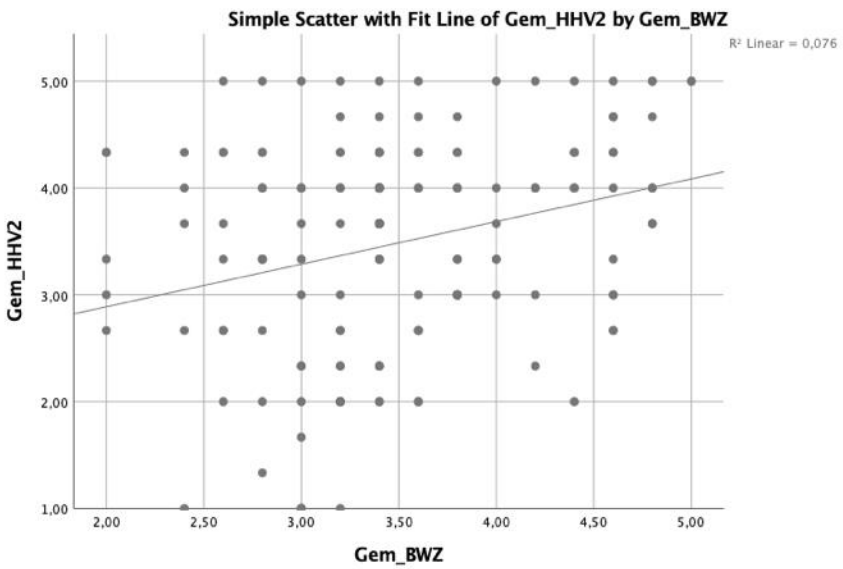


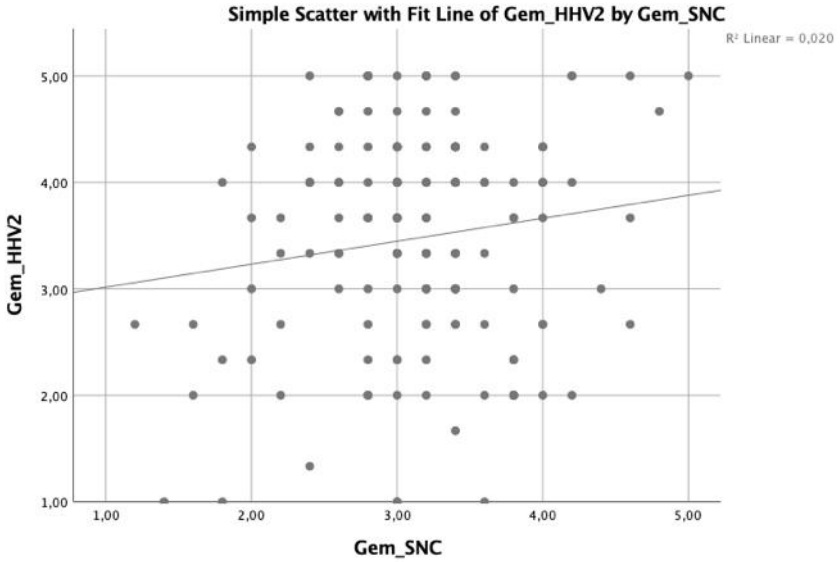


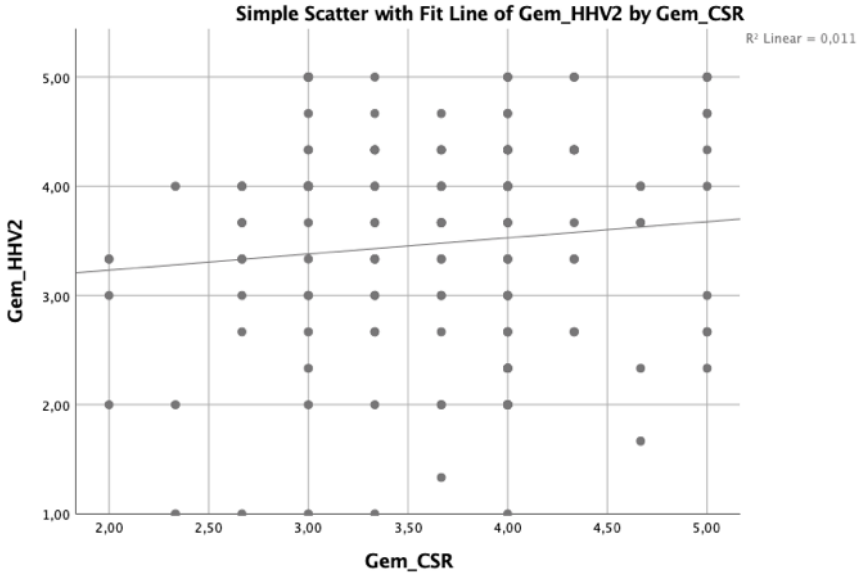


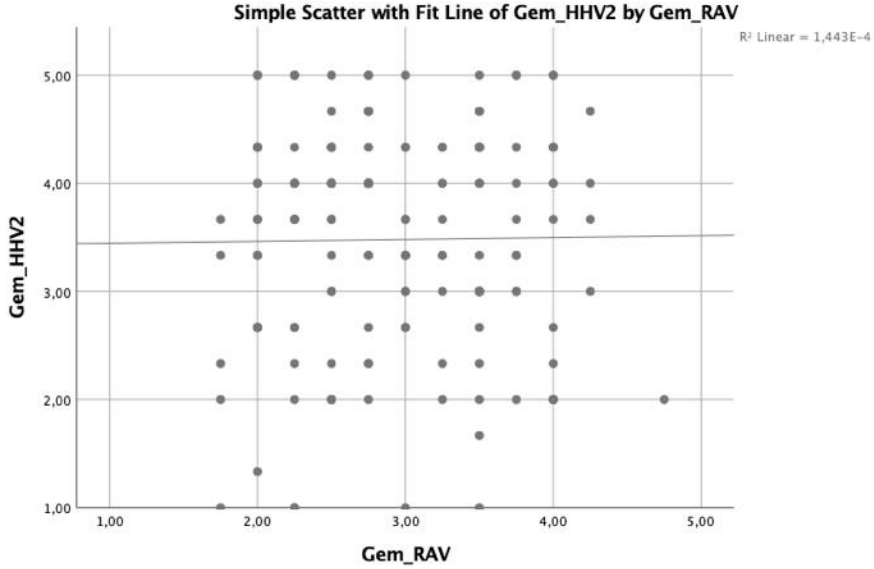


Handhaving 2









Handhaving 3