# MASTER'S THESIS

## De Human Aspects of Information Security Questionnaire (HAIS-Q)
## Een studie binnen de context van de gezondheidszorg

Verbeek, P.M.E.M.

**Award date:**
2021


# *DE HUMAN ASPECTS OF INFORMATION SECURITY QUESTIONNAIRE (HAIS-Q): EEN STUDIE BINNEN DE CONTEXT VAN DE GEZONDHEIDSZORG*


| | |
|---|---|
| Student: | P.M.E.M. Verbeek |
| Identiteitsnummer: | |
| Datum rapport: | 23 september 2021 |
| Versienummer: | 1.0 |
| Status: | Definitief |

# De Human Aspects of Information Security Questionnaire (HAIS-Q): Een studie binnen de context van de gezondheidszorg

# The Human Aspects of Information Security Questionnaire (HAIS-Q): A study within the context of health care


| | |
|---|---|
| Opleiding: | Open Universiteit, faculteit Management, Science & Technology |
| | Masteropleiding Business Process Management & IT |
| Programme: | Open University of the Netherlands, faculty of Management, Science & Technology<br>Master Business Process Management & IT |
| Cursus: | IM9806 Afstudeertraject Business Process Management & IT |
| Student: | P.M.E.M. Verbeek |
| Identiteitsnummer: | |
| Datum: | 23 september 2021 |
| Afstudeerbegeleider | Prof. Dr. L. Bijlsma |
| Meelezer | Dr. L. Rutledge |
| Versie nummer: | 1.0 |
| Status: | Definitief |

# Abstract

*Doel*

Het doel van dit onderzoek is de doorontwikkeling en validatie van de HAIS-Q voor het meten van het informatiebeveiligingsbewustzijn binnen de gezondheidszorg.

*Methodiek*

Middels een combinatie van interviews en documentstudie is het aandachtsgebied privacy geoperationaliseerd om toe te kunnen voegen aan de bestaande HAIS-Q. Een digitale enquête met opvolgende interviews heeft inzicht geboden in de validiteit en relevantie van de reeds bestaande aandachtsgebieden van de HAIS-Q voor de gezondheidszorg. Met behulp van de resultaten van deze onderzoeken is een doorontwikkelde HAIS-Q samengesteld welke getoetst is op validiteit en betrouwbaarheid, gebruikmakend van cognitieve testen en de berekening van Cronbach's alfa.

*Resultaten en conclusies*

Het aandachtsgebied privacy is geoperationaliseerd naar vier subgebieden met elk drie vragen, waarmee de doorontwikkelde HAIS-Q bestaat uit 75 vragen. Onderzoek naar relevantie en validiteit van bestaande aandachtgebieden heeft geleid tot een vervanging van zes vragen.

De inhoudelijke validiteit van de vragenlijst is afdoende vastgesteld, daar waar de constructvaliditeit binnen het onderzoek niet aangetoond is. Met een Cronbach's alfa van 0,9 is de doorontwikkelde vragenlijst betrouwbaar bevonden.

*Suggesties voor vervolgonderzoek*

De doorontwikkelde HAIS-Q zou verder gevalideerd kunnen worden binnen andere organisaties, gebruik makend van resultaten uit dit onderzoek.

## Sleutelbegrippen

Informatiebeveiligingsbewustzijn, gezondheidszorg, HAIS-Q, privacy, informatiebeveiliging

## Samenvatting

Met de verdergaande digitalisering neemt de afhankelijkheid van informatiesystemen steeds verder toe. Het gemak is toegenomen, maar ook de omvang van de risico's die we lopen. Dit merken we pas als we de systemen met opgeslagen informatie niet meer tot onze beschikking hebben. Zonder inzicht in gezondheidsinformatie van de patiënten kunnen zorgverleners geen zorg verlenen. Het is dan ook belangrijk dat de informatieveiligheid, vertaald naar beschikbaarheid, integriteit en vertrouwelijkheid, goed geborgd is. Waar mogelijk gebeurt dit door het nemen van technische maatregelen, waar dit niet kan bieden procedurele maatregelen, die vaak minder rigide zijn, een uitkomst. Naleving van beleid in procedures is afhankelijk van de medewerkers en hun mate van informatiebeveiligingsbewustzijn.

Het meten van informatiebeveiligingsbewustzijn kan organisaties helpen om gerichte campagnes op te zetten ter verbetering, met als doel een verbeterde informatieveiligheid en een vermindering van beveiligingsincidenten. Binnen de wetenschappelijke literatuur zijn weinig methoden te vinden om het bewustzijn te meten. De meest gevalideerde methode is de 'Human Aspects of Information Security Awareness Questionnaire', kortweg de HAIS-Q. De HAIS-Q bestaat uit 63 vragen die opgedeeld zijn naar inhoudelijke aandachtsgebieden die gezamenlijk het bewustzijn weergeven. De vragen zijn daarnaast onderverdeeld naar de dimensies kennis, houding en gedrag aangaande het beleid om inzicht te krijgen in staat van het bewustzijn op deze dimensies per aandachtsgebied.

Binnen de gehele digitale wereld, maar zeker bij gezondheidsinformatie, is vertrouwelijkheid van informatie zeer belangrijk. Dit vertaalt zich onder andere in verschillende wetgeving op het gebied van privacy. Onderzoek naar de HAIS-Q onderkent dat dit een onderwerp is wat toegevoegd zou moeten worden aan de vragenlijst om het informatiebeveiligingsbewustzijn verder vorm te geven. Dit onderzoek heeft tot hoofddoel om de bestaande HAIS-Q uit te breiden met dit onderwerp om vervolgens deze te toetsen op validiteit en betrouwbaarheid. Hiermee neemt de bruikbaarheid van de HAIS-Q toe, zeker voor organisaties in de gezondheidszorg.

Ontwikkeling van het onderwerp privacy heeft plaatsgevonden door middel van documentstudie en interviews met experts en management. Dit heeft geleid tot een viertal subgebieden binnen het hoofdgebied privacy en toevoeging van twaalf vragen. Toetsing op relevantie en validatie van de bestaande HAIS-Q is gebeurd middels een enquête gevolgd door interviews met experts en management. Resultaat is dat een zestal vragen zijn vervangen door nieuwe vragen die beter passen in de huidige staat van de technologie. Ook zijn een aantal vragen anders geformuleerd. Daarnaast is aan de doorontwikkelde HAIS-Q contextinformatie toegevoegd.

De doorontwikkelde HAIS-Q is getoetst op validiteit gebruik makend van resultaten uit andere onderzoeken en, zoals bovenstaand geschetst, enquêtes en interviews. Daarnaast zijn cognitieve tests afgenomen waar experts en zorgprofessionals hun begrip van de vragen hebben aangegeven door in bijzijn van de onderzoeker de HAIS-Q in te vullen en hardop aan te geven wat hun gedachten zijn. De resultaten laten zien dat 55 van de 75 vragen juist geïnterpreteerd worden. De overige vragen behoeven nog meer context of een aanpassing van gebruikte worden die misleidend kunnen zijn. De inhoudsvaliditeit van de doorontwikkelde HAIS-Q is daarmee afdoende. De constructvaliditeit is bij de ontwikkeling getoetst door een combinatie van interviews en documentonderzoek. De cognitieve test die hier ook uitspraak over zou moeten doen, heeft geen uitsluitsel geboden.

Om de interne consistentie van de vragenlijst, ofwel de betrouwbaarheid, te kunnen toetsen is de HAIS-Q binnen een pilotgroep van 63 medewerkers uitgezet werkzaam met digitale privacygevoelige informatie. Door corona is het niet mogelijk gebleken hier ook zorgprofessionals in te betrekken. 49 medewerkers hebben gereageerd, waarvan zeven een onvolledige invulling hebben gedaan. Het responspercentage komt daarmee op 66,7%. Om een uitspraak over de betrouwbaarheid te kunnen doen is de Cronbach's alfa bepaald, welke vergeleken is met overige onderzoeken. Een resultaat van 0,9 is in lijn met overige onderzoeken en duidt op een betrouwbare vragenlijst.

De enquête was aangevuld met feedbackvragen over de HAIS-Q. De resultaten laten zien dat de gemiddelde invultijd 22, 2 minuten is, wat als acceptabel is betiteld. Aan de duidelijkheid van de

vragen kan nog gewonnen worden. De toepasselijkheid van vragen is niet altijd aanwezig, wat maakt dat het wenselijk zou kunnen zijn om een extra antwoordoptie ‘niet van toepassing’ toe te voegen.

De doorontwikkelde HAIS-Q is een bruikbaar instrument en een aanvulling op de bestaande HAIS-Q. Het ontwikkelen van een methode of meetinstrument komt veelal tot stand door meerdere iteraties wat ook pleit voor vervolgonderzoek binnen meerdere organisaties en bij voorkeur met meer respondenten en een verschillend palet aan onderzoeksmethodes. Resultaten van dit onderzoek kunnen hierbij ondersteunen.

## Summary

With ongoing digitalisation, dependence on information systems is constantly increasing. Their convenience has increased, but so has the extent of the risks we run. We only notice this when we no longer have the systems with stored information at our disposal. Without insight into patients' health information, healthcare providers cannot provide care. It is therefore important that information security, translated into availability, integrity and confidentiality, is properly secured. Where possible, this is done by taking technical measures; where this is not possible, procedural measures, which are often less rigid, offer a solution. Compliance with policy in procedures depends on the employees and their degree of information security awareness.

Measuring information security awareness can help organisations to set up targeted improvement campaigns, with the aim of improving information security and reducing security incidents. Within the scientific literature, few methods can be found to measure awareness. The most validated method is the 'Human Aspects of Information Security Awareness Questionnaire', or the HAIS-Q for short. The HAIS-Q consists of 63 questions that are divided into content areas that collectively represent awareness. The questions are also subdivided according to the dimensions of knowledge, attitude and behaviour regarding the policy in order to gain insight into the level of awareness of these dimensions per focus area.

Within the entire digital world, but certainly in the case of health information, confidentiality of information is very important. This translates, among other things, into various legislation in the field of privacy. Research on the HAIS-Q recognises that this is a subject that should be added to the questionnaire to further shape information security awareness. The main objective of this study is to expand the existing HAIS-Q to include this subject and then to test it for validity and reliability. This will increase the usefulness of the HAIS-Q, especially for organisations in the healthcare sector.

The subject of privacy was developed by means of a document study and interviews with experts and management. This led to four sub-areas within the main area of privacy and the addition of twelve questions. The relevance and validation of the existing HAIS-Q was checked by means of a survey followed by interviews with experts and management. As a result, six questions were replaced by new questions that are more in line with the current state of technology. A number of questions have also been formulated differently. Context information has also been added to the redeveloped HAIS-Q.

The further developed HAIS-Q has been tested for validity using results from other studies and, as outlined above, surveys and interviews. In addition, cognitive tests were conducted in which experts and healthcare professionals indicated their understanding of the questions by filling in the HAIS-Q in the presence of the researcher and indicating their thoughts aloud. The results show that 55 of the 75 questions were interpreted correctly. The remaining questions require further context or an adjustment of words used that may be misleading. The content validity of the further developed HAIS-Q is therefore sufficient. The construct validity was tested during development through a combination of interviews and document research. The cognitive test, which should also make a statement about this, was inconclusive.

In order to test the internal consistency of the questionnaire, i.e. its reliability, the HAIS-Q was administered to a pilot group of 63 employees working with digital privacy-sensitive information. Due to corona, it was not possible to include healthcare professionals. Forty-nine employees responded, seven of whom did not complete the questionnaire fully. This brings the response rate to 66.7%. In order to make a statement about the reliability, the Cronbach's alpha was determined and compared to other surveys. A result of 0.9 is in line with other surveys and indicates a reliable questionnaire.

The survey was supplemented with feedback questions on the HAIS-Q. The results show that the average completion time is 22.2 minutes, which is considered acceptable. There is still room for improvement in the clarity of the questions. The applicability of questions is not always present, which makes it desirable to add an extra answer option 'not applicable'.

The further developed HAIS-Q is a useful instrument and an addition to the existing HAIS-Q. The development of a method or measuring instrument usually takes place through several iterations, which also argues in favour of follow-up research within several organisations and preferably with more respondents and a different range of research methods. The results of this study can support this.

# Inhoudsopgave

# 1 Introductie

## 1.1 Achtergrond

De ontwikkelingen binnen de informatie- en communicatietechnologie leiden tot steeds verdergaande digitalisering, zo ook in de gezondheidszorg. Binnen de keten van zorgverlening zijn zorgverleners voor het uitoefenen van hun taak in hoge mate afhankelijk van informatie die opgeslagen wordt in verschillende systemen, bijvoorbeeld bij de huisarts, de thuiszorg of in het ziekenhuisinformatiesysteem (hierna: ZIS) en het digitale patiëntendossier. Hiermee is ook de afhankelijkheid van deze digitale systemen meer en meer toegenomen. Dit wordt pas duidelijk als systemen het niet meer doen of als zij gecompromitteerd zijn. In de analoge wereld was de omvang van het risico gering, één of meer individuele dossiers. Een incident in de digitale wereld kan leiden tot het veelvoudig lekken van informatie of het niet kunnen helpen van vele patiënten. Met de digitalisering is het gemak toegenomen, maar ook de omvang van de risico's die we lopen. In de afgelopen jaren hebben we meerdere voorbeelden gezien van incidenten die zich hebben voorgedaan en de daarbij behorende gevolgen (Budding, 2018; Geest, 2019; NOS, 2017, 2018; Skipr, 2018; Z-CERT, 2020; Zondervirus, 2018).

Informatiebeveiliging en privacy zijn, mede door de digitalisering, steeds belangrijkere onderwerpen geworden. Regulering vindt plaats vanuit wettelijke kaders, sector regulering en organisatie behoeften, waaronder de Algemene Verordening Gegevensbescherming (hierna: AVG) en de normen van het Nederlandse Normalisatie instituut (hierna: NEN), de NEN7510, NEN7512 en NEN7513. Dit leidt tot een wirwar aan regels en richtlijnen die vaak door gebruikers niet worden begrepen en daarmee op gespannen voet kunnen staan met het gebruikersgemak wat eindgebruikers ervaren. Parsons, McCormac, Pattinson, Butavicius, and Jerram (2013) constateren dat managers het spanningsveld tussen de noodzaak om de veiligheidsvoorschriften na te leven en de noodzaak om de klus te klaren herkennen.

In te regelen maatregelen om aan regels te voldoen en informatieveiligheid en privacy te borgen, kunnen verschillend van aard zijn. Te denken valt aan organisatorische en technische maatregelen, maar ook aan gedragsbeïnvloeding wanneer technisch 'afdwingen' van maatregelen niet mogelijk of wenselijk is en naleving afhankelijk is van menselijk gedrag. Doordat digitalisering binnen de gezondheidszorg de afgelopen jaren stapsgewijs heeft plaatsgevonden, zijn juist mensen zich niet altijd bewust van onderliggende afhankelijkheden en risico's.

Ook binnen de gezondheidszorg zijn spanningsvelden te onderkennen tussen het inregelen maatregelen om regels na te leven en de werkbaarheid voor de zorgverlener, bijvoorbeeld bij het borgen van de privacy van patiënten en hun gegevens. De Wet op de Geneeskundige Behandelingsovereenkomst (hierna: WGBO) bepaalt dat artsen, verpleegkundigen of medewerkers een (deel van het) medisch dossier alleen mogen inkijken als er een behandelingsovereenkomst bestaat met de patiënt. Bestaat deze overeenkomst niet of wil men medische gegevens delen, dan moet de patiënt om expliciete toestemming worden gevraagd (Rijksoverheid, 1994). Deze regel kan niet in zijn geheel technisch worden afgedwongen, omdat dat ten koste gaat van de zorgverlening. Het ZIS is daarom naast geautoriseerde toegang ook uitgerust zijn met een zogenaamde 'breaking-the-glass' procedure. Dit is een noodprocedure om patiënten te kunnen helpen in acute zorgsituaties, zonder dat de patiënt toestemming tot inzage van zijn gegevens geeft. Een voorbeeld waar deze procedure gebruikt kan worden is wanneer een patiënt door een hartaanval niet in staat is toestemming te geven, maar inzicht in zijn gegevens wel noodzakelijk is voor het leveren van zorg. Het juiste gebruik van deze procedure is afhankelijk van het menselijke handelen.

De omvang van incidenten binnen de gezondheidszorg is zodanig hoog dat het vermoeden bestaat dat de informatiebeveiligingsmaatregelen regelmatig niet voldoen aan wet- en regelgeving. De Autoriteit Persoonsgegevens (hierna: AP) meldt in haar jaarverslag 2018 20.881 gerapporteerde datalekken, waarvan 29% in de sector gezondheid en welzijn (Autoriteit Persoonsgegevens, 2019b). Dit is een

indicatie dat niet alle maatregelen zorgvuldig worden nageleefd of juist zijn geïmplementeerd. Een recent onderzoek van de AP binnen een ziekenhuis heeft aangetoond dat de beveiliging van patiëntendossiers niet op orde was, leidend tot een zeer hoge boete (Autoriteit Persoonsgegevens, 2019a, 2019c).

De complexiteit van zorgprocessen in combinatie met de urgentie van de beschikbaarheid van informatie om zorgtaken uit te voeren maakt dat de maatregelen ten behoeve van informatiebeveiliging en privacy in systemen vaak een combinatie zijn van technische restricties en organisatorische procedures uit te voeren door medewerkers. Verschillende onderzoeken laten zien dat juist deze menselijke factor vaak oorzaak is van beveiligingsincidenten en daarmee een kritieke factor binnen de informatiebeveiliging (Evans, Maglaras, He, & Janicke, 2016; Parsons et al., 2010; Schultz, 2005). De mate van informatiebeveiligingsbewustzijn (hierna: IBB) van de medewerkers wordt daarmee een belangrijk onderdeel van het mitigeren van risico's binnen de informatiebeveiliging.

Hoe kan een organisatie inzicht krijgen in het IBB van haar medewerkers; hoe effectief is dit bewustzijn? Men kan zich bewust zijn van de noodzaak van beveiliging, maar doet men er in de praktijk ook wat mee?

Het doel van dit onderzoek is om te bepalen hoe het IBB van medewerkers effectief en correct te meten. Uitgangspunt is dat meer informatiebeveiligingsbewuste medewerkers minder incidenten tot gevolg hebben.

## 1.2 Context

Een onderzoek naar de mate van informatiebeveiligingsbewustzijn is het beste te plaatsen binnen het vakgebied Informatiekunde, waar management van informatiebeveiliging een onderdeel van is. Binnen het vakgebied van de informatiekunde, maar ook binnen het onderzoeksgebied van de gezondheidszorg worden verschillende vaktermen en begrippen gehanteerd. Ten behoeve van de leesbaarheid, betrouwbaarheid en validiteit van dit onderzoek is het noodzakelijk dat gehanteerde en van belang zijnde begrippen binnen dit onderzoek duidelijk gedefinieerd en toegelicht worden op de betekenis in de context van dit onderzoek (Verschuren & Doorewaard, 2007). Onderstaande worden de definities van begrippen omschreven, waar nodig met toelichting aangaande de context van dit onderzoek.

Informatiebeveiliging wordt door de ISO gedefinieerd als het behouden van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie (ISO/IEC, 2018). Vertrouwelijkheid definiëren zij als "informatie wordt niet beschikbaar gesteld of openbaar gemaakt aan onbevoegde personen, entiteiten of processen"; integriteit wordt omschreven als "informatie is nauwkeurig en compleet"; en beschikbaarheid als "informatie is toegankelijk en bruikbaar op verzoek van een bevoegde instantie".

Informatiebeveiligingsbeleid wordt binnen dit onderzoek omschreven als de intenties en richting van een organisatie op het gebied van informatiebeveiliging, zoals formeel tot uitdrukking gebracht door het topmanagement (ISO/IEC, 2018). De AP noemt dit privacybeleid, waarmee een organisatie in kaart brengt welke maatregelen zij heeft genomen om de persoonsgegevens van bijvoorbeeld klanten, patiënten, cliënten en medewerkers te beschermen. Daarnaast is het een manier om als organisatie aan zowel de doelgroep als aan de AP te laten zien dat ze voldoet aan de AVG (Autoriteit Persoonsgegevens, 2019d).

Privacy wordt in het juridische woordenboek omschreven als een grondrecht; het recht om met rust gelaten te worden, zowel fysiek (onaantastbaarheid menselijk lichaam, huisrecht) als informationeel (verwerking van persoonsgegevens, briefgeheim) (Juridisch Woordenboek, 2018). In het kader van dit onderzoek gaat het voornamelijk om het informationele deel van het recht op privacy, te weten persoonsgegevens die worden opgeslagen in informatiesystemen. Binnen artikel 4 van de AVG worden persoonsgegevens gedefinieerd als alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen

die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (Europees Parlement, 2016).

Artikel 33, lid 1 AVG spreekt over “een inbreuk in verband met persoonsgegevens” (Europees Parlement, 2016). In dit onderzoek wordt dit gehanteerd als de definitie van datalek. De ISO definieert een informatiebeveiligingsincident als enkele of een reeks van ongewenste of onverwachte geïdentificeerde voorvallen van een systeem-, dienst- of netwerkstatus die wijzen op een mogelijke inbreuk op het informatiebeveiligingsbeleid of het falen van controles, of een voorheen onbekende situatie die van belang kan zijn voor de beveiliging en die een grote kans op compromittering van de bedrijfsactiviteiten en een bedreiging van de informatiebeveiliging vormen (ISO/IEC, 2018).

Parsons et al. (2017) hebben informatiebeveiligingsbewustzijn (IBB) gedefinieerd als: “de mate waarin de medewerkers van een organisatie het belang en de gevolgen van informatiebeveiliging inzien en de mate waarin zij zich gedragen in overeenstemming met het beleid en de procedures van de organisatie op het gebied van informatiebeveiliging”.

Naast duiding van begrippen uit de vakgebieden informatiekunde en informatiebeveiliging is het ook noodzakelijk om de binnen dit onderzoek gehanteerde begrippen uit het onderzoeksgebied van de gezondheidszorg nader te duiden. Eén van de meeste relevante wetten binnen de gezondheidszorg is de, in het Burgerlijk Wetboek opgenomen, WGBO. Deze wet ligt aan de basis van alle zorgverlening en hierin staan de rechten en plichten van patiënten die zorg krijgen. Deze wet is van toepassing zodra een behandelingsovereenkomst ontstaat. Artikel 7:446, lid 1 BW definieert de behandelingsovereenkomst als: “De overeenkomst inzake geneeskundige behandeling - in deze afdeling verder aangeduid als de behandelingsovereenkomst - is de overeenkomst waarbij een natuurlijke persoon of een rechtspersoon, de hulpverlener, zich in de uitoefening van een geneeskundig beroep of bedrijf tegenover een ander, de opdrachtgever, verbindt tot het verrichten van handelingen op het gebied van de geneeskunst, rechtstreeks betrekking hebbende op de persoon van de opdrachtgever of van een bepaalde derde. Degene op wiens persoon de handelingen rechtstreeks betrekking hebben wordt verder aangeduid als de patiënt”.

## 1.3 Probleemstelling

Informatieveiligheid is zeer belangrijk in de gezondheidszorg. Het vertrouwen van patiënten dat zorgvuldig wordt omgegaan met hun gegevens is van groot belang, maar zonder integere en beschikbare informatie is het leveren van zorg onmogelijk. Maar hoe kan informatieveiligheid gewaarborgd worden zonder dat dit ten koste gaat van de werkbaarheid van het systeem voor de zorgverlener?

De inrichting van de ‘breaking-the-glass’ procedure is hier een mogelijkheid voor. De omvang van het gebruik van deze procedure binnen het onderzochte ziekenhuis is zodanig groot dat het vermoeden bestaat dat de maatregelen zeer regelmatig niet voldoen aan wet- en regelgeving. Het is echter onduidelijk wat de oorzaken zijn van het hoge gebruik van deze procedure en zodoende is er geen reëel beeld van de mate waarin de medewerkers het belang en de gevolgen van het gebruik van deze procedure inzien en de mate waarin zij zich gedragen in overeenstemming is met het beleid en de procedures van de organisatie.

Daarnaast laten onderzoeken zien dat de mens de zwakke schakel is binnen het geheel aan maatregelen en dat de gevolgen van beveiligingsincidenten zeer groot kunnen zijn, zeker binnen de gezondheidszorg.

## 1.4 Opdrachtformulering

De probleemstelling laat zien dat inzicht in de oorzaken van het veelvuldig gebruik van een ‘breaking-the-glass’ procedure ontbreekt, waarmee het dus ook niet duidelijk is hoe vaak en waarom deze procedure (on)terecht wordt gebruikt. Het vermoeden bestaat dat, ten aanzien van deze procedure, het informatiebeveiligings- en/of privacybeleid niet altijd wordt nageleefd.

Naleving van het informatiebeveiligings- en/of privacybeleid wordt vormgegeven in de maatregelen die een organisatie treft. De 'breaking-the-glass' procedure is een voorbeeld waarmee bewust afgeweken kan worden van de technisch ingerichte restricties en daarmee een bewuste keuze van een medewerker. De vraag is echter of de medewerkers het belang en de gevolgen van hun handelen inzien en of zij zich bewust zijn wanneer zij wel of niet invulling geven aan het informatiebeveiligings- en/of privacybeleid, het zogenaamde IBB.

Wanneer een organisatie inzicht zou hebben in dit IBB, zou zij ook in staat zijn om gerichte maatregelen te nemen om waar nodig dit bewustzijn te verhogen. Het doel van dit onderzoek is een methode te vinden of (verder) te ontwikkelen om het IBB van medewerkers effectief te meten.

De onderzoeksvraag is daarmee te formuleren als:

***Welke geschikte, en bij voorkeur gevalideerde, methode kan worden gebruikt voor het effectief meten van het informatiebeveiligingsbewustzijn binnen de gezondheidszorg?***

De onderzoeksvraag is opgedeeld in navolgende deelvragen die via literatuur (L) - of empirisch (E) onderzoek worden beantwoord en gezamenlijk leiden tot het beantwoorden van de onderzoeksvraag.

*L1 : Is IBB een van belang zijnde factor bij de naleving van het informatiebeveiligings- en/of privacybeleid?*

Het uitgangspunt van dit onderzoek, de mate van IBB is van invloed op naleving van het beleid, wordt middels antwoord op deze vraag gevalideerd.

*L2 : Welke gevalideerde methoden zijn er binnen de recente literatuur bekend om het IBB te meten en in hoeverre zijn deze bruikbaar binnen de gezondheidszorg?*

Op basis van de gevonden resultaten heeft het empirische vervolgonderzoek vorm gekregen.

*L3: Is het mogelijk om bestaande methoden voor het meten van IBB door te ontwikkelen en vervolgens te valideren, en zo ja op welke wijze?*

Onderzocht is op welke wijze een gevonden methode verder ontwikkeld en gevalideerd kan worden.

*E1 : Hoe ziet de uiteindelijke methode voor het meten van IBB van medewerkers binnen de gezondheidszorg eruit?*

Het doel van dit onderzoek is een bruikbare methodiek voor het meten van IBB te ontwikkelen, eventueel gebaseerd op een gevonden methode in de literatuur.

*E2 : In hoeverre is de uiteindelijke methode voor het meten van IBB valide en betrouwbaar?*

In het geval dat er een nieuwe methode voor het meten van IBB is ontwikkeld, zal deze methode gevalideerd moeten worden opdat deze nieuwe methode toepasbaar is binnen toekomstig onderzoek.

## 1.5 Motivatie / relevantie

***Wetenschappelijke relevantie***

De doelstelling van dit onderzoek is het onderzoeken en/of verder ontwikkelen en valideren van een methode voor het meten van het IBB binnen de gezondheidszorg. Literatuuronderzoek toont aan dat het IBB zeer relevant is voor de naleving van informatiebeveiliging- en/of privacy beleid. Ook toont literatuuronderzoek aan dat er momenteel wel methoden zijn voor het meten van IBB, maar dat de relatie tussen IBB en privacy verder onderzocht moet worden. De ontwikkeling en toetsing van een dergelijke methode is zodoende wetenschappelijk relevant.

***Maatschappelijke relevantie***

Wanneer middels een gevalideerde methode gemeten kan worden in hoeverre medewerkers informatiebeveiligingsbewust zijn, kan dit organisaties helpen om het IBB van hun medewerkers te

ontwikkelen om zo de naleving van informatiebeveiligings- en/of privacy beleid te optimaliseren. Meer informatiebeveiligingsbewuste medewerkers leidt tot een betere naleving van het beleid en tot minder informatiebeveiligings- en/of privacy incidenten. Hier is de hele samenleving bij gebaat.

## 1.6 Leeswijzer

Hoofdstuk 2 beschrijft de aanpak, de uitvoering en de resultaten van het literatuuronderzoek wat de basis legt voor het doel en de uitvoering van het empirisch vervolgonderzoek. In hoofdstuk 3 is aangegeven wat in de empirie is onderzocht, waarom en op welke wijze. De uitvoering en resultaten van het empirisch onderzoek worden in hoofdstuk 4 en 5 weergegeven. In het laatste hoofdstuk (6) wordt afgesloten met een discussie van de resultaten, de conclusie en aanbevelingen voor zowel de praktijk als voor vervolgstudies.

# 2 Literatuuronderzoek

Het literatuuronderzoek vormt een theoretisch kader dat als basis dient voor het empirisch onderzoe. Dit hoofdstuk beschrijft de aanpak, uitvoering, resultaten en uiteindelijke conclusies van het literatuuronderzoek. Er wordt afgesloten met het doel voor het empirisch vervolgonderzoek.

## 2.1 Onderzoeksaanpak en -uitvoering

Voor beantwoording van de deelvragen voor de vorming van het theoretisch kader is gebruik gemaakt van verschillende methoden. Op basis van zoekwoorden, kernwoorden uit de geformuleerde deelvraag of afgeleide woorden hiervan, is gezocht naar geschikte publicaties in tertiaire (databases) en secundaire (officiële publicaties) bronnen die beschikbaar zijn via de universiteitsbibliotheek van de Open Universiteit. Er is zoveel mogelijk gebruik gemaakt van publicaties die getoetst zijn door erkende deskundigen, de zogenaamde peer reviewed publicaties, ten behoeve van de betrouwbaarheid.

Naast deze methodiek is gebruik gemaakt van twee vooraf bekende relevante publicaties, te weten de rapporten van Wissen (2017) en van Schaeken (2018), beide aangaande het meten van IBB. De door hen gebruikte literatuur is onderzocht op het belang voor dit onderzoek.

Voor alle deelvragen is uit het totaal van de gevonden publicaties een selectie gemaakt van geschikte publicaties voor de beantwoording van de deelvragen. Deze publicaties zijn samengevat, geanalyseerd en verwerkt in een onderbouwde beantwoording van de deelvragen. Deze beantwoording vormt de basis voor het doel van het opvolgende empirische onderzoek.

Een gedetailleerde beschrijving van de gebruikte query's, de gebruikte bronnen, de aantallen gevonden publicaties en de uiteindelijk gebruikte publicaties voor beantwoording van de deelvragen worden weergegeven in bijlage I.

## 2.2 Resultaten en conclusies

### 2.2.1 Het belang van informatiebeveiligingsbewustzijn

Binnen de wetenschappelijke literatuur zijn veel onderzoeken te vinden die het onderwerp informatiebeveiliging behandelen, wat in lijn is met het belang van het onderwerp in de steeds verdergaande digitalisering van de samenleving en de daarbij behorende afhankelijkheid van informatiesystemen en data. In het verleden waren informatiebeveiligingsoplossingen grotendeels technisch van aard, met de nadruk op de ontwikkeling van hardware-, software- en netwerkoplossingen (Parsons, McCormac, Pattinson, et al., 2013). Naast technische oplossingen worden voor de beveiliging van de systemen en data ook organisatorische procedures, uit te voeren door medewerkers, ontwikkeld om informatiebeveiligingsmaatregelen te implementeren. Verschillende onderzoeken laten zien dat juist deze menselijke factor vaak oorzaak is van beveiligingsincidenten en daarmee een kritieke factor is binnen de informatiebeveiliging (Bragdon, 2018; Evans, He, Maglaras, & Janicke, 2019; Evans et al., 2016; Schultz, 2005).

Onderzoeken gericht op identificatie van factoren die informatiebeveiligingsgedrag beïnvloeden, maken veelal gebruik van gedragsmodellen die hun oorsprong vinden in de criminologie of de psychologie (Bulgurcu, Cavusoglu, & Benbasat, 2010; Chen, Chen, Wu, & Teng, 2018; Choi & Song, 2018; Cox, 2012; D'arcy & Herath, 2011; D'Arcy, Hovav, & Galletta, 2009; Haeussinger & Kranz, 2013; Ifinedo, 2014; Kim, Yang, & Park, 2014; Kruger & Kearney, 2006; E. H. Park, Kim, Wiles, & Park, 2018; Y. S. Park, Park, & Kim, 2017; Rocha Flores & Ekstedt, 2016; Siponen & Vance, 2010; Vance, Siponen, & Pahnila, 2012).

Karjalainen and Siponen (2011) beweren dat veel literatuur zich alleen op verificatie of validatie van de gebruikte theorieën richt en zodoende een bevooroordeeld gezichtspunt hebben ten aanzien van de gekozen theorie. Daarnaast worden binnen deze onderzoeken over het algemeen alleen factoren bestudeert die uit de gebruikte theorie (gedragsmodel) naar voren komen, wat maakt dat deze onderzoeken veelal eenzijdig en/of onvolledig zijn. Dit is met name binnen onderzoek naar informatiebeveiliging een risico, omdat gedrag van medewerkers door vele factoren kan worden

beïnvloed (Vroom & von Solms, 2004). Dit blijkt ook uit de literatuurstudie van Sommestad, Hallberg, Lundholm, and Bengtsson (2014) waarbinnen een van onderzochte factoren zichtbaar is met daarbij inzicht in factoren die bewezen van invloed zijn op gedrag.

Andere onderzoeken combineren verschillende gedragsmodellen in één onderzoek om zoveel mogelijk factoren van interesse te kunnen testen (Bauer & Bernroider, 2017; Box & Pottas, 2014; Herath & Rao, 2009a, 2009b; Ifinedo, 2012, 2014; Rajab & Eydgahi, 2019; Siponen, Adam Mahmood, & Pahnila, 2014). Onderzoeken waarin meerdere theorieën in één model worden samengevoegd, zonder wetenschappelijk bewijs dat deze samenvoeging geen ongewenste effecten heeft, zijn om die reden niet gebruikt binnen dit onderzoek.

Als we de verschillende modellen meer in detail bekijken zien we dat het merendeel van de modellen het gedrag of gewenste gedrag, veelal naleving van informatiebeveiligingsbeleid, als afhankelijke factor onderzoekt. De onafhankelijke en/of mediërende en/of modererende factoren zijn zeer veel en divers van aard en de verschillende onderzoeken variëren nog wel eens in de resultaten van vergelijkbare factoren, wat het onderzoek van Sommestad et al. (2014) bevestigt.

IBB als factor komt in meerdere onderzoeken naar voren (Al-Omari, El-Gayar, & Deokar, 2012; Bauer & Bernroider, 2017; Bulgurcu et al., 2010; Chua, Wong, Low, & Chang, 2018; D'Arcy et al., 2009; Haeussinger & Kranz, 2013; E. H. Park et al., 2018; Y. S. Park et al., 2017; Rocha Flores & Ekstedt, 2016), waarbij de gehanteerde definitie van IBB kan variëren. Enkele onderzoeken laten IBB zien als mediërende factor, in andere onderzoeken is IBB een onafhankelijke factor, **maar binnen de onderzoeken waar IBB als factor is benoemd wordt deze statistisch aangemerkt als een factor met invloed op het gedrag. Dit bevestigt het uitgangspunt van dit onderzoek.**

### 2.2.2 Bruikbare en gevalideerde methoden voor het meten van IBB

Zoals uit vorige paragraaf gebleken, komt uit verschillende onderzoeken naar voren dat IBB een factor van belang is bij de naleving van informatiebeveiligings- en/of privacybeleid. Een wetenschappelijk gevalideerde methode voor het bepalen van IBB wordt binnen die onderzoeken niet gebruikt.

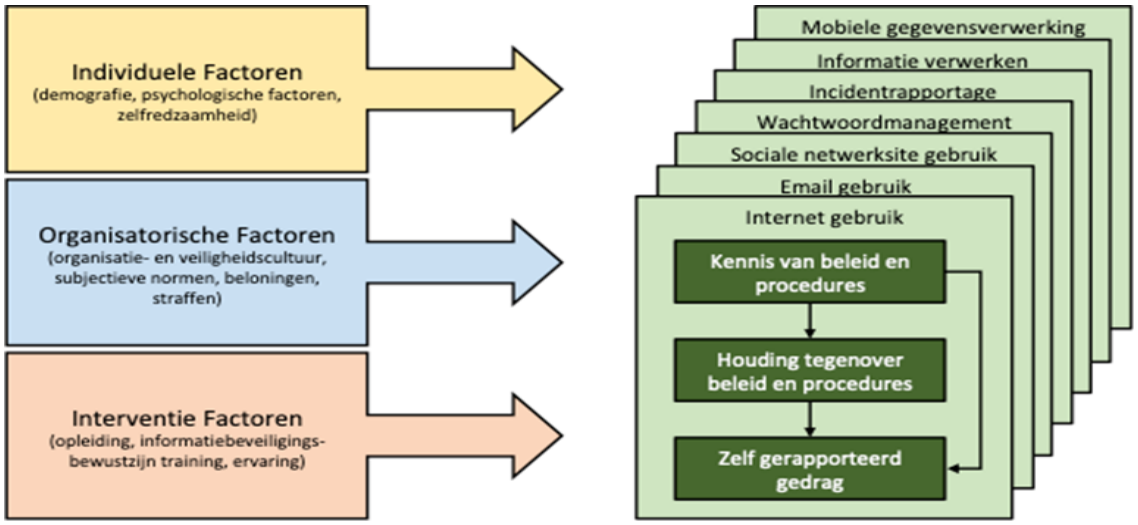
De bestaande literatuur is nog niet heel rijk als het gaat om gevalideerde methoden voor het meten van IBB. Kruger and Kearney (2006) zijn gestart met de ontwikkeling van een prototype voor het meten van IBB. Binnen dit prototype, gebaseerd op het KAB model, zijn de drie dimensies kennis (wat weet iemand), houding (wat vindt iemand) en gedrag (wat doet iemand) opgesplitst naar zes inhoudelijke aandachtsgebieden. Het prototype van het model is getest in Australië.

Op basis van dit prototype hebben Kruger, Drevin, and Steyn (2006) een framework voor de evaluatie van IBB ontwikkeld. Dit framework heeft als extra toevoeging dat systeemdata wordt geanalyseerd om het daadwerkelijk beveiligingsgedrag van de medewerkers te bepalen. Het framework is toegepast in een universitaire omgeving.

Parsons, McCormac, Pattinson, et al. (2013) ontwikkelden de, eveneens gebruikmakend van aandachtsgebieden en gebaseerd op het KAB-model, Human Aspects of Information Security Questionnaire (hierna: HAIS-Q) om het IBB te meten. Om een zo onbevooroordeeld mogelijk instrument te ontwikkelen, is bij de ontwikkeling gebruik gemaakt van zowel kwantitatieve als kwalitatieve onderzoeksmethoden (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2013), een aanpak die aanbevolen wordt door Karjalainen and Siponen (2011). Bij de ontwikkeling onderkennen zij dat er naast de dimensies kennis en houding meerdere factoren zijn die van invloed zijn op het gedrag. Dit is in overeenstemming met het onderzoek van Vroom and von Solms (2004) en Sommestad et al. (2014). Hiertoe nemen ze in hun ontwikkelde HAIS-Q ook individuele, organisatorische en interventiefactoren op. Een eerste validatie laat positieve resultaten zien.

Verdere validatie en mogelijke uitbreiding van de HAIS-Q heeft onder andere plaatsgevonden binnen de onderzoeken van McCormac et al. (2016); McCormac et al. (2017); Parsons et al. (2017); Parsons, McCormac, Butavicius, Pattinson, and Jerram (2014); Schaeken (2018); Wissen (2017), waarbij het instrument steeds breder is getoetst. Naast het feit dat ook deze onderzoeken positieve resultaten laten

zien aangaande het gebruik van de HAIS-Q, worden ook suggesties gedaan voor vervolgonderzoek om het instrument te verbeteren.




Figuur 1 The Human Aspects of Information Security (HAIS) model

Binnen andere onderzoeken zijn eveneens methoden ontwikkeld voor het meten van IBB (Egelman & Peer, 2015; Öğütçü, Testik, & Chouseinoglou, 2015; Rezgui & Marks, 2008; Velki, Solic, & Ocevcic, 2014). Deze methoden zijn echter alleen in het eigen onderzoek gevalideerd. Verdere validatie van deze methoden heeft naar mijn weten niet plaatsgevonden.

Concluderend kan gesteld worden dat het aantal gevalideerde methoden voor het meten van IBB zeer gering is, waarbij het meten van IBB gebruikmakend van de HAIS-Q als meest gevalideerde methode wordt beschouwd.

Naast een gevalideerd model, is een andere voorwaarde voor bruikbaarheid van een model binnen de gezondheidszorg het kunnen meten van bewustzijn op het gebied van privacy. Uit figuur 1 wordt duidelijk dat binnen dit model het aandachtsgebied privacy ontbreekt. Parsons et al. (2017) hebben in hun artikel als suggestie voor vervolgonderzoek aangegeven dat de relatie tussen IBB en privacybelangen verder zou kunnen worden onderzocht, door opname van maatregelen van privacybelangen en –gedrag.

**Als antwoord op de vraag welke gevalideerde methoden er binnen de recente literatuur bekend zijn om het IBB te meten kan worden gesteld dat de HAIS-Q de meest gevalideerde methode is. Op de vraag of deze methode ook bruikbaar is binnen de gezondheidszorg, is het antwoord dat deze methode een uitermate geschikte basis biedt. Echter het model behoeft uitbreiding met het aspect privacy.**

### 2.2.3 Doorontwikkeling en validatie van het basismodel

Voor de initiële model ontwikkeling hebben Parsons, McCormac, Butavicius, et al. (2013) gebruik gemaakt van een hybride onderzoeksmethode, waarbij de inductieve, verkennende aanpak is opgenomen die wordt aanbevolen door Karjalainen and Siponen (2011). Hybride om een mix van kwalitatieve en kwantitatieve methoden voor het verzamelen en analyseren van gegevens aan te duiden. Ten behoeve van de ontwikkeling van de informatiebeveiligingsvragenlijst, zijn interviews gehouden met het senior management.

Het resultaat van dit verkennende proces is uiteindelijk de hypothese dat naarmate het kennisniveau van computergebruikers over informatiebeveiligingsbeleid en -procedures toeneemt, hun houding ten opzichte van informatiebeveiligingsbeleid en -procedures verbetert, wat zich zou moeten vertalen in meer risicomijdend gedrag op het gebied van informatiebeveiliging. Dit veranderingsproces wordt ook wel het KAB-model genoemd en een verfijnde en specifieke versie van dit model is een onderdeel van het HAIS-model.

Op basis van de aanbeveling van McGuire (1969) is binnen het theoretische model het begrip kennis eerst geconceptualiseerd als 'kennis van beleid en procedures'. Binnen die verfijnde context zijn verschillende informatiebeveiligingsbeleidsregels herzien en de bevindingen van interviews met het senior management gebruikt om specifieke aandachtsgebieden te ontwikkelen. Deze waren bedoeld om de gebieden van een informatiebeveiligingsbeleid weer te geven die relevant zijn voor werkgevers en computergebruikers en die het meest vatbaar zijn voor niet-naleving. Op deze wijze zijn de zeven aandachtsgebieden geïdentificeerd. Per aandachtsgebied zijn drie subgebieden ontwikkeld om per subgebied een stelling op elke dimensie van het KAB-model (kennis, houding en gedrag) te ontwikkelen. De KAB-component van de HAIS-Q bestaat daarmee uit 63 stellingen, elk te scoren op een 5 punt Likert-schaal.

Parsons, McCormac, Butavicius, et al. (2013) hebben vervolgens middels drie technieken de validiteit en betrouwbaarheid van de onderzoeksonderdelen getest, te weten:

1) Expert toetsing door vragen naar begrip van de termen, de duidelijkheid van de richting en eventuele andere mogelijke misverstanden.
2) Uitvoeren van een cognitieve test met een informatiebeveiliging expert, waarbij een combinatie van hardop denken en mondelinge toetsing wordt toegepast.
3) Pilotstudie waarbij de resultaten zijn onderzocht om eventuele resterende problemen op te sporen en de betrouwbaarheid van de belangrijkste onderdelen van het onderzoek vast te stellen.

McCormac et al. (2016) hebben daarnaast de validiteit en betrouwbaarheid van het model getest door dezelfde meting op 2 momenten uit te voeren en de Cronbachs alfa van beide metingen met elkaar te vergelijken en door te zoeken naar correlatie tussen de resultaten van de twee metingen.

Binnen het onderzoek van Parsons et al. (2017) is de validiteit van de HAIS-Q getoetst door een maatregel voor gedrag te nemen en aan te tonen dat deze correleert met de theoretisch-gerelateerde meting van het IBB. Dit naast een studie onder een groot aantal respondenten.

Andere onderzoeken die de HAIS-Q uitbreiden, wijzigen en/of valideren (Parsons et al., 2014; Parsons, McCormac, Pattinson, et al., 2013; Schaeken, 2018; Wissen, 2017) maken allen gebruik van hybride methodieken zoals gebruikt bij de ontwikkeling van het model. Wissen (2017) geeft in zijn onderzoek aan dat het ten behoeve van de validiteit goed zou zijn om de vragenlijst voorafgaand te toetsen op relevantie voor de organisatie van onderzoek. Ook geeft hij aan dat de betrouwbaarheid van het model kan worden vergroot door te kijken naar daadwerkelijk gedrag in plaats van zelf gerapporteerd gedrag. De verhoging van de interne validiteit kan volgens Wissen (2017) bereikt worden door de verschillende vragen uit de HAIS-Q te voorzien van meer context.

**Het antwoord op de vraag of het mogelijk is om bestaande methoden voor het meten van IBB door te ontwikkelen en vervolgens te valideren is ja. Op de vraag op welke wijze dit kan geschieden, is het antwoord dat hiervoor een combinatie van methodieken gebruikt kan worden. Voor de uitbreiding van het model met een aandachtsgebied kunnen op basis van documentenstudie en interviews binnen de te onderzoeken branche subgebieden met stellingen per dimensie worden ontwikkeld. Tevens kunnen op deze wijze de bestaande aandachtsgebieden worden getoetst voor toepassing binnen de branche. De uiteindelijke vragenlijst kan worden gevalideerd op verschillende wijzen, waaronder expert toetsing, uitvoering van een cognitieve test en uitvoeren van een pilotstudie waarbij de resultaten statistisch worden onderzocht.**

## 2.3 Doel van het empirisch vervolgonderzoek

Literatuuronderzoek heeft aangetoond dat IBB een factor van invloed is bij de naleving van het informatiebeveiligingsbeleid. Ook laat het literatuuronderzoek zien dat de meest gevalideerde methode voor het meten van IBB de HAIS-Q is. Binnen deze HAIS-Q worden verschillende aandachtsgebieden onderscheiden, echter geen van deze gebieden is specifiek gericht op privacy wat voor de gezondheidszorg een zeer belangrijk aandachtsgebied is.

Omdat de HAIS-Q een zeer solide basis biedt voor meting van IBB, is het doel van het vervolgonderzoek de bestaande HAIS-Q binnen de branche te toetsen op relevantie en eventueel uit te breiden met het aspect privacy, opdat er een bruikbaar model ontstaat wat binnen de gezondheidszorg gebruikt kan worden voor het meten van IBB.

De nieuw ontwikkelde HAIS-Q zal vervolgens getoetst moeten worden op betrouwbaarheid en validiteit.

Voor het bereiken van deze onderzoeksdoelen, zijn de volgende empirische onderzoeksvragen benoemd, startend met een E.

***E1 : Hoe ziet de uiteindelijke methode voor het meten van informatiebeveiligingsbewustzijn van medewerkers binnen de gezondheidszorg eruit?***

***E2 : In hoeverre is de uiteindelijke methode voor het meten van IBB valide en betrouwbaar?***

# 3 Methodologie

Dit hoofdstuk is de methodologische verantwoording van het empirisch onderzoek, waarin strategie, aanpak en verantwoording van strategie en aanpak worden beschreven.

## 3.1 Conceptueel ontwerp onderzoek: de methode

Het doel van het empirisch onderzoek kan worden omschreven als:

***De doorontwikkeling en validatie van de HAIS-Q voor het meten van IBB binnen de gezondheidszorg.***

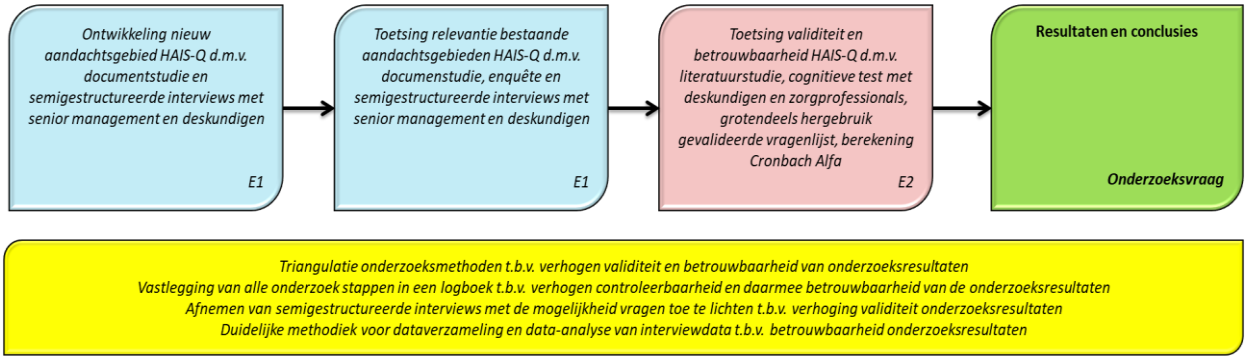
Voor de doorontwikkeling van dit model is een verkennend onderzoek uitgevoerd binnen één ziekenhuis om een aandachtsgebied toe te voegen aan het HAIS-model, de bestaande aandachtsgebieden te toetsen op relevantie en het doorontwikkelde model te toetsen op validiteit en betrouwbaarheid.

Om een aandachtsgebied toe te kunnen voegen en bestaande aandachtsgebieden te toetsen op relevantie, is informatie noodzakelijk over aandachtsgebieden die vatbaar zijn voor niet-naleving. Belangrijk hierbij is dat het niet naleven vooral veroorzaakt wordt door menselijk handelen. Deze informatie is te vinden in beleidsstukken en bij betrokken (senior) management en deskundigen op het gebied van informatiebeveiliging en privacybescherming. Voor het verkrijgen van deze informatie is gebruik gemaakt van een combinatie van een tweetal kwalitatieve onderzoeksmethoden, de documentstudie en semigestructureerde interviews. Daarnaast is voor het bepalen van de relevantie en validatie van bestaande HAIS-Q onderdelen gebruik gemaakt van een kwantitatieve methode, de enquête, gevolgd door een kwalitatieve methode, het semigestructureerde interview waarin ingegaan is op de antwoorden in de enquête voor nadere duiding. Het gebruik van verschillende bronnen voor ontwikkeling van de nieuwe vragenlijst, draagt bij aan de constructvaliditeit van het onderzoek.

Op basis van analyse van vergaarde data is een vernieuwde HAIS-Q samengesteld. Voor de bepaling van de validiteit en betrouwbaarheid van deze vragenlijst is een combinatie van een kwalitatieve (cognitieve test) en kwantitatieve methode (pilot test) toegepast.

Saunders, Lewis, and Thornhill (2016) beschrijven de gehanteerde methodiek als een inductieve onderzoeksaanpak middels een enkelvoudige holistische casestudy. Er is gekozen voor deze aanpak, omdat uit literatuuronderzoek is gebleken dat dit een valide aanpak is voor modelontwikkeling en -validering, waaronder bij de opzet van het originele HAIS-model (Parsons, McCormac, Butavicius, et al., 2013). Als case is een ziekenhuis genomen, het ziekenhuis waar de onderzoeker werkzaam is. Dit omdat op deze wijze de informatie en respondenten goed toegankelijk waren.

Onderstaande figuur geeft de onderzoeksstrategie visueel weer, waarbij een link gelegd wordt met de empirische onderzoeksvragen. De detailuitvoering wordt besproken in paragraaf 3.2. In onderstaande figuur is ook weergegeven op welke wijze validiteit en betrouwbaarheid van het onderzoek zelf gewaarborgd zijn. Dit wordt verder besproken in paragraaf 3.3.




Figuur 2 Onderzoeksstrategie

## 3.2 Technisch ontwerp onderzoek: de aanpak

### 3.2.1 Ontwikkeling nieuwe en toetsing bestaande aandachtsgebieden HAIS-Q

Binnen dit deel van het onderzoek is het doel het aandachtsgebied privacy aan de vragenlijst toe te voegen. Hiertoe zal nagegaan moeten worden of dit inderdaad een relevant aandachtsgebied is en zo ja, hoe dit te operationaliseren. Tevens zullen de bestaande aandachtgebieden beoordeeld worden op toepasbaarheid binnen de context van de gezondheidszorg, zijn ze nog relevant en zo ja, zijn ze op juiste wijze geoperationaliseerd. Deze paragraaf beschrijft gedetailleerd op welke wijze de gekozen methoden van onderzoek zijn uitgevoerd.

#### *3.2.1.1 Documentstudie*

Gestart is met documentonderzoek van vigerend beleid binnen de gezondheidszorg op het gebied van informatiebeveiliging en privacy, volgens het volgende stappenplan:

1. Selectie relevante documenten, in samenspraak met deskundigen. Bij de keuze van documenten is gelet op de geldigheid van het document binnen de gehele gezondheidszorg en niet alleen bij de case-organisatie. In geval van wet- en regelgeving dient het document afkomstig te zijn van de wetgever, in geval van richtlijnen dient het document afkomstig te zijn van een binnen de branche erkende organisatie;
2. Lezen van geselecteerde documenten op mogelijk relevante teksten voor het onderzoek om te komen tot een overzicht van relevante teksten;
3. Analyse overzicht van relevant bevonden teksten om te komen tot een set met relevante aandachtsgebieden die het meest vatbaar zijn voor niet-naleving.

#### *3.2.1.2 Semigestructureerde interviews*

Naast documentstudie zijn semigestructureerde interviews gehouden met verschillende betrokken (senior) managers en deskundigen op het gebied van informatiebeveiliging en privacybescherming[1] voor de ontwikkeling van een nieuw aandachtsgebied. Het voorstel voor de deelnemers betreft personen die op basis van hun rol of functie inzicht hebben in de risico's die een organisatie in de gezondheidszorg loopt op het gebied van informatiebeveiliging en privacy. De keuze voor een semigestructureerd interview ligt in het feit dat bepaalde informatie verkregen moest worden, maar het juist ook mogelijk moest zijn om dieper door te vragen. Hiertoe is op voorhand een interviewprotocol met te stellen open vragen opgesteld wat ruimte geeft om door te vragen (zie bijlage II).

Alle interviews zijn, met toestemming van de geïnterviewde, opgenomen voor verdere analyse.

#### *3.2.1.3 Enquête in combinatie met semigestructureerde interviews*

Voor toetsing van de relevantie en validiteit van de bestaande aandachtsgebieden uit de HAIS-Q is het noodzakelijk te bepalen of alle vragen relevant zijn voor meting van het IBB binnen de gezondheidszorg. Om dit vast te kunnen stellen is gebruik gemaakt van twee methoden, te weten een enquête en een semigestructureerd interview over de resultaten van de enquête.

Met behulp van de enquête kon de deelnemer per vraag uit de originele HAIS-Q aangeven of hij/zij deze vraag 1. Essentieel, 2. Nuttig maar niet essentieel of 3. Niet noodzakelijk vond om op te nemen in een vragenlijst voor het meten van het IBB binnen de gezondheidszorg. Hiertoe zijn alle vragen uit de originele vragenlijst met behulp van een vertaalprogramma naar het Nederlands vertaald en uitgezet in een (niet anonieme) digitale enquête. Het daaropvolgende semigestructureerde interview bood de mogelijkheid om de interpretatie van de vragen door de deelnemer te toetsen, door te vragen op de gegeven antwoorden en extra informatie aangaande de mening van de deelnemer over de vragenlijst op te halen. Hiertoe is op voorhand een interviewprotocol met te stellen open vragen opgesteld wat ruimte geeft om door te vragen (zie bijlage III).

[1] Voorstel voor te interviewen personen is besproken met de informatiebeveiligingsfunctionaris, de functionaris gegevensbescherming en de privacyofficer van de participerende organisatie.

Om een betrouwbare uitspraak te kunnen doen over de vragen in de huidige vragenlijst is de lijst met deelnemers aan de eerste set semigestructureerde interviews uitgebreid met managers die aan gespecialiseerde onderdelen van de operatie leidinggeven[2].

Alle interviews zijn, met toestemming van de geïnterviewde, opgenomen voor verdere analyse.

### 3.2.2 Toetsing validiteit en betrouwbaarheid ontwikkelde HAIS-Q

Het doel van dit onderdeel van het onderzoek is het vaststellen van de validiteit en betrouwbaarheid van de (door)ontwikkelde HAIS-Q. Deze paragraaf beschrijft gedetailleerd op welke wijze de gekozen methoden van onderzoek zijn uitgevoerd.

Om de validiteit van de (door)ontwikkelde HAIS-Q te kunnen toetsen is het noodzakelijk om informatie te vergaren over:

- de inhoudsvaliditeit; is het begrip IBB juist geoperationaliseerd in het meetinstrument?
- de constructvaliditeit; meet het meetinstrument wat het moet meten?

Naast dat het van belang is dat de (door)ontwikkelde HAIS-Q valide is, is het ook van belang te toetsen dat deze betrouwbaar is.

#### *3.2.2.1 Inhoudsvaliditeit*

Binnen dit onderzoek wordt onder IBB de mate waarin de medewerkers van een organisatie het belang en de gevolgen van informatiebeveiliging inzien en de mate waarin zij zich gedragen in overeenstemming met het beleid en de procedures van de organisatie op het gebied van informatiebeveiliging verstaan. Om inhoudsvaliditeit van de HAIS-Q aan te tonen is een juiste operationalisering van dit begrip nodig. Saunders et al. (2016) geven aan dat er drie methoden zijn om vast te stellen of een vragenlijst een begrip adequaat operationaliseert, te weten literatuuronderzoek, spreken van deskundigen en het voorleggen van de vragenlijst aan verschillende individuen en hen te vragen of de vragen essentieel, nuttig maar niet essentieel of niet noodzakelijk zijn. Binnen dit onderzoek zijn alle methoden toegepast. Hierbij moet opgemerkt worden dat eventuele nieuwe onderdelen in de HAIS-Q alleen middels gesprekken met deskundigen geoperationaliseerd worden.

#### *3.2.2.2 Constructvaliditeit*

Saunders et al. (2016) betogen dat deze vorm van validiteit verkregen kan worden door de resultaten van de vragenlijst te vergelijken met eerder onderzoek naar hetzelfde begrip en dit vooral te doen door te kijken naar de correlatie tussen beide onderzoeken. Parsons, McCormac, Butavicius, et al. (2013) hebben bij de constructie van de originele HAIS-Q de constructvaliditeit vastgesteld door middel van cognitieve testen met experts uit het vakgebied van informatiebeveiliging en privacy. Binnen dit onderzoek wordt voor deze methode gekozen, omdat binnen de case-organisatie geen eerder onderzoek beschikbaar is. De experts op het vakgebied kan gevraagd worden of zij denken dat de verschillende subgebieden dekkend zijn voor het aandachtsgebied. De cognitieve test wordt ook afgenomen bij zorgprofessionals omdat hun begrip van de vragenlijst met name belangrijk is. Tijdens de cognitieve test is de (door)ontwikkelde HAIS-Q door de deelnemers ingevuld in bijzijn van de onderzoeker, waarbij de deelnemers hardop hun gedachtegang hebben uitgesproken. Deze manier van testen stelt de onderzoeker in de gelegenheid additionele vragen te stellen als niet duidelijk was hoe de deelnemers de vragen interpreteerden en te vragen naar de duiding van gebruikte begrippen in de vragen.

#### *3.2.2.3 Betrouwbaarheid*

De betrouwbaarheid, ook wel consistentie, van een vragenlijst kan volgens Saunders et al. (2016) met behulp van meerdere methoden worden vastgesteld, te weten:

- Vergelijken van resultaten uit het eigen onderzoek met resultaten uit andere onderzoeken;
- Test – hertest waarbij schattingen van de betrouwbaarheid worden verkregen door resultaten te correleren met die van dezelfde vragenlijst verzameld onder zo gelijk mogelijke omstandigheden;

[2] Voorstel voor te enquêteren en interviewen personen is besproken met de informatiebeveiligingsfunctionaris, de functionaris gegevensbescherming en de privacyofficer van de participerende organisatie.

- Interne consistentie, wat inhoudt dat de antwoorden op vragen in de vragenlijst met elkaar worden gecorreleerd. De meest gebruikte methode hiervoor is Cronbach's alfa.
- Alternatieve vorm, waarbij dezelfde vraag in verschillende vormen wordt gesteld.

Alle bovenstaande methoden gaan ervan uit dat de vragenlijst in ieder geval door een pilotgroep is ingevuld. Hiertoe wordt de (door)ontwikkelde vragenlijst middels een anonieme digitale enquête uitgezet. Deze personen dienen in de praktijk te werken met digitale middelen en bij voorkeur ook toegang te hebben tot privacygevoelige informatie. Binnen de case-organisatie is het niet toegestaan om zorgprofessionals te bevragen in verband met belastbaarheid als gevolg van Corona. Een andere groep die voldoet aan de gestelde criteria is de human resources afdeling. Aan alle 59 medewerkers die hier werkzaam zijn, is een digitale uitnodiging via mail gestuurd.

Binnen dit onderzoek is gebruik gemaakt van twee methoden om de consistentie van de vragenlijst vast te stellen. Ten eerste is de interne consistentie vastgesteld door middel van de berekening van de Cronbach's alfa, omdat dit goed uitvoerbaar is binnen de kaders van het onderzoek. Ten tweede zijn de resultaten van de pilotgroep vergeleken met de resultaten uit andere onderzoeken, omdat deze via literatuuronderzoek makkelijk verkrijgbaar zijn.

De methode test-hertest is niet gebruikt vanwege de beschikbare tijd. De alternatieve vorm is niet toegepast omdat dit de vragenlijst verlengt en daarmee de kans op niet willen invullen vergroot en de groep die deel mag nemen al niet te groot is.

## 3.3 Analyse van de resultaten

Voor het onderzoek zijn 4 verschillende methoden toegepast, welke elk een verschillende wijze van analyse vragen.

Vanuit de documentstudie worden alle relevante documenten gelezen, waarbij ter zake doende artikelen en/of teksten worden overgenomen om te kunnen categoriseren naar relevante aandachtsgebieden die het meest vatbaar zijn voor niet-naleving.

De interviewdata, inclusief de data uit de cognitieve test, zijn op de volgende wijze geanalyseerd:
- Vooraf vaststellen van categorieën en subcategorieën relevant voor het doel van het interview;
- Vanuit de transcriptie van de opname worden relevante uitspraken ingedeeld in de vastgestelde categorieën en subcategorieën. Categorieën kunnen worden aangevuld indien daar noodzaak toe is;
- Op basis van de data per categorie wordt bepaald welke actie dit tot gevolg heeft voor het vervolg van het onderzoek of de samenstelling van de (door)ontwikkelde HAIS-Q.

De uitgezette enquêtes dienen een verschillend doel en zodoende worden de resultaten verschillend geanalyseerd. De eerste enquête is ter toetsing van relevantie en validiteit. De antwoorden krijgen eerst een waarde toegekend, waarna de antwoorden per aandachtsgebied, per vraag en per deelnemer worden getotaliseerd om de antwoorden te kunnen analyseren. Voor analysedoeleinden worden schalen gemaakt die een indicatie geven van de draagkracht voor een vraag. De opmerkingen die deelnemers bij vragen hebben gegeven, worden meegenomen bij de analyse van de interviewdata van het interview wat na het invullen van de enquête is afgenomen.

De resultaten van de uitgezette enquête bij de pilot groep worden statistisch geanalyseerd met behulp van SPSS. Hiertoe worden eerst onvolledig ingevulde enquêtes verwijderd uit de resultaten en worden de resultaten van alle negatief gestelde vragen zo gecodeerd dat de resultaten vergelijkbaar zijn met die van de positief gestelde vragen.

## 3.4 Validiteit en betrouwbaarheid van het onderzoek

De waarde van een onderzoek wordt mede bepaald door de wijze waarop het onderzoek is uitgevoerd, ofwel de validiteit en de betrouwbaarheid van het onderzoek. Beide aspecten worden in deze paragraaf besproken.

### 3.4.1 Interne validiteit onderzoek

Onder interne validiteit kan de mate waarin een test is gebaseerd op goed uitgevoerd onderzoek worden verstaan, onder te verdelen naar statistische validiteit (zijn de statistische analyses juist uitgevoerd en beoordeeld) en causale-interpretatie validiteit (zijn gevonden verbanden juist geïnterpreteerd).

De data die vergaart wordt in de enquête en de pilotstudie is ordinale data, waarop niet alle statistische analyses uitgevoerd kunnen worden. De gekozen statistische methode is gangbaar voor het doel van het onderzoek en toepasbaar op ordinale data.

Ten behoeve van causale-interpretatie validiteit is onder andere bij het opstellen van de interviewvragen aandacht geschonken aan de wijze van vraagstelling en het voorkomen van sociaal wenselijke antwoorden. Bijlagen II en III bevatten de gehanteerde interviewprotocollen en de gestelde vragen.
Ook het gebruik van verschillende onderzoeksmethoden, ofwel methode triangulatie, draagt bij aan deze vorm van validiteit.

### 3.4.2 Externe validiteit onderzoek

Onder externe validiteit wordt de mate waarin de resultaten generaliseerbaar zijn over de algemene populatie verstaan. Het hoofddoel van het onderzoek is de doorontwikkeling en verdere validering van de HAIS-Q, wat inhoudt dat het niet noodzakelijk is de resultaten te generaliseren. De doelstelling is wel een valide en betrouwbaar meetinstrument te ontwikkelen voor de gehele gezondheidszorg. De methode van de enkelvoudige casestudie brengt het risico met zich mee dat dit mogelijk niet het geval is. Het feit dat er binnen dit onderzoek geen toestemming is om zorgprofessionals te betrekken in de pilotstudie kan afdoen aan de mate van bruikbaarheid binnen de gezondheidszorg.

### 3.4.3 Betrouwbaarheid onderzoek

Betrouwbaarheid van het onderzoek kan worden beoordeeld door vast te stellen of het onderzoek consistent is uitgevoerd, bijvoorbeeld door gebruik te maken van meerdere onderzoekers. Omdat dit binnen dit onderzoek niet mogelijk is, kan betrouwbaarheid worden verkregen door alle stappen van het onderzoek vast te leggen, zodat deze controleerbaar zijn. Deze methode zal tijdens dit onderzoek worden toegepast. Betrouwbaarheid kan daarnaast worden verkregen door data vergaring en analysetechnieken zo op te zetten en te beschrijven dat deze herhaalbaar zijn. Dit is in dit onderzoek het geval.

Saunders et al. (2016) geven echter wel aan dat er verschillende risico's zijn die de betrouwbaarheid van het onderzoek kunnen ondermijnen, waaronder:

- Deelnemersfouten; deze kunnen bijvoorbeeld worden veroorzaakt door vragen onjuist of op een onjuist moment te stellen waardoor de manier van reageren van de respondent anders is dan als dezelfde vraag op een andere wijze of ander moment wordt gesteld. Binnen dit onderzoek kan zich dit vooral voordoen binnen het kwalitatieve deel van het onderzoek. Om dit risico te mitigeren is de deelnemers de mogelijkheid geboden zelf aan te geven waar en wanneer zij het interview of de cognitieve test willen laten plaatsvinden.
- Bewust sociaal wenselijk antwoorden; dit kan zich onder andere voordoen bij niet anonieme enquêtes en het houden van interviews in open ruimtes. Binnen dit onderzoek worden enquêtes, die niet gevolgd worden door een interview, anoniem afgenomen en worden interviews in gesloten ruimten afgenomen.
- Onderzoekersfouten; dit betreft alle factoren die zorgdragen voor een verkeerde interpretatie van de onderzoeker. Binnen dit onderzoek worden de gehouden interviews opgenomen en getranscribeerd om zorg te dragen dat bij twijfel de transcriptie nagelezen kan worden op de feitelijke antwoorden.

Een zwak punt binnen het onderzoek is het feit dat het uitgevoerd wordt door één onderzoeker, wat maakt dat maatregelen lastig controleerbaar zijn en vooroordelen van de onderzoeker in de resultaten terecht kunnen komen.

# 4 Uitvoering van het empirisch onderzoek

Binnen dit hoofdstuk is het verloop van het onderzoek beschreven. Tevens is aangegeven welke afwijkingen het onderzoek kent ten opzichte van het originele onderzoek.

## 4.1 Enkelvoudige casestudie

Het doel van het onderzoek is de doorontwikkeling en validatie van de HAIS-Q voor het meten van IBB binnen de gezondheidszorg. Dit maakt dat het voor de hand ligt dat de case, ofwel de organisatie, er één binnen deze branche is. De onderzoeker is werkzaam binnen een topklinisch ziekenhuis in Noordwest Nederland. Binnen deze organisatie is door de onderzoeker bij de Raad van Bestuur toestemming gevraagd het onderzoek uit te voeren, wat het voordeel biedt dat bronnen makkelijker toegankelijk waren. Als gevolg van de coronacrisis is deze toestemming pas gevraagd aan het einde van de 2$^{e}$ golf van de crisis, november 2020. Voor de originele opzet is geen toestemming verkregen omdat dit een te grote belasting zou geven op de al overbelaste zorgprofessional. Zodoende is een andere onderzoeksopzet gekozen die eind november 2020 is voorgelegd. Voor deze opzet is eind januari 2021 toestemming verkregen, waarna gestart is met het onderzoek.

## 4.2 Afwijkingen ten opzichte van het originele onderzoek

Met de uitvoering van de voorbereidende module voor afstuderen was de gedachte om het gevonden meetinstrument voor het meten van IBB uit te breiden met aandachtsgebied privacy, dit nieuwe meetinstrument te valideren om het daarna breed uit te zetten binnen één of meer organisaties in de gezondheidszorg ter toetsing van de hypothesen in het model. Extra element zou zijn om de vragenlijst uit te breiden met individuele en organisatie factoren om te kijken of deze van invloed zijn op het IBB en om het zelf gerapporteerde gedrag te toetsen aan daadwerkelijk gedrag ter toetsing van de betrouwbaarheid. Zoals geschetst in vorige paragraaf is geen toestemming verkregen voor deze opzet.

Binnen de gestelde kaders van de case-organisatie is een nieuwe onderzoeksopzet gekozen, waar meer kwalitatief onderzoek wordt uitgevoerd ten behoeve van de (door)ontwikkeling en validatie van het in de literatuur gevonden meetinstrument. Het aantal interviews is opgehoogd van vier naar 23 en de cognitieve test is ook met zorgprofessionals afgenomen om het instrument extra te valideren. Door deze veranderde opzet kunnen de niet uitgevoerde onderdelen dienen als suggestie voor vervolgonderzoek.

Binnen het uitgevoerde onderzoek zijn minder interviews uitgevoerd dan gepland, omdat potentiële deelnemers niet hebben gereageerd of niet konden deelnemen. De interviews zijn opgenomen, ruw getranscribeerd, gecategoriseerd op basis van beide, waarna analyse heeft plaatsgevonden. Dit wijkt enigszins af van de originele opzet, waarbij categorisering alleen vanuit transcripties zou gebeuren.

De cognitieve test waarmee de constructvaliditeit van de doorontwikkelde HAIS-Q zou moeten worden vastgesteld heeft met name gezorgd voor inhoudsvaliditeit door toetsing op begrip van vragen.

## 4.3 Semigestructureerde interviews

Het onderzoek bevat interviews gehouden voor de ontwikkeling van een nieuw aandachtsgebied binnen het meetinstrument en interviews gehouden voor de validatie van de aandachtsgebieden in het originele meetinstrument.

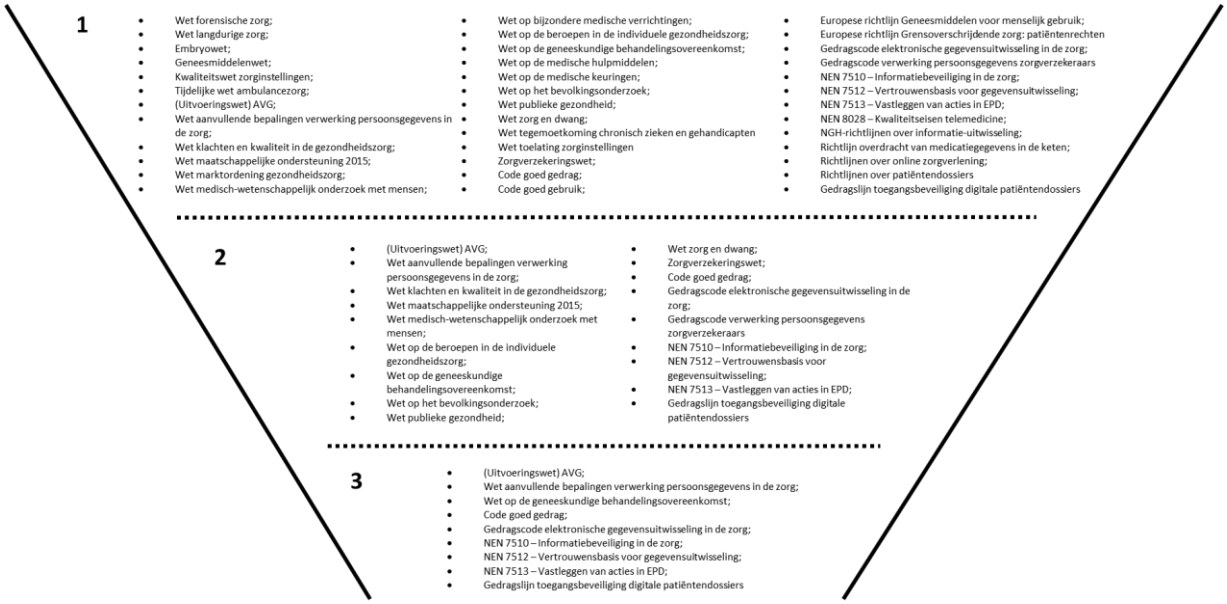
Het voorstel voor de deelnemers betrof vooral personen die op basis van hun rol of functie inzicht hebben in de risico's die een organisatie in de gezondheidszorg loopt op het gebied van informatiebeveiliging en privacy. Alle potentiële deelnemers, tien voor het interview aangaande ontwikkeling en dertien voor het interview aangaande validatie, zijn telefonisch of via mail benaderd met de vraag deel te nemen aan het onderzoek. Alle deelnemers die hebben toegezegd deel te willen nemen, zeven voor ontwikkeling en tien voor validatie, hebben via de mail een afgestemd agendaverzoek ontvangen met informatie over het onderzoek en de interviewopzet (zie bijlage IV). Interviews zijn op afgestemde momenten en locaties afgenomen en van allen is een audio opname en ruwe transcriptie gemaakt voor categorisering van uitspraken en verdere analyse.

## 4.4 Documentstudie

Om te komen tot de documenten die in nader detail bekeken konden worden is vanuit de algemene en sectorspecifieke documenten (laag 1 in onderstaande figuur) teruggewerkt naar documenten die specifieke regels rond informatiebeveiliging en/of bescherming van persoonsgegevens bevatten (laag 2 in onderstaande figuur) en van daaruit, in overleg met experts, naar de te bestuderen documenten (laag 3 in onderstaande figuur).

Bij de selectie is gelet op het feit dat het documenten betreft die voor de gehele branche gelden en dat aan de overige eisen is voldaan.

De documenten komen van de volgende bronnen: Europees Parlement (2016), Ministerie van Justitie en Veiligheid (2018), Ministerie van Justitie (2008), Rijksoverheid (1994), COREON (2005), KNMG and Nictiz (2019), NEN (2017a), NEN (2017b), NEN (2015, 2018), NVZ (2020).




**Figuur 3 Documentenselectie beleidsdocumenten voor documentstudie**

Relevante artikelen uit de documenten zijn ingedeeld in vooraf vastgestelde categorieën die ook gebruikt zijn voor de categorisering van de interviewdata. Indelingen zijn gebruikt voor analyse.

## 4.5 Enquêtes

### 4.5.1 Enquête toetsing validiteit

Voor toetsing op relevantie en validiteit van de originele vragenlijst is de vragenlijst in een enquête uitgezet bij alle deelnemers die hebben toegezegd deel te willen nemen aan het interview ter validatie. Hiertoe zijn de vragen eerst naar het Nederlands vertaald, gebruik makend van een vertaalprogramma van Google. De vragen zijn verwerkt in een digitale enquête met behulp van de tool Limesurvey. Met de uitnodiging voor het interview is de link naar de enquête meegestuurd. Per vraag kon de deelnemer aangeven in hoeverre hij/zij de vraag 1. Essentieel, 2. Nuttig maar niet essentieel of 3. Niet noodzakelijk vond. Het was ook mogelijk om een opmerking bij de vraag te plaatsen. Daarnaast zijn er een tweetal vragen toegevoegd aan de enquête waar de deelnemer wordt gevraagd of de HAIS-Q het IBB meet en of de deelnemer nog aandachtsgebieden heeft gemist. Alvorens het interview is bekeken of de deelnemer de enquête had ingevuld. Indien dit niet het geval was, is telefonisch contact gezocht met de deelnemer.

De enquêteresultaten zijn geëxporteerd naar Excel. Voor het verkrijgen van een gewogen oordeel zijn aan de antwoorden van de ordinale schaal numerieke waarden toegekend om de somscore te kunnen bepalen. Hierbij moet opgemerkt worden dat het toekennen van een metrische schaal aan de ordinale variabele suggereert dat er een gelijke afstand zit tussen de antwoordmogelijkheden, dat is niet het geval. In het navolgende interview zijn onder andere de antwoorden van de deelnemer besproken. De

uiteindelijke resultaten hebben bijgedragen aan de opzet van de uiteindelijke HAIS-Q. De opmerkingen zijn meegenomen in de analyse van de interviewdata.

### 4.5.2 Enquête pilotgroep

Na analyse van de interviewdata en de data uit de eerste enquête is een nieuwe HAIS-Q opgesteld. Hierin is het onderwerp privacy toegevoegd in een vergelijkbare opzet als de overige vragen. Ook zijn verschillende subgebieden vervangen of zijn vragen binnen de subgebieden anders geformuleerd. De digitale enquête is gemaakt met de tool Limesurvey, waarbij elke vraag gescoord kon worden op een 5-punts Likert-schaal, van helemaal mee oneens tot helemaal mee eens. Voor de gehele enquête is, op basis van de resultaten uit de interviews en eerdere enquêtes, een andere vormgeving gekozen en is contextinformatie toegevoegd op verschillende niveaus. Het onderzoek van Wissen (2017) geeft aan dat dit de validiteit van het onderzoek verhoogt. Ook zijn een tweetal optionele persoonlijke vragen toegevoegd en feedbackvragen aangaande de enquête. De deelnemers, alle 59 medewerkers van de afdeling Human Resources (hierna: HR), zijn twee weken voorafgaand aan de enquête op de hoogte gesteld van de enquête via een generieke mail van de HR manager waarin iets beschreven is over het onderzoek, de doelstelling en het moment van uitzetten. Daarna is aan de populatie, eveneens via mail, een link naar de enquête gestuurd met extra informatie over onder andere duur van invullen en doorlooptijd van uitzetten, te weten twee weken. Er is nadrukkelijk aangegeven dat de enquête anoniem wordt afgenomen en dat invullen vrijwillig is. Na één week en drie dagen voor afloop zijn reminders gestuurd naar de deelnemers. In het digitale werkoverleg van het HR-team, halverwege de doorlooptijd, is nogmaals aandacht gevraagd voor de enquête.

De resultaten zijn verwerkt in SPSS. Hiertoe zijn onvolledig ingevulde enquêtes uit de resultaten verwijderd. De antwoorden zijn gemeten op een Likert-schaal wat een ordinale schaal is. Om statistische analyses en berekeningen uit te kunnen voeren, worden de antwoorden omgezet naar numerieke waarden van 1 voor totaal mee oneens tot en met 5 voor totaal mee eens. Hierbij moet opgemerkt worden dat het toekennen van een metrische schaal aan de ordinale variabele suggereert dat er een gelijke afstand zit tussen de antwoordmogelijkheden, dat is niet het geval. Het is wel algemeen aanvaard om met antwoorden op Likert-schalen te rekenen als ware hij van een interval of ratio schaal.
De negatief gestelde vragen zijn gehercodeerd om vergelijkbare resultaten te krijgen met de positief gestelde vragen, waarbij 5 de meest positieve uitkomst is.

Voor analyse van de HAIS-Q vragen is gebruik gemaakt van dezelfde analysemethodieken als in andere onderzoeken (Parsons et al., 2017; Parsons, McCormac, Butavicius, et al., 2013; Parsons et al., 2014; Schaeken, 2018; Wissen, 2017), te weten de betrouwbaarheidsanalyse door bepaling van Cronbach's alfa. De resultaten van Cronbach's alfa uit dit onderzoek zijn vergeleken met andere onderzoeken. Voor de feedbackvragen is gekeken naar de frequentie en het gemiddelde.

## 4.6 Cognitieve test

Voor de cognitieve test zijn de privacyofficer en informatiebeveiligingsfunctionaris benaderd. Daarnaast zijn twee zorgprofessionals gevraagd, werkzaam binnen de case-organisatie en bekend in het netwerk van de onderzoeker. Alle potentiële deelnemers zijn persoonlijk benaderd voor deelname en hebben allen toegezegd. De uitnodiging is vervolgens via outlook verstuurd tezamen met een informatieblad met meer informatie over het onderzoek en de test (zie bijlage IV). De cognitieve testen zijn op afgestemde momenten en locaties in persoon afgenomen, waarbij er een audio opname is gemaakt van de test voor analyse doeleinden. Daarnaast is door de onderzoeker ten tijde van de afname per vraag bijgehouden in een Excel bestand welke interpretatie van begrippen en vragen de deelnemer had. Voor afname van de cognitieve test is gebruik gemaakt van dezelfde enquête als degene die is uitgezet bij de pilotgroep. Voor de doelstelling van de cognitieve test is met name de opname en het bijgehouden Excel bestand belangrijk. De ingevulde enquêteresultaten zijn daarnaast gebruikt binnen de analyse van de enquêtes van de pilotgroep, herkenbaar aan de functie die afwijkt van de pilotgroep.

# 5 Resultaten

Om antwoord te geven op de onderzoeksvraag is empirisch onderzoek uitgevoerd. In de navolgende paragrafen worden de resultaten van het uitgevoerde empirisch onderzoek beschreven.

## 5.1 Ontwikkeling nieuwe en toetsing bestaande aandachtsgebieden HAIS-Q

Binnen deze paragraaf worden resultaten besproken van de uitgevoerde onderzoeken die uiteindelijk hebben geleid tot beantwoording van de volgende onderzoeksvraag:

***Hoe ziet de uiteindelijke methode voor het meten van IBB van medewerkers binnen de gezondheidszorg eruit?***

De methode voor het meten van IBB is gelijkwaardig aan de gevonden methode in de literatuurstudie, waarbij de HAIS-Q is aangevuld en aangepast als gevolg van de gevonden resultaten. De doorontwikkelde HAIS-Q is opgenomen in bijlage VII.

### 5.1.1 Nieuwe aandachtsgebieden in de HAIS-Q

Zowel vanuit de documentstudie als vanuit de interviews is grondslag gevonden om het aandachtsgebied 'omgang met privacygevoelige gegevens' toe te voegen[3]. Dit aandachtsgebied kon vervolgens op basis van onderzoeksresultaten geoperationaliseerd worden naar vier subgebieden om het IBB op dit aandachtsgebied te meten. De subgebieden worden onderstaand toegelicht op basis van de resultaten.

***Subgebied: Privacygevoelige gegevensverzamelingen buiten de applicaties***

De documentstudie heeft aangetoond dat het gebruik van privacygevoelige data voor studie, werk of onderzoek is toegestaan, mits dit voor gerechtvaardigde doeleinden gebeurt en een passende beveiliging gewaarborgd is.

> *"Deze wet en de daarop berustende bepalingen zijn van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen."(Ministerie van Justitie en Veiligheid, 2018)*

> *"Er zijn allerlei soorten informatie waarvan de beschikbaarheid, integriteit en vertrouwelijkheid beschermd behoren te worden:*
> *a) persoonlijke gezondheidsinformatie;*
> *b) gepseudonimiseerde gegevens die, via een methodiek voor pseudonieme identificatie, aan persoonlijke gezondheidsinformatie worden ontleend;*
> *c) statistische en onderzoeksgegevens, waaronder geanonimiseerde gegevens, die aan persoonlijke gezondheidsinformatie worden ontleend, door persoonlijke identificatiegegevens weg te halen;" (NEN, 2017a)*

Interviews met experts en management geven aan dat de omgang met gegevensverzamelingen buiten de applicatie lang niet altijd gebeurt conform beleid en richtlijnen. Daarnaast zijn medewerkers zich niet altijd bewust zijn van de geldende regels en hun afwijking hierop. Dit maakt dit een legitiem subgebied.

> *"Ik heb een set aan gevoelige data uit een applicatie gehaald en wat mag ik daarmee? Er wordt heel veel informatie uit applicaties gehaald."*

> *"…., omdat ik van collega's heb gezien dat zij gegevens naar hun privé mailadres sturen en het daar dan opslaan."*

***Subgebied: Privacygevoelige informatie afdrukken***

Binnen de NEN 7510-2 wordt gesproken over informatie labelen en expliciet over het labelen van papieren output als vertrouwelijk als deze persoonlijke gezondheidsinformatie bevat (NEN, 2017b). Hier

[3] In deze paragraaf worden verschillende citaten uit documenten (met bronvermelding) en interviews weergegeven om de resultaten te onderbouwen.

zit een duidelijk risico op niet-naleving als gevolg van menselijk gedrag. Dit zit niet zozeer in de labeling, maar wel in de omgang met de output die passend bij de labeling zou zijn. Tijdens de interviews wordt regelmatig aangegeven dat medewerkers uit oogpunt van gemak 'looplijstjes' afdrukken waarop patiënt informatie staat, terwijl zij ook een tablet of 'computer on wheels' (hierna: COW) ter beschikking hebben. De omgang van personeel met deze lijstjes geschiedt niet altijd conform beleid wat onderstaande citaten bevestigen.

*"Er worden briefjes afgedrukt met allerlei gegevens en die blijven slingeren. Dat kan natuurlijk niet en daar moet een ICT-oplossing voor komen. Daar is nu een COW voor en voor specialisten is er een app. Die wordt niet door iedereen gebruikt en sommige specialisten willen een lijstje hebben. Ze gebruiken die niet omdat het ziekenhuis dan beheerder van jouw telefoon wordt. Sommige mensen vinden dat niet prettig."*

*"Gebruik van looplijstjes waar veel privacygevoelige patiëntgegevens op staan i.p.v. registratie en raadplegen aan de bron."*

Bovenstaande maakt duidelijk dat hier een risico op niet-naleving is, waarbij de mens een rol speelt en het dus interessant maakt om het bewustzijn op te peilen.

***Subgebied: In publieke gelegenheden praten over patiënten en/of medewerkers***

Resultaten laten zien dat veel informatie ook buiten systemen om wordt gedeeld. Hierover is in de NEN 7510-2 de volgende norm over opgenomen:

*"Bovendien behoort personeel eraan te worden herinnerd dat ze geen vertrouwelijke gesprekken voeren in openbare gebieden of via onbeveiligde communicatiekanalen, in open kantoren en op vergaderlocaties." (NEN, 2017b)*

Geïnterviewden geven aan het bespreken van patiënten of medewerkers zeker niet altijd in de beslotenheid van een (afgesloten) kantoor plaatsvindt. Zij hebben hier ook persoonlijke ervaringen mee.

*"Praten met collega's over patiënten als ze net een dienst hebben afgesloten, op welke locatie dan ook."*

*"Visites lopen op meer persoons zalen zorgt er ook voor dat anderen informatie meekrijgen die niet voor hen bestemd is."*

Duidelijk is dat het praten in publiekelijke gelegenheden over patiënten en/of collega's een risico is op privacyschending. Het risico op voordoen zit dan ook vooral bij de medewerkers.

***Subgebied: Inzien van persoonsgegevens van patiënten en/of medewerkers***

Organisaties in de gezondheidszorg beschikken over bijzondere persoonsgegevens (Ministerie van Justitie en Veiligheid, 2018), te weten gezondheidsinformatie over personen. Zowel de WGBO als de NEN 7510-2 bevatten dan ook extra regels over de toegang tot deze informatie.

*"Onverminderd het in artikel 448 lid 3, tweede volzin, bepaalde draagt de hulpverlener zorg, dat aan anderen dan de patiënt geen inlichtingen over de patiënt dan wel inzage in of afschrift van de bescheiden, bedoeld in artikel 454, worden verstrekt dan met toestemming van de patiënt."(Rijksoverheid, 1994)*

*"Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren de toegang tot dergelijke informatie te controleren. In het algemeen behoren de gebruikers van gezondheidsinformatiesystemen hun toegang tot persoonlijke gezondheidsinformatie te beperken tot situaties:*
*a) waarin er een zorgrelatie bestaat tussen de gebruiker en de persoon waarop de gegevens betrekking hebben (de cliënt tot wiens persoonlijke gezondheidsinformatie er toegang wordt gemaakt);*
*b) waarin de gebruiker een activiteit uitvoert namens de persoon waarop de gegevens betrekking hebben;*

*c) waarin er specifieke gegevens nodig zijn om deze activiteit te ondersteunen." (NEN, 2017b)*

Binnen de inregeling van maatregelen wordt autorisatie technisch ingeregeld. Procedureel kan een medewerker om de autorisatie heen door gebruik te maken van de 'breaking-the-glass' procedure. Het juist gebruik maken van deze procedure komt altijd neer op de integriteit van de medewerker. Dit maakt het een legitiem onderwerp voor het meten van het bewustzijn. Geïnterviewden onderschrijven dit.

> "Het onderwerp privacy kun je duiden naar bijvoorbeeld het delen van privacy gevoelige gegevens of het raadplegen van gegevens waar je niets mee nodig hebt. Deze onderwerpen zitten er niet in."

> "Er wordt wel eens gekeken als het een bekende betreft, hier wordt ook wel op opgetreden. Er wordt veel over gesproken wanneer het wel en niet mag. Voorbeelden wat niet mag is bijvoorbeeld als de politie of de verzekering komt vragen. En er wordt erg op gehamerd dat het niet mag als de patiënt geen toestemming heeft gegeven. Bij doctoren hoort hij het eigenlijk niet, wel van ander personeel. Doktoren kunnen het wellicht ook beter uitleggen waarom zij in een dossier kijken waar ze niet direct toegang toe hebben."

### 5.1.2 Toetsing relevantie en validiteit bestaande aandachtsgebieden

Zowel de documentstudie als de enquête met opvolgende interviews bevestigen het belang van de bestaande aandachtsgebieden in de HAIS-Q. Uit de enquête en de interviews komt wel naar voren dat sommige aandachtsgebieden beter geoperationaliseerd kunnen worden met andere subgebieden of met andere nuances in de vraagstellingen.

Van de relevante documenten is met name binnen de NEN7510-2 een grondslag te vinden voor alle aandachtsgebieden van de HAIS-Q. Naast de genoemde richtlijnen, worden in dit document ook daadwerkelijke bedreigingen voor de beveiliging van gezondheidsinformatie beschreven. Hier zijn ook aanknopingspunten te vinden voor mogelijke aanpassingen van bestaande subgebieden. Reden hiervoor is dat veel informatie heden ten dage digitaal is en in mindere mate analoog. Daarnaast zijn veel zorginstellingen openbaar toegankelijke organisaties waar iedereen binnen kan stappen. Een voorbeeld hiervan is de volgende tekst uit bijlage A van de NEN7510-2:

> *"Het kan verrassend eenvoudig zijn om onbevoegd toegang te krijgen tot een gezondheidsinformatietoepassing, bijvoorbeeld door een cliënt die naar een verlaten werkstation in het kantoor van een arts loopt en het scherm bekijkt."*

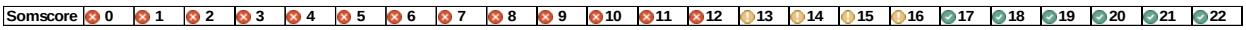
Naast de documentstudie is de originele HAIS-Q vertaald en middels een digitale enquête voorgelegd aan 11 deskundigen in de caseorganisatie. Zij konden per vraag aangeven of zij deze essentieel, nuttig maar niet essentieel of niet noodzakelijk vinden voor het meten van het IBB binnen de gezondheidszorg. De vertaalde versie van de originele HAIS-Q is opgenomen in bijlage V.

De antwoorden betreffen ordinale data die vervolgens gecodeerd zijn met een numerieke waarde om de somscore te kunnen bepalen en op basis daarvan systematisch inzichtelijk te kunnen maken hoe elke vraag scoort, vergelijkbaar met het onderzoek van Wissen (2017). Hierbij moet opgemerkt worden dat het toekennen van een metrische schaal aan de ordinale variabele suggereert dat er een gelijke afstand zit tussen de antwoordmogelijkheden, dat is niet het geval.

De volgende numerieke waarden zijn toegekend aan de antwoordmogelijkheden:

2 – Essentieel
1 – Nuttig, maar niet essentieel
0 – Niet noodzakelijk

Per vraag is een somscore berekend (minimum 0, maximum 22). Deze zijn ingedeeld in drie deelgebieden om een indicatie te krijgen van de relevantie en validiteit van een vraag binnen een sub aandachtsgebied, een sub aandachtsgebied en een aandachtsgebied. De deelgebieden komen overeen met de antwoordmogelijkheden en hebben ter visualisatie een kleur gekregen, groen voor essentieel, geel voor nuttig maar niet essentieel en rood voor niet noodzakelijk, zoals in onderstaande figuur weergegeven.



Figuur 4 Indeling somscores

In bijlage VI zijn de resultaten per respondent per vraag weergegeven. De respondenten zijn geanonimiseerd door het toekennen van een letter. In onderstaande figuur is een samenvatting van de resultaten per aandachtsgebied uit de HAIS-Q weergegeven. Hierbij staan de vragen op de horizontale as, waarbij zij zijn weergegeven als een Xn, waarbij de X staat voor de letter van één van de dimensies kennis, houding of gedrag. De n staat voor het nummer van het subgebied binnen het aandachtsgebied.

| Vraag | K1 | H1 | G1 | K2 | H2 | G2 | K3 | H3 | G3 |
|---|---|---|---|---|---|---|---|---|---|
| **Aandachtsgebied** | | | | | | | | | |
| *Wachtwoordmanagement* | 17 | 18 | 17 | 18 | 17 | 21 | 16 | 14 | 19 |
| *eMail gebruik* | 15 | 19 | 14 | 19 | 18 | 18 | 17 | 21 | 22 |
| *Internetgebruik* | 19 | 20 | 17 | 15 | 20 | 18 | 21 | 16 | 19 |
| *Sociale Media* | 17 | 16 | 13 | 15 | 12 | 22 | 21 | 19 | 19 |
| *Mobiele apparaten* | 19 | 14 | 14 | 21 | 19 | 20 | 18 | 20 | 20 |
| *Informatieverwerking* | 17 | 17 | 21 | 19 | 18 | 17 | 17 | 19 | 18 |
| *Melden incidenten* | 20 | 15 | 21 | 18 | 15 | 19 | 16 | 16 | 21 |

Figuur 5 Somscores enquête validiteit met experts en management

De meeste vragen worden essentieel gevonden, waarbij gedragsvragen het meeste en houdingsvragen het minste draagvlak kennen. De respondenten gaven aan dat zij het onderscheid in dimensies in de vraagstellingen niet altijd hebben begrepen. Zij geven aan dat dit ook komt doordat zij de toelichting bij de enquête onvoldoende hebben gelezen. Ook werd uit de vraagstelling in de enquête het onderscheid tussen de vragen niet duidelijk, wel werd opgemerkt dat vragen op elkaar leken. Na nadere uitleg van het model werd de opzet van de dimensies als waardevol bestempeld.

Binnen de aandachtsgebieden hebben vooral 'Internetgebruik' en 'Informatieverwerking' veel draagvlak. Voor het aandachtsgebied 'Internetgebruik' kunnen de vragen uit de originele HAIS-Q onaangepast blijven bestaan. Uit de interviews is naar voren gekomen dat de vragen binnen het aandachtsgebied 'Informatieverwerking' goed zijn, maar wel duiding van begrippen en uitbreiding nodig hebben. Geïnterviewden geven vooral aan dat naast 'clean desk' ook 'clear screen' een hardnekkig probleem is.

> "Sinds we geen statussen meer hebben is er niets wat zichtbaar is en zit alles wel achter slot en grendel, maar als de computer open staat is alles zichtbaar."

Verder wordt aangegeven dat binnen het onderzochte ziekenhuis het technisch vaak niet mogelijk is om een USB-stick te gebruiken, maar dat men wel verwacht dat dit binnen de gezondheidszorg in het algemeen anders is en daarom zeer relevant.

Het aandachtsgebied 'Sociale media' wordt minder noodzakelijk gevonden. Dit komt voornamelijk door de scores bij de subgebieden 'privacy instellingen' en 'rekening houden met de gevolgen'. In de interviews komt niet een duidelijke reden naar voren waarom hier een lagere relevantie aan wordt toegekend.

Vanwege het technisch goed kunnen afdwingen van een sterk wachtwoord, wordt het subgebied 'gebruik van een sterk wachtwoord' binnen het aandachtsgebied 'Wachtwoordmanagement' minder belangrijk gevonden. Daarentegen wordt het vastleggen van wachtwoorden op blaadjes gemist, net als het delen van andere authenticatiemiddelen.

> "Er zijn nog steeds artsen die inlognamen en wachtwoorden op een blaadje op hun PC hebben staan."

De respondenten geven verder aan dat zij het subgebied 'klikken op links van bekenden' in het aandachtsgebied 'eMail gebruik' minder relevant vinden. Tijdens de interviews wordt aangegeven dat dit onderwerp al zo vaak is behandeld, dat de verwachting bestaat dat hier een goede score op zal komen en het daarom minder relevant is dit te meten. Het subgebied 'fysieke beveiliging van mobiele apparaten' binnen het aandachtsgebied 'Mobiele apparaten' wordt als minder relevant ervaren. Reden hiervoor is dat het gros van de medewerkers binnen de onderzochte organisatie niet beschikt over een laptop. Wel wordt erkend dat er meer en meer gebruik gemaakt wordt van tablets en apps op telefoons.

Een aantal van de geïnterviewden vindt dat de vragen in de vragenlijst context missen en hier en daar suggestief zijn en kunnen leiden tot sociaal wenselijk antwoorden. Ook verwachten zij dat niet alle vragen voor alle medewerkers van toepassing zijn. Unaniem werd aangegeven dat het invullen van de vragenlijst het bewustzijn op dat moment al verhoogd, wat dan ook als een sterk punt werd gezien. Ook zijn zij allen van mening dat de vragenlijst een adequaat beeld zal geven van het IBB.

Bij de ontwikkeling van de nieuwe HAIS-Q is zoveel als mogelijk rekening gehouden met de opmerkingen van respondenten die ook ondersteund worden door eerder onderzoek van Wissen (2017).

## 5.2 Toetsing validiteit en betrouwbaarheid ontwikkelde HAIS-Q

Binnen deze paragraaf worden resultaten besproken van de uitgevoerde onderzoeken die uiteindelijk hebben geleid tot beantwoording van de volgende onderzoeksvraag:

***In hoeverre is de uiteindelijke methode voor het meten van IBB valide en betrouwbaar?***

De voor beantwoording van deze deelvraag uitgevoerde cognitieve test en pilottest hebben parallel aan elkaar plaatsgevonden met de doorontwikkelde HAIS-Q. Resultaten van de onderzoeken laten zien dat de doorontwikkelde HAIS-Q valide en betrouwbaar is. Extra onderzoek met verschillende methode kan bijdragen aan de bruikbaarheid van het nieuw ontwikkelde meetinstrument.

### 5.2.1 Validiteit

Uit literatuuronderzoek is gebleken dat de oorspronkelijke HAIS-Q een valide meetinstrument is. Daarnaast is deze vragenlijst voorgelegd aan deskundigen die hebben aangegeven of zij de vragen essentieel, nuttig maar niet essentieel of niet noodzakelijk zijn. Hun antwoorden zijn vervolgens met hen besproken. De resultaten hiervan zijn uitgebreid besproken in paragraaf 5.1.2. De verwijdering en toevoeging van subgebieden zijn overgenomen uit onderzoek van Schaeken (2018), die deze heeft getoetst op validiteit en valide bevonden. De overige gedane aanpassingen aan de vragenlijst betreffen tekstuele aanpassingen in bestaande vragen om het begrip te vergroten.

Op basis van uitgevoerd onderzoek, zoals beschreven in paragraaf 5.1, is een nieuw aandachtsgebied met subgebieden toegevoegd aan de HAIS-Q. Om de validiteit van de nieuwe HAIS-Q te toetsen is een cognitieve test uitgevoerd met twee zorgprofessionals en twee experts op het gebied van informatieveiligheid en privacy.

Het afnemen van een cognitieve test is zowel voor onderzoeker als voor de deelnemers nieuw. De deelnemers hebben in eerste instantie moeite om niet direct hun mening te geven over de inhoud van de vraag of om hun gedrag te vertellen in plaats van in te gaan op hun opvatting van de vraag. De onderzoeker heeft in mindere mate de gelegenheid genomen om te toetsen of de subgebieden in voldoende mate de aandachtsgebieden operationaliseren, ofwel meten zij het construct. Bij de interviews aangaande de ontwikkeling is dit wel ter sprake gekomen, zoals beschreven in paragraaf 5.1.

Ondanks de repeterende indeling van de vragen, begeleid met voorbeeldvragen, geven de deelnemers aan dat het zou helpen als per vraag de dimensie wordt opgenomen. Daarnaast wordt het als lastig ervaren dat vragen negatief gesteld worden of een dubbele ontkenning bevatten.

Vragen die onduidelijk zijn of niet juist geïnterpreteerd worden, bevatten vaak bijvoeglijk naamwoorden die voor meerdere uitleg vatbaar zijn, zoals ‘slechts’, ‘riskant’, ‘openbare’ of ‘gevoelige’; zes vragen. Daarnaast worden vragen die onbepaalde bijwoorden bevatten zoals ‘altijd’ of ‘nooit’ als te stellig ervaren en dan ook als zodanig ingevuld, daar waar bij sommige vragen eigenlijk naar een nuance wordt gevraagd; drie vragen. Dit kan dus leiden tot onjuiste interpretatie en onjuist antwoorden. Ook het gebruik van onbepaalde voornaamwoorden zoals ‘bepaalde’ kan leiden tot onjuiste interpretatie van de vraag; één vraag. Bij verschillende vragen is (technische) kennis of contextinformatie nodig om een juist begrip te hebben van de vraag, bijvoorbeeld ‘openbaar wifi netwerk’, ‘privacygevoelige gegevensverzameling’ of ‘buiten de applicatie’; tien vragen. 55 van de 75 vragen worden door de deelnemers juist geïnterpreteerd.

Bij vragen binnen de dimensie gedrag wordt het als prettig ervaren dat die beginnen met het woord 'ik', omdat daardoor direct de vertaling naar het eigen gedrag wordt gemaakt.

De ontwikkelde vragenlijst biedt nog ruimte voor verbetering op het gebied van de validiteit. De resultaten geven met name aanknopingspunten voor een verdere verhoging van de inhoudsvaliditeit. In lijn met de resultaten van Wissen (2017) zal het verder toevoegen van context bijdragen aan de validiteit. De resultaten geven onvoldoende uitsluitsel over de constructvaliditeit. Deze zou in vervolgonderzoek nader bekeken kunnen worden.

### 5.2.2 Betrouwbaarheid

Voor het toetsen van de betrouwbaarheid van de vragenlijst is de vragenlijst uitgezet bij een pilotgroep binnen de case-organisatie. De respons is 66,6 % met 42 valide responsen van de 63 uitgezette.

Om de interne consistentie van de vragenlijst te bepalen is de Cronbach's alfa berekend voor de totale lijst, per aandachtsgebied en per dimensie. De Cronbach's alfa kan een waarde hebben van negatief oneindig tot maximaal 1, waarbij de hoogte van de waarde afhankelijk is van de correlatie tussen de antwoordscores. Veel statistici suggereren dat alfa's in het bereik van 0,65 tot 0,80 acceptabel zijn (Vaske, Beaman, & Sponarski, 2017).

De resultaten van dit onderzoek zijn vergeleken met die van verschillende andere onderzoeken en zijn weergegeven in onderstaande tabel.

**Tabel 1 Cronbach's alfa scores verschillende onderzoeken**

| | **Onderhavig onderzoek** | **Parsons, McCormac, Butavicius, et al. (2013)** | **McCormac et al. (2016)** | | **Parsons et al. (2017)** | **Wissen (2017)** | **Schaeken (2018)** |
|---|---|---|---|---|---|---|---|
| | | | **T1** | **T2** | | | |
| **# Deelnemers** | 42 | 113 | 197 | | 505 | 58 | 27 |
| **Totaal IBB** | 0,908 | - | 0,96 | 0,96 | | 0,86 | 0,90 |
| **Aandachtsgebieden** | | | | | | | |
| *Wachtwoord management* | 0,679 | - | 0,83 | 0,84 | 0,82 | 0,60 | - |
| *eMail gebruik* | 0,602 | - | 0,77 | 0,81 | 0,78 | 0,70 | - |
| *Internetgebruik* | 0,698 | - | 0,79 | 0,80 | 0,78 | 0,69 | - |
| *Social media gebruik* | 0,621 | - | 0,75 | 0,78 | 0,75 | 0,70 | - |
| *Mobiele apparaten* | 0,556 | - | 0,83 | 0,82 | 0,71 | 0,69 | - |
| *Informatieverwerking* | 0,679 | - | 0,76 | 0,79 | 0,79 | 0,59 | - |
| *Melden van incidenten* | 0,832 | - | 0,78 | 0,78 | 0,79 | 0,66 | - |
| *Omgang met privacygevoelige gegevens* | 0,676 | - | - | - | - | - | - |
| **Dimensies** | | | | | | | |
| *Kennis van beleid en procedures* | 0,808 | 0,875 | 0,84 | 0,86 | - | - | 0,77 |
| *Houding tov beleid en procedures* | 0,765 | 0,878 | 0,93 | 0,92 | - | - | 0,73 |
| *Zelf gerapporteerd gedrag* | 0,733 | 0,906 | 0,90 | 0,91 | - | - | 0,72 |

De resultaten voor het totaal van het IBB zijn vergelijkbaar met overige onderzoeken. Op de diverse aandachtsgebieden en dimensies zijn de resultaten over het algemeen lager dan die van onderzoeken van de groep die het model heeft gecreëerd, maar wel vergelijkbaar met die van de onderzoeken van Wissen (2017) en Schaeken (2018).

Binnen dit onderzoek is de Cronbach's alfa voor de bestaande aandachtsgebieden 'eMail gebruik', 'Social Media gebruik' en 'Mobiele apparaten' relatief laag. Een lagere Cronbach's alfa kan mogelijk veroorzaakt worden door de grootte van de steekproef. Hoe kleiner de steekproef, hoe groter het effect van een onjuist geïnterpreteerde vraag. De score in de kolom 'Corrected Item-Total Correlation' (zeer laag of negatief) in relatie met de score in de kolom 'Conbach's Alpha if Item Deleted' (hoger dan de huidige Cronbach alfa) kan een indicatie zijn van eventueel onjuist geïnterpreteerde vragen of een onjuiste poling van een vraag. Binnen de aandachtsgebieden 'Social Media gebruik' en 'Mobiele apparaten' komen vragen voor met een negatieve score in de kolom 'Corrected Item-Total Correlation', respectievelijk -0,05

en -0,440 in combinatie met een hogere 'Conbach's Alpha if Item Deleted', respectievelijk 0,705 en 0,772. Dit zou kunnen komen door een inconsistente poling van de vragen, de grootte van de steekproef of onjuiste interpretatie van de vraag waarom inconsistentie aanwezig lijkt. Ook kan het zo zijn dat de vraag niet bijdraagt aan het construct. Dit zou in vervolgonderzoek nader onderzocht kunnen worden.

De score van Cronbach's alfa voor het nieuw ontwikkelde aandachtsgebied 'Omgang met privacygevoelige gegevens' heeft een waarde van 0,676 wat net binnen de acceptabele grenzen is. De grootte van de steekproef kan mede bijdragen aan de relatief lage waarde. Binnen de resultaten laat de vraag 'Als ik over patiënten of medewerkers praat, let ik op waar ik ben en doe ik dat altijd anoniem' een lage 'Corrected Item-Total Correlation' (0,062) in combinatie met een 'Conbach's Alpha if Item Deleted' van 0,688. Ook dit kan duiden op een inconsistente poling van de vraag, maar zou ook veroorzaakt kunnen worden door een onjuiste interpretatie van de vraag door een deel van de steekproefpopulatie. Vanuit de cognitieve test is naar voren gekomen dat het gebruik van verschillende woorden kan leiden tot een onjuiste interpretatie, dit geldt ook voor deze vraag.

## 5.3 Ervaring van respondenten

Naast de vragen om het IBB te meten zijn ook vragen gesteld om feedback over de HAIS-Q op te halen, mede om te bepalen wat de kwaliteit en invulbereidheid is. Voor elk van de gestelde vragen is de frequentie per mogelijk antwoord bepaald en het gemiddelde.

De antwoordmogelijkheden waren bij elke vraag gelijk, te weten:
1 – Helemaal mee oneens
2 - Mee oneens
3 – Nog mee oneens, nog mee eens
4 – Mee eens
5 – Helemaal mee eens

### 5.3.1 Invultijd

De respondenten is de vraag gesteld: 'De tijd die het mij heeft gekost deze enquête in te vullen is acceptabel.' Uit de gemiddelde score van 4,14 kan afgeleid worden dat de tijd inderdaad acceptabel is.

Bij de welkomsttekst van de enquête is aangegeven dat het invullen 20 tot 30 minuten van hun tijd zou vragen. De gemiddelde daadwerkelijke invultijd is 22,2 minuten. Hierbij zijn de tijdscores van de deelnemers die de cognitieve test hebben ingevuld verwijderd. Daarnaast is een outlier van 272 minuten verwijderd, omdat dit lijkt te zijn ontstaan door tussentijds onderbreken van het invullen.

De overeenkomst tussen de gemiddelde invultijd en de vooraf aangegeven invultijd kan een reden zijn waarom de respondenten de invultijd acceptabel vinden. De laagste antwoordwaarde is 3, welke door 3 respondenten is ingevuld. Alle overige respondenten scoren een 4 of een 5.

### 5.3.2 Aantal vragen

De respondenten is de vraag gesteld: "Het aantal vragen in deze enquête is acceptabel." De gemiddelde score is 4,19 waaruit afgeleid kan worden dat het aantal vragen inderdaad acceptabel is. Eén respondent scoort een 2 en één respondent scoort een 3, de overige 40 scoren een 4 of 5.

### 5.3.3 Duidelijkheid vragen

De respondenten is de vraag gesteld: "Alle vragen uit de enquête waren duidelijk voor mij". Hier is het gemiddelde lager dan bij de vorige feedback vragen, namelijk 3,95. De frequentie is als volgt verdeeld:

| | |
|---|---|
| 1 – Helemaal mee oneens | → 0 respondenten |
| 2 – Mee oneens | → 3 respondenten |
| 3 – Noch mee oneens, noch mee eens | → 2 respondenten |
| 4 – Mee eens | → 31 respondenten |
| 5 – Helemaal mee eens | → 6 respondenten |

Het volgende feedback commentaar geeft hier ook wat duiding aan: *"Bij de vraag of je over anderen in de openbare ruimte mag praten was niet helemaal duidelijk wie er anoniem bleef. Werd bedoeld dat degene over wie je praatte anoniem bleef (zo heb ik de vraag geïnterpreteerd) of werd bedoeld dat je zelf anoniem bleef?"*

Deze resultaten zijn in lijn met de resultaten van de cognitieve test, waar ook onduidelijkheden zijn geconstateerd.

### 5.3.4 Toepasselijkheid vragen

De respondenten is de vraag gesteld: "Alle vragen uit de enquête waren op mij van toepassing". Uit het gemiddelde van 3,59 kan worden afgeleid dat dit niet altijd het geval is. Tien respondenten geven aan dat zij het hiermee oneens waren en 6 waren het er noch mee oneens, noch mee eens. Van de overige 26 respondenten waren zeventien het eens met de stelling en negen het helemaal eens. Deze bevindingen sluiten aan bij het onderzoek van Wissen (2017).

# 6 Discussie, conclusies en aanbevelingen

## 6.1 Discussie en reflectie

Door de verdergaande digitalisering wordt de impact van niet-naleving van informatiebeveiligingsbeleid steeds groter. Zodoende willen organisaties beter grip krijgen op de factoren die dit beïnvloeden. Vele onderzoeken hebben aangetoond dat het IBB één van die factoren is. Dit maakt het onderzoek naar de status van dat IBB meer en meer interessant en dit onderzoek neemt ook toe. Methodieken zijn schaars. De HAIS-Q behoort tot één van de vaker onderzochte methodieken. Veel van deze onderzoeken toetsen de validiteit en betrouwbaarheid van de achterliggende vragenlijst en hypothesen, gevolgd door vele suggesties voor vervolgonderzoek, waaronder toevoeging van het aspect privacy. Het doel van dit onderzoek was om de originele HAIS-Q door te ontwikkelen met het aandachtsgebied privacy wat, mede door strenge (internationale) wetgeving, in vele organisaties binnen de gezondheidszorg een belangrijk item is om te borgen. Daarnaast zijn initiële betrouwbaarheids- en validiteitstesten uitgevoerd.

De ontwikkeling van het nieuwe aandachtsgebied is op vergelijkbare wijze uitgevoerd als de ontwikkeling van het originele model van Parsons, McCormac, Butavicius, et al. (2013). Het door Parsons, McCormac, Butavicius, et al. (2013) ontwikkelde model is in vervolgonderzoeken meermaals gevalideerd met positieve resultaten. Hieruit zou je kunnen afleiden dat de methode van ontwikkeling tot een bruikbaar resultaat leidt. De wijze van operationalisering van het complexe begrip IBB en de daarbinnen eveneens complexe aandachtsgebieden is echter wel aan verandering onderhevig. Dit blijkt ook uit latere onderzoeken, zoals die van Wissen (2017) en Schaeken (2018), en ook in dit onderzoek is gebleken dat de operationalisering van bestaande aandachtsgebieden aan verandering onderhevig is als gevolg van de verdergaande mogelijkheden van de techniek. Dit heeft geleid tot een verdere evolutie van het model, vergelijkbaar met het onderzoek van Schaeken (2018).

De operationalisering van het nieuwe aandachtsgebied is gedaan door interviews met deskundigen binnen slechts één organisatie, in dit onderzoek een topklinisch ziekenhuis waar de stand der techniek relatief ver is. Door daarnaast, net als bij de eerste ontwikkeling van de HAIS-Q, gebruik te maken van binnen de branche geldende wet- en regelgeving en sector richtlijnen voor operationalisering heeft het nieuwe aandachtsgebied een stabiele basis met vier benoemde subgebieden. De subgebieden betreffen allen gebieden waar de menselijke factor van grote invloed is op niet-naleving van beleid en bieden zodoende een prima basis en aanvulling op het bestaande model. De verdere toetsing van de constructvaliditeit middels de cognitieve test heeft geen uitsluitsel kunnen bieden of het construct privacy juist geoperationaliseerd is. Dit heeft mede met de vorm van onderzoek te maken. In toekomstig onderzoek zou de operationalisering van dit construct verder onderzocht kunnen worden met andere methodieken.

Zoals aangegeven in onderzoek van Wissen (2017) kan de inhoudsvaliditeit van de HAIS-Q verhoogt worden door toevoeging van context. De binnen dit onderzoek uitgevoerde enquête en interviews voorafgaand aan het opstellen van de doorontwikkelde HAIS-Q hebben aangetoond dat het toevoegen van context wenselijk is. Aan de doorontwikkelde HAIS-Q is context toegevoegd door een welkomsttekst met uitleg, voorbeeldvragen en inleidende teksten bij alle aandachtsgebieden.

De doorontwikkelde HAIS-Q is getest op betrouwbaarheid bij een pilotgroep. Deze groep bestond uit 59 medewerkers, aangevuld met vier medewerkers waarmee ook een cognitieve test is afgenomen. Uiteindelijk hebben 49 medewerkers de enquête ingevuld, waarvan zeven responses zijn verwijderd wegens onvolledigheid. Doordat het vanwege corona niet mogelijk was om zorgmedewerkers uit te nodigen deel te nemen, zijn HR-medewerkers gevraagd die ook met privacygevoelige data werken. Het is niet gezegd dat deze medewerkers hetzelfde reageren als medewerkers met direct patiëntcontact. De doelstelling van dit onderzoek is doorontwikkeling van een bruikbare methode voor de gezondheidszorg wat maakt dat de resultaten niet per se generaliseerbaar hoeven te zijn naar andere organisaties. Echter, het effect van het niet kunnen betrekken van zorgprofessionals in de doorontwikkeling op de realisatie van de doelstelling is onbekend.

Voor de betrouwbaarheid is Cronbach's alfa bepaald voor het totaal van het IBB, voor bestaande aandachtsgebieden en dimensies. Waar mogelijk zijn de resultaten vergeleken met die uit andere onderzoeken. De Cronbach's alfa voor het totaal van IBB is 0,9 en wijkt daarmee nauwelijks af van die van het onderzoeksteam. Hiermee kan gesteld worden dat de toevoeging van het aandachtsgebied privacy geen negatieve invloed heeft op de betrouwbaarheid van de meting van het construct IBB. De Cronbach's alfa voor het nieuwe aandachtsgebied is 0,676 wat conform vele statistici een acceptabele score is voor het bepalen van de interne consistentie van een construct (Vaske et al., 2017). Ook dit bevestigt dat de doorontwikkelde HAIS-Q een aanvulling is op de bestaande HAIS-Q.

De inhoudsvaliditeit van de doorontwikkelde HAIS-Q is op meerder wijzen vastgesteld. Literatuuronderzoek heeft aangetoond dat de bestaande HAIS-Q binnen verschillende onderzoeken (McCormac et al., 2016; McCormac et al., 2017; Parsons et al., 2017; Parsons et al., 2010; Parsons et al., 2014) is gevalideerd. In dit onderzoek zijn elf experts en senior managers middels een enquête gevraagd of zij vragen uit de bestaande HAIS-Q essentieel vonden. Hier zijn vergelijkbare resultaten gevonden als in het onderzoek van Wissen (2017) die ook deze methodiek heeft gebruikt voor toetsing van validiteit. Daarnaast zijn deze elf mensen geïnterviewd en zijn deze vragen nader besproken. Resultaat is vergelijkbaar met het onderzoek van Schaeken (2018), waar twee subgebieden zijn vervangen door nieuwe, meer bij de stand van de huidige techniek passende, subgebieden.

De constructvaliditeit van de doorontwikkelde HAIS-Q zou binnen dit onderzoek getest worden middels uitvoering van een cognitieve test met experts en zorgprofessionals. De cognitieve test was binnen het onderzoek van Parsons, McCormac, Butavicius, et al. (2013) immers succesvol gebruikt. Doelstelling was om na te gaan of het construct IBB juist geoperationaliseerd is, waar ook binnen andere onderdelen van dit onderzoek aandacht voor is geweest. De cognitieve test heeft veel inzicht gegeven in de inhoudsvaliditeit maar geen extra bewijs geleverd voor de constructvaliditeit. Dit heeft mede te maken met de onbekendheid van de onderzoeker met deze vorm van testen. Ondanks deze tegenvallende resultaten op het gebied van de constructvaliditeit bieden de overige resultaten voldoende bewijs voor een juiste operationalisering. De afname van een cognitieve test door meer dan één onderzoeker of een meer ervaren onderzoeker zou bij kunnen dragen aan de betrouwbaarheid van de resultaten op dit gebied.

Vragenlijsten, zoals de HAIS-Q, en interviews hebben het gevaar in zich dat de vragen sociaal wenselijk worden beantwoord. Dit zou dan ten koste gaan van de betrouwbaarheid van het onderzoek en daarmee de resultaten. Binnen dit onderzoek zijn daar verschillende maatregelen voor getroffen, zoals het afnemen van interviews in afgesloten ruimten op momenten dat het de geïnterviewde uitkwam. Waar mogelijk zijn enquêtes anoniem afgenomen. Tijdens de interviews is naar voren gekomen dat de geïnterviewden vinden dat verschillende vragen in de HAIS-Q uitlokken tot sociaal wenselijk antwoorden. De enquêteresultaten zijn niet getoetst op aanwezigheid van sociaal wenselijk antwoorden, wat maakt dat er niet bewezen kan worden of dit wel of niet is gebeurd. De cultuur van een organisatie kan hier ook een rol in spelen.

Het ontwikkelen van een meetinstrument, zoals de HAIS-Q, is een proces van meerdere iteraties, wat ook blijkt uit de eerdere onderzoeken naar de HAIS-Q. Zoals verwacht heeft dit onderzoek naast de doorontwikkeling van de originele HAIS-Q resultaten opgeleverd die gebruikt kunnen worden in een volgende iteratie bij een volgend onderzoek.

## 6.2 Conclusies

Het onderzoek beoogt de volgende onderzoeksvraag te beantwoorden:

***Welke geschikte, en bij voorkeur gevalideerde, methode kan worden gebruikt voor het meten van het IBB binnen de gezondheidszorg?***

Vanuit het literatuuronderzoek is de HAIS-Q naar voren gekomen als een geschikte basis voor het meten van het IBB. De operationalisering van het complexe begrip IBB in zeven verschillende aandachtsgebieden met elk drie subgebieden biedt een zeer ruime basis en geeft een brede dekking van onderwerpen. De

onderliggende hypothesen geven daarnaast mooie aanknopingspunten voor een eventueel op te zetten awareness campagne. Validatie is binnen verschillende organisaties uitgevoerd, echter niet binnen de gezondheidszorg.

Privacy was echter nog geen aandachtsgebied binnen de bestaande HAIS-Q, wat maakt dat de methodiek nog niet voldoende bruikbaar was voor de gezondheidszorg. Literatuuronderzoek heeft ook aangetoond hoe de methodiek is ontwikkeld en dat het mogelijk is om deze methodiek verder te ontwikkelen.

Dit onderzoek heeft de methode doorontwikkeld door toevoeging van het aandachtsgebied privacy. Vervolgens zijn validiteits- en betrouwbaarheidstesten uitgevoerd, met als conclusie dat de doorontwikkelde HAIS-Q valide en betrouwbaar is bevonden voor een eerste model. Zoals verwacht zijn bij de validiteits- en betrouwbaarheidstesten nog aandachtspunten gevonden die gebruikt kunnen worden in volgende onderzoeken.

## 6.3 Aanbevelingen voor de praktijk

Vanuit de Nederlandse Vereniging van Ziekenhuizen worden ziekenhuizen verplicht te voldoen aan de gedragslijn toegangsbeveiliging. Eén van de onderdelen hierbinnen is het opzetten van een awareness campagne. Ziekenhuizen, maar ook andere zorginstellingen, kunnen de doorontwikkelde HAIS-Q gebruiken om een nulmeting uit te voeren op het IBB binnen hun organisatie. Een op te zetten awareness campagne kan plaatsvinden op basis van de gevonden resultaten, waarbij de resultaten per dimensie en aandachtsgebied een goed inzicht geven waar het zwaartepunt van de campagne zou moeten liggen. Vervolgmetingen kunnen ook gebeuren met behulp van de doorontwikkelde HAIS-Q, eventueel toegespitst op enkele onderdelen.

Binnen de case-organisatie hebben deelnemers aangegeven dat het invullen van de HAIS-Q al bijdraagt aan hun IBB en zijn er verschillende maatregelen genomen om het IBB te verhogen. Betrokken management is erg enthousiast over de methode en zij willen hiervan gebruik maken voor het uitvoeren van een nulmeting.

## 6.4 Aanbevelingen voor verder onderzoek

De resultaten laten zien dat de doorontwikkelde HAIS-Q valide en betrouwbaar is. De ontwikkeling heeft echter binnen één organisatie plaatsgevonden, waarbij pilotgroep niet uit zorgprofessionals bestond. Vervolgonderzoek kan bestaan uit meerdere en verschillende validiteits- en betrouwbaarheidstesten met zorgprofessionals uit meerdere organisaties.

Gedurende het proces van doorontwikkeling is gebleken dat de stand der techniek kan zorgen dat de operationalisering van begrippen niet meer juist is. Ook kunnen gebieden binnen een organisatie of branche om andere redenen niet relevant zijn. Het wordt daarom aanbevolen om de HAIS-Q altijd te toetsen op validiteit op het moment van gebruik en binnen de organisatie van onderzoek. Een methode om de HAIS-Q makkelijk te valideren voor het doel van gebruik zou in de toekomst onderzocht kunnen worden.

Tijdens dit onderzoek is gebleken dat het toevoegen van contextinformatie bijdraagt aan het begrip van de vragen en daarmee aan de resultaten. Naast de reeds toegevoegde contextinformatie laten de resultaten van de cognitieve test zien dat ook hier nog ruimte voor verbetering is.

Dit onderzoek heeft aangetoond dat verschillende woorden binnen de vragen van de HAIS-Q voor meerdere uitleg vatbaar zijn, enkele vragen te stellig worden bevonden en begrippen onbekend of niet duidelijk zijn. Het voorleggen van de vragenlijst aan een communicatiedeskundige kan de validiteit van de HAIS-Q verhogen.

Feedback op de HAIS-Q laat onder meer zien dat niet alle vragen van toepassing zijn. Toekomstig onderzoek kan kijken naar de mogelijkheid van het toevoegen van een antwoordoptie ‘niet van toepassing’ en het effect daarvan op de validiteit en betrouwbaarheid van de resultaten.

# Referenties


Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Information security policy compliance: The role of information security awareness.

Autoriteit Persoonsgegevens. (2019). Boetebesluit HAGA Ziekenhuis. Retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_haga_-_ter_openbaarmaking.pdf

Autoriteit Persoonsgegevens. (2019). Cijfers datalekken 2018. Retrieved from https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/overzichten-datalekken/cijfers-datalekken-2018

Autoriteit Persoonsgegevens. (2019). Onderzoek toegang digitale patientendossiers. Retrieved from https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/haga_rapport_def.pdf

Autoriteit Persoonsgegevens. (2019). Zes aanbevelingen voor een privacybeleid. Retrieved from https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/zes-aanbevelingen-voor-een-privacybeleid

Baranowski, T., Cullen, K. W., Nicklas, t., Thompshon, D., & Baranowski, J. (2003). Are current health behavioral change models helpful in guiding prevention of weight gain efforts? *Obesity research, 11*(October), 23S-43S.

Bauer, S., & Bernroider, E. (2017). From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 48*(3), 44-68. doi:10.1145/3130515.3130519

Box, D., & Pottas, D. (2014). A Model for Information Security Compliant Behaviour in the Healthcare Context. *Procedia Technology, 16*, 1462-1470. doi:10.1016/j.protcy.2014.10.166

Bragdon, B. (2018). 2018 Global state of Information Security Survey.

Budding, J. (2018). Datalek patientgegevens van 22 kinderen Viecuri ziekenhuis op straat. Retrieved from https://www.medicalfacts.nl/2018/10/25/datalek-patientgegevens-van-22-kinderen-viecuri-ziekenhuis-op-straat/

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523-548. doi:10.2307/25750690

Chen, X., Chen, L., Wu, D., & Teng, J. K. L. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management, 55*(8), 1049-1060. doi:10.1016/j.im.2018.05.011

Choi, M., & Song, J. (2018). Social control through deterrence on the compliance with information security policy. *Soft Computing, 22*(20), 6765-6772. doi:10.1007/s00500-018-3354-z

Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. *Telematics and Informatics, 35*(6), 1770-1780. doi:10.1016/j.tele.2018.05.005

Gedragscode gezondheidsonderzoek, (2005).

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior, 28*(5), 1849-1858. doi:10.1016/j.chb.2012.05.003

D'arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems, 20*(6), 643-658.

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, 20*(1), 79-98. doi:10.1287/isre.1070.0160

Egelman, S., & Peer, E. (2015). *Scaling the security wall: Developing a security behavior intentions scale (sebis).* Paper presented at the Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems.

Verordening (EU) 2016/679 van het Europees Parlement en de Raad, 32 C.F.R. § lid 1 (2016).

Evans, M., He, Y., Maglaras, L., & Janicke, H. (2019). HEART-IS: A novel technique for evaluating human error-related information security incidents. *Computers & Security, 80*, 74-89. doi:10.1016/j.cose.2018.09.002

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks, 9*(17), 4667-4679. doi:10.1002/sec.1657

Geest, M. v. d. (2019). Patiëntdossiers in te zien door lek bij ziekenhuis OLVG. Retrieved from https://www.volkskrant.nl/nieuws-achtergrond/patientdossiers-in-te-zien-door-lek-bij-ziekenhuis-olvg~bab966c4/?referer=https%3A%2F%2Fwww.google.com%2F

Haeussinger, F., & Kranz, J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behavior.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165. doi:10.1016/j.dss.2009.02.005

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.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95. doi:10.1016/j.cose.2011.10.007

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69-79. doi:10.1016/j.im.2013.10.001

ISO/IEC 27000:2018(en) Information technology — Security techniques — Information security management systems — Overview and vocabulary, (2018).

Juridisch Woordenboek. (Ed.) (2018) Juridische Woordenboek. AMO institute of sciences

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), 518-555.

Keeney, R. L. (1994). Creativity in decision making with value-focused thinking. *Sloan Management Review*(Summer), 33-41.

Kim, S. H., Yang, K. H., & Park, S. (2014). An Integrative Behavioral Model of Information Security Policy Compliance. *SCIENTIFIC WORLD JOURNAL, 2014*, 463870-463812. doi:10.1155/2014/463870

Gedragscode Elektronische Gegevensuitwisseling in de Zorg, (2019).

Kollmuss, A., & Agyeman, J. (2002). Mind the gap: why do people act environmentally and what are the barriers to pro-environmental behavior? *Environmental education research, 8:3*(August), 239-260.

Kruger, H. A., Drevin, L., & Steyn, T. (2006). *A Framework for Evaluating ICT Security Awareness.* Paper presented at the ISSA.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289-296. doi:10.1016/j.cose.2006.02.008

McCormac, A., Calic, D., Parsons, K., Zwaans, T., Butavicius, M., & Pattison, M. (2016). Test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q).

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior, 69*, 151-156. doi:10.1016/j.chb.2016.11.065

McGuire, W. J. (1969). The nature of attitudes and attitude change. *3*.

Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, (2008).

Uitvoeringswet Algemene verordening gegevensbescherming, (2018).

Moody, G. D., Siponen, M., Pahnila, S., University of Nevada, L. V., University of, J., & University of, O. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42*(1), 285-285. doi:10.25300/MISQ/2018/13853

NEN 7512:2015 nl Medische informatica - Informatiebeveiliging in de zorg - Vertrouwensbasis voor gegevensuitwisseling, 7512 C.F.R. (2015).

NEN 7510-1:2017 nl Medische informatica - Informatiebeveiliging in de zorg - Deel 1: Managementsysteem, Deel 1: Managementsysteem C.F.R. (2017).

NEN 7510-2:2017 nl Medische informatica - Informatiebeveiliging in de zorg - Deel 2: Beheersmaatregelen, (2017).

NEN 7513:2018 nl Medische informatica - Logging - Vastleggen van acties op elektronische patiëntdossiers, (2018).

Netemeyer, R. G., Bearden, W. O., & Sharma, S. (2003). *Scaling procedures: Issues and applications*: Sage Publications.

NOS. (2017). Zeker vijftien ziekenhuizen geïnfecteerd met ransomware. Retrieved from https://nos.nl/artikel/2179941-zeker-vijftien-ziekenhuizen-geinfecteerd-met-ransomware

NOS. (2018). Tientallen onbevoegden bekeken medisch dossier Barbie. Retrieved from https://nos.nl/artikel/2225867-tientallen-onbevoegden-bekeken-medisch-dossier-barbie.html

Gedragslijn Toegangsbeveiliging digitale patiëntdossiers, (2020).

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2015). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83-93. doi:10.1016/j.cose.2015.10.002

Park, E. H., Kim, J., Wiles, L. L., & Park, Y. S. (2018). Factors affecting intention to disclose patients' health information. *Computers & Security*.

Park, Y. S., Park, E. H., & Kim, J. (2017). The role of information security learning and individual factors in disclosing patients' health information. *Computers & Security, 65*, 64-76. doi:10.1016/j.cose.2016.10.011

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 66*, 40-51. doi:10.1016/j.cose.2017.01.004

Parsons, K., McCormac, A., Butavicius, M., Ferguson, L., Defence, S., Technology Organisation Edinburgh Command Control, C., & Intelligence, D. I. V. (2010). Human Factors and Information Security: Individual, Culture and Security Environment. In.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2013, 2013). *The development of the human aspects of information security questionnaire (HAIS-Q)*.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165-176. doi:10.1016/j.cose.2013.12.003

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013). A study of information security awareness in Australian government organisations. *Information Management & Computer Security, 22*(4), 334-345. doi:10.1108/IMCS-10-2013-0078

Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security, 80*, 211-223. doi:10.1016/j.cose.2018.09.016

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security, 27*(7), 241-253. doi:10.1016/j.cose.2008.07.008

De overeenkomst inzake geneeskundige behandeling, § Artikel 446 tm 468 (1994).

Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security, 59*, 26-44. doi:10.1016/j.cose.2016.01.004

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research Methods for Business Students* (7 ed.). Amsterdam: Pearson Education.

Schaeken, M. (2018). *Information security awareness measuring & social engineering 2.0.* (Thesis). Open Universiteit,

Schultz, E. (2005). The human factor in security. *Computers & Security, 24*(6), 425-426. doi:10.1016/j.cose.2005.07.002

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management and Computer Security 8*(1), 31-41.

Siponen, M. (2001). Five dimensions of information security awareness. *ACM SIGCAS Computers and Society, 31*(2), 24-29. doi:10.1145/503345.503348

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224. doi:10.1016/j.im.2013.08.006

Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly, 34*(3), 487-502. doi:10.2307/25750688

Skipr. (2018). Zorg is wederom koploper aantal datalekken. Retrieved from https://www.skipr.nl/actueel/id34170-zorg-is-wederom-koploper-aantal-datalekken.html

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: a systematic review of quantitative studies. *Information Management & Computer Security, 22*(1), 42-75.

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information systems, 13*(1), 24.

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. doi:10.1016/j.im.2012.04.002

Vaske, J. J., Beaman, J., & Sponarski, C. C. (2017). Rethinking Internal Consistency in Cronbach's Alpha. *Leisure sciences, 39*(2), 163-173. doi:10.1080/01490400.2015.1127189

Velki, T., Solic, K., & Ocevcic, H. (2014). *Development of Users' Information Security Awareness Questionnaire (UISAQ)—Ongoing work.* Paper presented at the 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).

Verschuren, P. J. M., & Doorewaard, H. (2007). *Het ontwerpen van een onderzoek*: Lemma.

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198. doi:10.1016/j.cose.2004.01.012

Wissen, D. v. (2017). *Meten van informatiebeveiligingsbewustzijn.* (Thesis). Open Universiteit,

Z-CERT. (2020). Hackers laten gijzelsoftware los op zorgsector. Retrieved from https://www.z-cert.nl/nieuws/hackers-laten-gijzelsoftware-los-op-zorgsector/

Zondervirus. (2018). Ziekenhuis betaalt $55.000 gedurende aanval met gijzelsoftware. Retrieved from https://zondervirus.nl/ziekenhuis-betaalt-55-000-gedurende-aanval-met-gijzelsoftware/

## Bijlage I Literatuuronderzoek

Op de volgende pagina begint het volledige literatuuronderzoeksrapport.

LET OP: De eerstvolgende bijlagen (met een opvolg LETTER) horen alleen bij het literatuuronderzoek.

De eerstvolgende bijlage van het afstudeeronderzoek is “Bijlage II: Onderzoeklogboek empirisch onderzoek ”.


# *DE HUMAN ASPECTS OF INFORMATION SECURITY QUESTIONNAIRE (HAIS-Q): EEN STUDIE BINNEN DE CONTEXT VAN DE GEZONDHEIDSZORG*

Literatuuronderzoek naar een meetmethodiek

| | |
|---|---|
| Cursus: | IM0602 Voorbereiden Afstuderen BPMIT |
| Student: | P.M.E.M. Verbeek |
| Identiteitsnummer: | 851547527 |
| Datum rapport: | 2 februari 2020 |
| Versienummer: | 1.0 |
| Status: | Definitief |

# De Human Aspects of Information Security Questionnaire (HAIS-Q): Een studie binnen de context van de gezondheidszorg

Literatuuronderzoek naar een meetmethodiek

# The Human Aspects of Information Security Questionnaire (HAIS-Q): a study within the context of a hospital

Literature study for a measurement method


| | |
|---|---|
| Opleiding: | Open Universiteit, faculteit Management, Science & Technology |
| | Masteropleiding Business Process Management & IT |
| Programme: | Open University of the Netherlands, faculty of Management, Science & Technology<br>Master Business Process Management & IT |
| Cursus: | IM0602 Voorbereiden Afstuderen BPMIT |
| Student: | P.M.E.M. Verbeek |
| Identiteitsnummer: | 851547527 |
| Datum: | 2 februari 2020 |
| Afstudeerbegeleider | prof. dr. A. Bijlsma |
| Meelezer | Dhr. L. Rutledge |
| Versie nummer: | 1.0 |
| Status: | Definitief |

# Inhoudsopgave

## Doelstelling

De doelstelling van het literatuuronderzoek is te komen tot een theoretisch kader wat gebruikt wordt om het empirisch onderzoek uit te voeren. Vorming van dit theoretisch kader gebeurt door de beantwoording, op basis van gevonden literatuur, van drie vooraf opgestelde deelvragen.

## Deelvragen

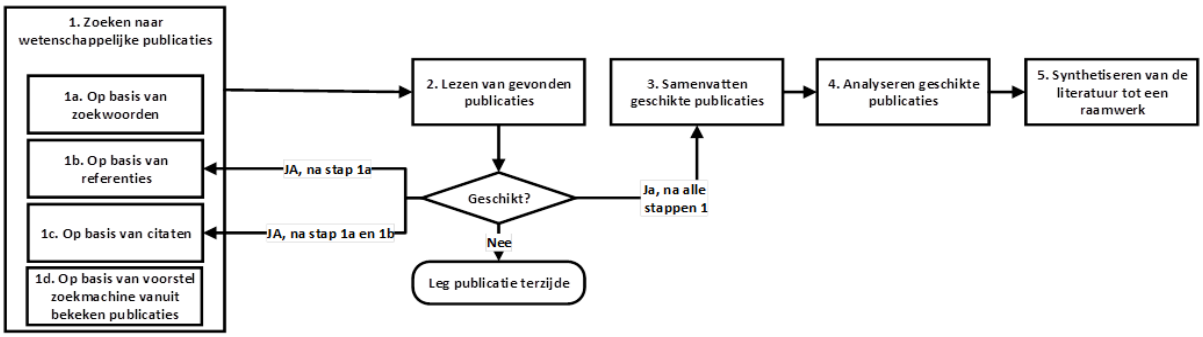
*L1 : Is IBB een van belang zijnde factor bij de naleving van het informatiebeveiligings- en/of privacybeleid?*

*L2 : Welke gevalideerde methoden zijn er binnen de recente literatuur bekend om het IBB te meten en in hoeverre zijn deze bruikbaar binnen de gezondheidszorg?*

*L3: Is het mogelijk om bestaande methoden voor het meten van IBB door te ontwikkelen en vervolgens te valideren, en zo ja op welke wijze?*

## Stappenplan

Om een onderbouwd antwoord op de deelvragen te kunnen geven, wordt het literatuuronderzoek uitgevoerd conform een vooraf opgesteld stappenplan. Op basis van dit stappenplan en de daarbinnen gebruikte factoren, is goed navolgbaar hoe de resultaten van het literatuuronderzoek tot stand zijn gekomen. Onderstaande afbeelding geeft het stappenplan schematisch weer. Daarna worden alle stappen kort beschreven.




**Afbeelding 1 Stappenplan literatuuronderzoek**

### Stap 1 Zoeken naar wetenschappelijke publicaties

#### *Bronnen*

Voor de beantwoording van de deelvragen wordt gestart met het, op basis van zoekwoorden, zoeken naar recente literatuur in tertiaire (databases) en secundaire (officiële publicaties) bronnen die beschikbaar zijn via de universiteitsbibliotheek van de Open Universiteit. Hiervoor wordt in eerste instantie gebruik gemaakt van de QuickSearch optie. Daarnaast wordt gebruik gemaakt van de volgende databases om met dezelfde zoekstring relevante literatuur te zoeken of om gevonden titels in full tekst versie op te halen:

- **ACM Digital Library**
  De ACM Digital Library is een database voor literatuur op het gebied van de Informatica. De database bevat fulltext van en verwijzingen naar publicaties van de ACM (Association for Computing Machinery): tijdschriftartikelen, artikelen in newsletters en conference proceedings vanaf 1954.
- **Association for Information Systems (hierna: AIS)**
  AIS electronic library bevat onderzoekspapers, tijdschriftartikelen en conferentiebijdragen op het gebied van informatiesystemen en informatica.
- **Business Source Premier (hierna: EBSCO)**
  Internationale economische onderzoeksdatabank met meer dan 2200 full-text tijdschriften, waaronder de top management- en marketingtijdschriften zoals Journal of Marketing, Harvard

Business Review, Fortune en Time Magazine. Daarnaast bevat Business Source Premier fulltext rapporten over:
    - de belangrijkste internationale bedrijven (Company Profiles);
    - branches en markten (Industry Profiles and Market Research Reports);
    - landen (Country Reports).
- **Directory of Open Access Journals (hierna: DOAJ)**
  De DOAJ is een website met circa 10.000 open access tijdschriften.
  Het doel van DOAJ is een zo compleet mogelijk overzicht te geven van kwalitatieve, open access, peerreviewed tijdschriften. Van meer dan de helft van deze tijdschriften zijn ook de artikelen geïndexeerd. Een overzicht van op kwaliteit beoordeelde wetenschappelijke open access tijdschriften.
- **Emerald management plus**
  Emerald [management plus] biedt toegang tot meer dan 220 managementtijdschriften. Oudere jaargangen zijn vanaf 1988 beschikbaar.
- **Google Scholar**
  Google Wetenschap is een zoekmachine waarmee een groeiende verzameling wetenschappelijke publicaties wordt doorzocht van academische uitgeverijen, professionele organisaties, universiteiten en andere wetenschappelijk organisaties. Deze publicaties vind je niet met de 'gewone' Google. Sommige uitgevers geven Google Scholar toegang tot de full text van hun elektronische tijdschriften. Verder zijn via deze zoekmachine o.a. citations en verwijzingen naar boeken te vinden.
- **Journal STORage (hierna: JSTOR)**
  JSTOR biedt toegang tot een archief van elektronische tijdschriftartikelen, waarin de artikelen beschikbaar zijn vanaf de eerste jaargang van een tijdschrift tot drie à vijf jaar geleden (de zgn. 'moving wall'). Het omvat archieven van toonaangevende wetenschappelijke tijdschriften uit de geesteswetenschappen, sociale wetenschappen en wetenschappen, evenals geselecteerde monografieën en ander materiaal dat waardevol is voor wetenschappelijk werk. Beschikbare collecties:
    - Business and Economics
    - Mathematics and Statistics
    - Life Sciences
    - Arts and Sciences.

  Alleen toegang tot oudere jaargangen.
- **Sciencedirect (Elsevier)**
  ScienceDirect provides access to the *scientific, technical and medical (=STM) journals of Elsevier and participating publishers.* The full text of over 2,500 journals is available. Most of the journals are posted from 1995 forward. Since the archives of Elsevier are included most journals go even back to issue 1 of volume 1. New titles are added on a regular basis. 'Articles in press' (=peer-reviewed papers, that have been accepted but not yet been corrected or published in the printed journal) are available as well. Additional books however and journals of several publishers which have been integrated into this database are not always full text available. However tables of contents and abstracts of all journals are freely accessible. The new Elsevier platform 'SciVerse' is also available via ScienceDirect. This platform integrates content and discovery tools from Elsevier, participating publishers and relevant scientific websites. Your institution has access to ScienceDirect, but not to Scopus. Please note that Scopus results are, therefore, not included in SciVerse search results.
- **SpringerLink**
  Platform van uitgever Springer dat toegang biedt tot een grote hoeveelheid bronnen op het gebied van wetenschap, technologie en geneeskunde. SpringerLink bevat eBooks, wetenschappelijke publicaties, naslagwerken en protocollen die diverse vakgebieden bestrijken. Bij het openen van de databank zijn per documentsoort de aantallen te zien. Via SpringerLink heb je tevens toegang tot een collectie Nederlandstalige e-books van uitgever Bohn Stafleu van Loghum.
- **Web of Science**

With *citation indexes* – besides searching for articles on a Topic or Author(s) – you can also find the articles that cite a person's work, i.e. 'Cited reference searching'. Coverage:

- Science Citation Index Expanded™ (SCIE) last 10 years. Fully indexes over 8,500 major journals across 150 disciplines.
- Social Sciences Citation Index™ last 10 years. Fully indexes over 3,000 social sciences journals, covering the most significant social sciences discoveries from all of the 20th century.
- Arts & Humanities Citation Index® last 10 years. Fully indexes over 1,700 arts and humanities journals, as well as selected items from over 250 scientific and social sciences journals.

Gevonden resultaten uit tertiaire bronnen worden gebuikt om gericht te kunnen zoeken naar specifieke publicaties in secundaire bronnen (officiële publicaties). Hierbij wordt gezocht naar publicaties die getoetst zijn door erkende deskundigen, peer reviewed, wat inhoudt dat er gezocht wordt naar publicaties die gepubliceerd zijn in wetenschappelijke en/of vaktijdschriften. Bij het gebruik van boeken dienen dit wetenschappelijke boeken te zijn.

*Stap 1a. Zoeken van recente publicaties o.b.v. zoekwoorden*

Algemene selectiecriteria binnen 'quicksearch' en waar mogelijk databases

- Zoekwoorden in het Engels
- Publicatiedatum: 01-04-2014 tm 01-04-2019
- Content type: Artikel in vakblad OR Magazine article OR Publicatie OR Tijdschriftartikel
- Vakgebied: Business OR Computer science OR Publich Health
- Taal: English
- Selectie beperken tot: Volledige tekst online AND Peer reviewed publicaties
- Uitsluiten uit resultaat: Geen selectie
- Resultaten selectie uitbreiden met: Resultaten opnemen uit andere bronnen dan de verzameling in uw bibliotheek

*Stap 1b. Zoeken van recente publicaties o.b.v. referenties uit relevante publicaties*

Naast het zoeken van geschikte publicatie middels zoekwoorden, is ook gebruik gemaakt van de referenties in gevonden geschikte publicaties om eerder verschenen geschikte publicaties te vinden.

*Stap 1c. Zoeken van recente publicaties o.b.v. citaten over gevonden relevante publicaties*

Naast het zoeken van geschikte publicaties middels zoekwoorden en referenties, is ook gezocht naar later verschenen geschikte publicaties door na te gaan in welke publicaties de gevonden geschikte publicaties geciteerd worden.

*Stap 1d. Aangeboden publicaties door zoekmachine vanuit bekeken publicaties*

Bij het bekijken van de publicaties gevonden op basis van zoekwoorden, worden door de zoekmachine voorstellen gedaan voor interessante publicaties. Ook deze worden beschouwd in de volgende stap.

### Stap 2. Lezen van publicaties om te komen tot een selectie van geschikte publicaties

Vanuit de gevonden publicaties is een selectie van geschikte publicaties gemaakt. Dit is gedaan door op basis van de samenvatting en het daarin geformuleerde doel, opzet, resultaten en conclusie een mening te vormen betreffende de geschiktheid van de publicatie. Indien de publicatie niet geschikt leek, is deze terzijde gelegd. Indien de publicatie op inhoud wel geschikt leek, is geschiktheid ook beoordeeld op basis van het aantal malen dat het artikel geciteerd is in combinatie met de publicatiedatum en/of de breedte van het onderzoek (branche, land, etc.). Bij ongeschiktheid is het artikel ter zijde gelegd. Indien de publicatie ook op deze kenmerken geschikt leek, zijn de inleiding en genoemde suggesties voor verder onderzoek gelezen om te toetsen of de publicatie inderdaad inhoudelijk geschikt is. Vervolgens zijn de overige paragrafen doorgekeken om de relevantie van die paragrafen te bepalen. Daar waar de paragrafen relevant geacht werden, zijn deze volledig doorgelezen. Minder relevante paragrafen zijn 'diagonaal' doorgelezen. Als laatste zijn de conclusie en de samenvatting nogmaals doorgelezen om de details van het artikel te kunnen relateren aan de hoofdlijn van het artikel.

### Stap 3. Samenvatten van geschikte publicaties

Van de geschikte publicaties is een korte samenvatting gemaakt. Voorafgaand aan en ten behoeve van het maken van de samenvatting, zijn per publicatie de resultaten, conclusies, implicaties en aanbevelingen geïnventariseerd. Ook is de essentie van de publicatie in relatie tot de gestelde deelvraag opgeschreven. Op basis van de essenties van de verschillende publicaties is een overzicht gemaakt waarmee inzichtelijk wordt hoe de publicaties zich tot elkaar verhouden.

### Stap 4. Analyseren van geschikte publicaties

Op basis van de gemaakte samenvattingen en de onderlinge samenhang van de publicaties is bekeken welke (delen van) publicaties in welk opzicht en in welke mate gebruikt kunnen worden. Waar mogelijk zijn deze delen verduidelijkt met voorbeelden. Tijdens de analyse is bekeken welke publicaties elkaar kunnen bevestigen of versterken, zodat conclusies uit een gezamenlijke set van publicaties kunnen worden getrokken. Ook is bekeken of publicaties elkaar juist tegenspreken of tegenstrijdig aan elkaar zijn. De analyse heeft geleid tot een samenhangend betoog per deelvraag, waarbij duidelijk wordt wat en hoe het onderzoek zou kunnen bijdragen.

### Stap 5. Het synthetiseren van de literatuur ter beantwoording van de deelvragen

Op basis van de analyse van gevonden literatuur worden de deelvragen beantwoord. De gevonden antwoorden bepalen de doelstelling van het uit te voeren onderzoek in de werkelijkheid en de verwachtingen van wat we binnen dit onderzoek aan zullen treffen. De resultaten van het empirisch onderzoek zullen we gaan vergelijken met deze verwachtingen.

## Uitvoering

### Stap 1. Zoeken naar wetenschappelijke publicaties

### Stap 1a. Zoeken van recente publicaties o.b.v. zoekwoorden

*Deelvraag 1*

Zoekwoorden deelvraag 1

De te gebruiken zoekwoorden betreffen de (afgeleide) kernwoorden van de deelvraag die beantwoord moet worden.
Zoekwoorden alle velden: information security policy AND compliance AND behaviour AND information security awareness
Op basis van de Engelse zoekwoorden zijn met behulp van de ‘quicksearch’ mogelijkheid 2.590 publicaties gevonden. Sortering van de resultaten is op basis van relevantie. De eerste 20 publicaties zijn opgehaald door gebruik te maken van één van de genoemde databases uit de paragraaf bronnen.

*Deelvraag 2*

Voor deelvraag 2 is deze methode niet gebruikt.

*Deelvraag 3*

Voor deelvraag 3 is deze methode niet gebruikt.

### Stap 1b. Zoeken van recente publicaties o.b.v. referenties uit geschikte publicaties

*Deelvraag 1*

De 8 geschikte publicaties uit stap 1a. zijn bekeken op gebruikte referenties. Referenties die in meer dan 5 van de 8 geschikte publicaties zijn benoemd, worden opgenomen om verder te bekijken in stap 2. Dit betreft 17 publicaties.

Naast het onderkennen van mogelijk geschikte publicaties op basis van aantallen keren dat hieraan is gerefereerd, zijn ook publicaties bekeken waaraan gerefereerd werd in gelezen publicaties en die interessant leken. Op deze wijze zijn nog 4 publicaties toegevoegd.

*Deelvraag 2*

Voor deelvraag 2 is uitgegaan van de relevante publicaties in de literatuurlijst van het literatuuronderzoek van twee bekende geschikte publicaties, te weten die van Wissen (2017) en Schaeken (2018). Deze literatuurlijst bevat op basis van titel 18 mogelijk geschikte publicaties om verder te bekijken in stap 2.

*Deelvraag 3*

Voor deelvraag 3 is uitgegaan van alle relevante publicaties uit deelvraag 2. Gekeken is naar onderzoeken die gebruik maken van de te prefereren methode voor mijn eigen onderzoek, te weten de HAIS-Q. Daarnaast is gekeken of de publicaties de methode verder ontwikkelen, deze valideren of deze toepassen. Dit betreft 7 publicaties.

### Stap 1c. Zoeken van recente publicaties o.b.v. citaten over gevonden geschikte publicaties

*Deelvraag 1*

Voor deelvraag 1 is niet verder gezocht naar geschikte publicaties om 2 redenen:

1. De publicatiedatumrange waarbinnen is gezocht op basis van zoekwoorden loopt tot bijna de dag van het literatuuronderzoek.
2. Het aantal geschikte publicaties voor het verkrijgen van een antwoord op deze deelvraag is op basis van zoekwoorden en referenties al vrij veel.

*Deelvraag 2*

Voor deelvraag 2 is deze methode niet gebruikt.

*Deelvraag 3*

Voor deelvraag 3 is deze methode niet gebruikt.

### Stap 1d. Aangeboden publicaties vanuit bekeken publicaties

*Deelvraag 1*

Bij het bekijken van de publicaties die in vorige stappen zijn gevonden zijn door de zoekmachine voorstellen gedaan voor mogelijk interessante publicaties. Op deze wijze zijn 24 publicaties opgehaald.

*Deelvraag 2*

Voor deelvraag 2 is deze stap niet uitgevoerd, echter zijn vanuit het zoeken naar publicaties voor deelvraag 1 wel voorstellen gedaan voor publicaties die mogelijk interessant zijn voor deelvraag 2.

*Deelvraag 3*

Voor deelvraag 3 is deze stap niet uitgevoerd.

### Stap 2. Lezen van publicaties om te komen tot een selectie van geschikte publicaties

Gevonden publicaties die na het lezen geschikt zijn bevonden voor beantwoording van de deelvragen en de vorming van het theoretisch kader, zijn in stap 3 samengevat. Publicaties die alleen gebruikt zijn voor ondersteuning van de introductie of ter inleiding van het theoretisch kader, worden niet samengevat.

*Deelvraag 1*

De eerste 20 publicaties gevonden met behulp van Engelse zoekwoorden (stap 1a) zijn conform de beschreven aanpak in stap 2 uit het stappenplan gelezen. Op basis van deze selectie zijn 13 publicaties terzijde gelegd en 7 publicaties geschikt bevonden voor gebruik in de introductie en/of het theoretische kader. Dit zijn de volgende publicaties:

- Kim, S. H., Yang, K. H., & Park, S. (2014). An Integrative Behavioral Model of Information Security Policy Compliance.
- Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness.
- Bauer, S., & Bernroider, E. (2017). From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization.
- Park, Y. S., Park, E. H., & Kim, J. (2017). The role of information security learning and individual factors in disclosing patients' health information.

- Chen, X., Chen, L., Wu, D., & Teng, J. K. L. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables.
- Choi, M., & Song, J. (2018). Social control through deterrence on the compliance with information security policy.
- Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education.

In stap 1b. zijn de referenties van de bovenstaande publicaties bekeken om op zoek te gaan naar meer geschikte publicaties. De 17 publicaties die 5 of meer keer voorkwamen als referentie, zijn conform de beschreven aanpak in stap 2 uit het stappenplan gelezen. Op basis van deze selectie zijn 5 publicaties terzijde gelegd en 12 publicaties geschikt bevonden voor gebruik in de introductie en/of het theoretische kader.

Naast het onderkennen van mogelijk geschikte publicaties op basis van aantallen keren dat hieraan is gerefereerd, zijn ook publicaties bekeken waaraan gerefereerd werd in gelezen publicaties en die interessant leken. Op deze wijze zijn nog 4 publicaties toegevoegd.

Op basis van referenties zijn de volgende publicaties gevonden t.b.v. het literatuuronderzoek:

- Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance.
- D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach.
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations.
- Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness.
- Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations.
- D'arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings.
- Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches.
- Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Information security policy compliance: The role of information security awareness.
- Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap.
- Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory.
- Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory.
- Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition.
- Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study.
- Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: a systematic review of quantitative studies.
- Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance.

Stap 1c. is voor deelvraag 1 niet uitgevoerd.

In stap 1d. zijn de publicaties die door de zoekmachine zijn voorgesteld als mogelijk interessante publicaties bekeken of hier geschikte publicaties bij zitten. De 24 voorgestelde publicaties zijn conform de beschreven aanpak in stap 2 uit het stappenplan gelezen. Op basis van deze selectie zijn 18 publicaties terzijde gelegd, waarvan er 4 mogelijk geschikt zijn voor de beantwoording van deelvraag 2. De overige 6 publicaties zijn geschikt bevonden voor gebruik in de introductie en/of het theoretische kader. Dit zijn de volgende publicaties:

- Haeussinger, F., & Kranz, J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behavior.
- Box, D., & Pottas, D. (2014). A Model for Information Security Compliant Behaviour in the Healthcare Context.
- Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations.
- Moody, G. D., Siponen, M., Pahnila, S., University of Nevada, L. V., University of, J., & University of, O. (2018). Toward a unified model of information security policy compliance.
- Park, E. H., Kim, J., Wiles, L. L., & Park, Y. S. (2018). Factors affecting intention to disclose patients' health information.
- Evans, M., He, Y., Maglaras, L., & Janicke, H. (2019). HEART-IS: A novel technique for evaluating human error-related information security incidents.

*Deelvraag 2*

Stap 1a is voor deelvraag 2 niet uitgevoerd, omdat gewerkt is vanuit de benoemde referenties in twee bekende geschikte publicaties, te weten:

- van Wissen, D. (2017). *Measuring Information Security Awareness.*
- Schaeken, M. (2018). *Information security awareness measuring & social engineering 2.0.*

In stap 1b zijn de 18 gevonden publicaties vanuit de referenties in de bekende publicaties en de bekende publicaties conform de beschreven aanpak in stap 2 uit het stappenplan gelezen. Op basis van deze selectie zijn 3 publicaties terzijde gelegd, 2 publicaties reeds gevonden in stap 1a voor deelvraag 1 en 13 publicaties geschikt bevonden voor gebruik in de introductie en/of het theoretische kader, naast de bekende publicaties. Dit zijn de volgende publicaties:

- Siponen, M. (2001). Five dimensions of information security awareness.
- Kruger, H. A., Drevin, L., & Steyn, T. (2006). *A Framework for Evaluating ICT Security Awareness.*
- Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness.
- Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study.
- Parsons, K., McCormac, A., Butavicius, M., Ferguson, L., Defence, S., Technology Organisation Edinburgh Command Control, C., & Intelligence, D. I. V. (2010). Human Factors and Information Security: Individual, Culture and Security Environment.
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2013, 2013). *The development of the human aspects of information security questionnaire (HAIS-Q)*.
- Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013). A study of information security awareness in Australian government organisations.
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q).
- Velki, T., Solic, K., & Ocevcic, H. (2014). *Development of Users' Information Security Awareness Questionnaire (UISAQ)—Ongoing work.*
- Egelman, S., & Peer, E. (2015). *Scaling the security wall: Developing a security behavior intentions scale (sebis).*
- Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2015). Analysis of personal information security behavior and awareness.
- McCormac, A., Calic, D., Parsons, K., Zwaans, T., Butavicius, M., & Pattison, M. (2016). Test-retest

reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q).
- Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies.

In stap 1d. zijn de publicaties die door de zoekmachine zijn voorgesteld als mogelijk interessante publicaties bekeken of hier geschikte publicaties bij zitten. Voor deelvraag 2 is niet gezocht op basis van zoekwoorden. Bij het zoeken voor deelvraag 1 zijn 4 voorgestelde publicaties naar voren gekomen die mogelijk relevant worden voor deelvraag 2. Van deze 4 publicaties, zijn er 3 reeds genoemd in de referenties, wat betekent dat er binnen deze stap 1 publicatie overblijft welke conform de beschreven aanpak in stap 2 uit het stappenplan is gelezen. Deze publicatie is geschikt bevonden voor gebruik in de introductie en/of het theoretische kader. Dit is de volgende publicatie:

- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness.

#### *Deelvraag 3*

De 7 gevonden publicaties uit stap 1b zijn conform de aanpak in stap 2 gelezen. Alle publicaties hebben elementen die geschikt bevonden zijn voor de beantwoording van deelvraag 3 en leveren zodoende ook een bijdrage aan het doel en de opzet van het empirisch onderzoek. Het betreft de volgende publicaties:

- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2013, 2013). *The development of the human aspects of information security questionnaire (HAIS-Q)*.
- Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013). A study of information security awareness in Australian government organisations. *Information Management & Computer Security, 22*(4), 334-345. doi:10.1108/IMCS-10-2013-0078
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165-176. doi:10.1016/j.cose.2013.12.003
- McCormac, A., Calic, D., Parsons, K., Zwaans, T., Butavicius, M., & Pattison, M. (2016). Test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q).
- Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 66*, 40-51. doi:10.1016/j.cose.2017.01.004
- Wissen, D. v. (2017). *Meten van informatiebeveiligingsbewustzijn.* (Thesis). Open Universiteit,
- Schaeken, M. (2018). *Information security awareness measuring & social engineering 2.0.* (Thesis). Open Universiteit.

### Stap 3. Samenvatten van geschikte publicaties

Publicaties die geschikt zijn bevonden voor het opbouwen van het theoretisch kader en/of de beantwoording van één of meerdere deelvragen zijn samengevat. Elke samenvatting is opgebouwd conform eenzelfde structuur. Per publicatie is onder andere weergegeven wat de relevantie van de publicatie is voor het eigen onderzoek.

Samenvattingen van publicaties ten behoeve van de beantwoording van deelvraag 1 zijn te vinden in bijlage A, samenvattingen van publicaties ten behoeve van de beantwoording van deelvraag 2 in bijlage B. De publicaties ten behoeve van de beantwoording van deelvraag 3 zijn reeds samengevat voor deelvraag 2 en worden niet nogmaals samengevat.

### Stap 4. Analyseren van geschikte publicaties

#### *Deelvraag 1*

*Is IBB een van belang zijnde factor bij de naleving van het informatiebeveiligings- en/of privacybeleid?*

- Huidige literatuur maakt gebruik van gedragsmodellen binnen onderzoek naar informatiebeveiliging, bijvoorbeeld TPB, PMT, GDT, KAB model. De oorsprong van veel van deze gedragsmodellen bevindt zich in de gezondheid, criminologie en psychologie. Omdat hier alleen factoren worden bestudeert die uit de gebruikte theorie naar voren komen zijn de onderzoeken eenzijdig en/of onvolledig. Dit is met name binnen onderzoek naar informatiebeveiliging een risico, omdat gedrag van medewerkers door vele factoren kan worden beïnvloed. Dit blijkt ook uit de verschillende literatuurstudies die naar een overal van onderzochte factoren kijken.
- Veel literatuur richt zich op verificatie of validatie van gebruikte theorieën en hebben zodoende een bevooroordeeld gezichtspunt ten aanzien van de gekozen theorie.
- Sommige modellen zijn een samenvoeging van meerdere theorieën, zonder te weten of de samenvoeging ook kan, andere modellen zijn gebaseerd op een enkele theorie.
- Binnen de modellen worden veelal de volgende afhankelijke factoren genoemd, intentie tot naleving, intentie tot misbruik, daadwerkelijke naleving, daadwerkelijk misbruik.
- De onafhankelijke en/of mediërende en/of modererende factoren zijn zeer veel en divers van aard en de verschillende onderzoeken variëren nog wel eens in de resultaten van vergelijkbare factoren.
- Niet alle onderzoeken zijn vergelijkbaar vanwege een ander gehanteerde theorie en/of andere definities van de voorgestelde factor.
- Er zijn verschillende onderzoeken die zich specifiek richten op IBB binnen een ziekenhuis.
- Overall literatuuronderzoeken geven veel informatie over de factor IBB en doen goede suggesties voor vervolg onderzoek.
- Onderzoek laat zien dat IBB van invloed is op de naleving van het informatiebeveiligingsbeleid.

*Deelvraag 2*

*Welke gevalideerde methoden zijn er binnen de recente literatuur bekend om het IBB te meten en in hoeverre zijn deze bruikbaar binnen de gezondheidszorg?*

- Gevonden onderzoeken in deelvraag 1 waar IBB een factor is meten dit niet met behulp van een gevalideerde methode.
- Binnen de literatuur zijn meerdere methoden te vinden voor het meten van het IBB, echter zijn lang niet alle methoden breed gevalideerd.
- Meest voorkomende en gevalideerde methode is de HAIS-Q.
- Gevonden methode bevat niet het aspect privacy. Het toevoegen van aandachtsgebieden, waaronder privacy, wordt wel als suggestie voor vervolgonderzoek benoemd.

*Deelvraag 3*

*Is het mogelijk om bestaande methoden voor het meten van IBB door te ontwikkelen en vervolgens te valideren, en zo ja op welke wijze?*

- Het initiële HAIS model is middels een hybride methodologie ontwikkeld, waarin de inductieve, verkennende aanpak is opgenomen die wordt aanbevolen door Karjalainen and Siponen (2011). Hybride om een mix van kwalitatieve en kwantitatieve methoden voor het verzamelen en analyseren van gegevens aan te duiden. Er zijn interviews gehouden met het senior management (kwalitatieve gegevens) en de bevindingen van de interviews hebben bijgedragen aan de ontwikkeling van de gebieden die in de eerste (voornamelijk kwantitatieve) informatiebeveiligingsvragenlijst aan de orde komen. Het resultaat van dit verkennende proces is uiteindelijk de hypothese dat naarmate het kennisniveau van computergebruikers over informatiebeveiligingsbeleid en -procedures toeneemt, hun houding ten opzichte van informatiebeveiligingsbeleid en -procedures verbetert, wat zich zou moeten vertalen in meer risicomijdend gedrag op het gebied van informatiebeveiliging. Dit veranderingsproces wordt ook wel het KAB-model genoemd en een verfijnde en specifieke versie van dit model is een onderdeel van het HAIS-Q.
- In de literatuur bestaat meningsverschil aangaande de bruikbaarheid en validiteit van het KAB model. Kollmuss and Agyeman (2002) geven aan dat het model te rationeel is. Baranowski, Cullen, Nicklas, Thompshon, and Baranowski (2003) onderzochten de relevantie van het model op het gebied van

gezondheid, en concludeerden dat "de wetenschappelijke ondersteuning van de kenniscomponent van KAB-modellen zwak is" (p. 26S). Volgens McGuire (1969), zoals geciteerd in Parsons, McCormac, Butavicius, et al. (2013), is het probleem met het KAB-model echter niet het theoretische model zelf, maar de manier waarop het model wordt toegepast. In veel gevallen is het begrip kennis niet duidelijk gespecificeerd (Baranowski et al., 2003).
Op basis van de aanbeveling van McGuire (1969) is binnen het theoretische model achter de HAIS-Q het begrip kennis eerst geconceptualiseerd als 'kennis van beleid en procedures'. Binnen die verfijnde context zijn verschillende informatiebeveiligingsbeleidsregels herzien en de bevindingen van interviews met het senior management gebruikt om specifieke aandachtsgebieden te ontwikkelen. Deze waren bedoeld om de gebieden van een informatiebeveiligingsbeleid weer te geven die relevant zijn voor werkgevers en computergebruikers en die het meest vatbaar zijn voor niet-naleving. Op deze wijze zijn de zeven aandachtsgebieden geïdentificeerd. Per aandachtsgebied zijn 3 subgebieden ontwikkeld om per subgebied een stelling op elke dimensie van het KAB model (kennis, houding en gedrag) te ontwikkelen. De KAB component van de HAIS-Q bestaat daarmee uit 63 stellingen, elk te scoren op een 5 punt Likert-schaal. Op dezelfde wijze zou een aandachtsgebied toegevoegd kunnen worden.

- De relatie tussen kennis, houding en gedrag wordt beïnvloed door vele individuele, interventie- en organisatiefactoren. Daarom bevat het HAIS-Q specifieke items om elk van deze factoren te meten. De beoordeling van de invloed van deze factoren op KAB is initieel niet getoetst.
- Middels 3 technieken is de validiteit en betrouwbaarheid van de onderzoeksonderdelen getest, te weten:
  1) Expert toetsing door vragen naar begrip van de termen, de duidelijkheid van de richting en eventuele andere mogelijke misverstanden.
  2) Uitvoeren van een cognitieve test met een informatiebeveiliging expert, waarbij een combinatie van hardop denken en mondelinge toetsing wordt toegepast. De expert moest het onderzoek invullen in aanwezigheid van de onderzoekers en alles wat bij de beantwoording in gedachten kwam verbaliseren. Daar waar dit onduidelijk was, zijn aanvullende vragen gesteld.
  3) Pilotstudie waarbij de resultaten zijn onderzocht om eventuele resterende problemen op te sporen en de betrouwbaarheid van de belangrijkste onderdelen van het onderzoek vast te stellen. De deelnemers moesten het informatieblad en het toestemmingsformulier lezen en werden vervolgens gevraagd het HAIS-Q in te vullen. De vragenlijst werd online ingevuld. Cronbachs alfa is gebruikt als maatstaf voor de interne consistentie van het onderzoek. Dit verwijst naar de mate waarin de items dezelfde onderliggende constructie meten. Correlatieanalyse is gebruikt om de relatie tussen de items die gebruikt zijn om de drie hoofdconstructies te creëren verder te beoordelen.
- Onderzoeken waarin het model is uitgebreid of gewijzigd, maken gebruik van dezelfde methodiek die gebruikt is voor de initiële opzet.
- Extra toetsing op validiteit en betrouwbaarheid is gedaan door dezelfde meting op 2 momenten uit te voeren en de Cronbachs alfa van beide metingen met elkaar te vergelijken en door te zoeken naar correlatie tussen de resultaten van de twee metingen.
- Ook is de validiteit van de HAIS-Q getoetst door een maatregel voor gedrag te nemen en aan te tonen dat deze correleert met de theoretisch-gerelateerde meting van het IBB. Dit naast een studie onder een groot aantal respondenten.

### Stap 5. Het synthetiseren van de literatuur tot een raamwerk

#### *Deelvraag 1*

*L1 : Welke modellen zijn er binnen de literatuur te vinden die aantonen welke factoren een relatie hebben met de naleving van het informatiebeveiligingsbeleid en wordt de mate van IBB daarbinnen benoemd?*

Binnen de wetenschappelijke literatuur zijn veel onderzoeken te vinden die het onderwerp informatiebeveiliging behandelen. Dit is ook in lijn met het belang van het onderwerp in de steeds

verdergaande digitalisering van de samenleving en de daarbij behorende afhankelijkheid van informatiesystemen en data. In het verleden waren informatiebeveiligingsoplossingen grotendeels technisch van aard, met de nadruk op de ontwikkeling van hardware-, software- en netwerkoplossingen (Parsons, McCormac, Pattinson, et al., 2013). Naast technische oplossingen worden voor de beveiliging van de systemen en data ook organisatorische procedures, uit te voeren door medewerkers, ontwikkeld om informatiebeveiligingsmaatregelen te implementeren. Verschillende onderzoeken laten zien dat juist deze menselijke factor vaak oorzaak is van beveiligingsincidenten en daarmee een kritieke factor is binnen de informatiebeveiliging (Bragdon, 2018; Evans et al., 2019; Evans et al., 2016; Schultz, 2005). Veel onderzoeken binnen de literatuur zijn dan ook gericht op het onderkennen van factoren die het gedrag van deze medewerkers beïnvloeden.

Onderzoeken gericht op identificatie van factoren die informatiebeveiligingsgedrag beïnvloeden, maken veelal gebruik van gedragsmodellen die hun oorsprong vinden in de criminologie of de psychologie. Veelgebruikte gedragsmodellen zijn de Social Bond Theory (hierna: SBT) (Ifinedo, 2014), de Theory of Planned Behaviour van (hierna: TPB) (Bulgurcu et al., 2010; Cox, 2012; Haeussinger & Kranz, 2013; E. H. Park et al., 2018; Rocha Flores & Ekstedt, 2016), de Theory of Reasoned Action (hierna: TRA), de Protection Motivation Theory (hierna: PMT) (Cox, 2012; Kim et al., 2014; Vance et al., 2012), de General Deterrence Theory (hierna: GDT) (Chen et al., 2018; Choi & Song, 2018; D'arcy & Herath, 2011; D'Arcy et al., 2009; Y. S. Park et al., 2017), de Neutralization Theory (hierna: NT) (Kim et al., 2014; Siponen & Vance, 2010) en het Knowledge Attitude and Behaviour model (hierna: KAB model) (Kruger & Kearney, 2006).

Karjalainen and Siponen (2011) beweren dat veel literatuur zich alleen op verificatie of validatie van de gebruikte theorieën richt en zodoende een bevooroordeeld gezichtspunt hebben ten aanzien van de gekozen theorie. Daarnaast worden binnen deze onderzoeken over het algemeen alleen factoren bestudeert die uit de gebruikte theorie (gedragsmodel) naar voren komen, wat maakt dat deze onderzoeken veelal eenzijdig en/of onvolledig zijn. Dit is met name binnen onderzoek naar informatiebeveiliging een risico, omdat gedrag van medewerkers door vele factoren kan worden beïnvloed (Vroom & von Solms, 2004). Dit blijkt ook uit de literatuurstudie van Sommestad et al. (2014) die een overzicht geeft van onderzochte factoren en inzicht geeft in de factoren die bewezen van invloed zijn op gedrag.

Andere onderzoeken combineren verschillende gedragsmodellen in één onderzoek om zoveel mogelijk factoren of de factoren van interesse te kunnen testen (Bauer & Bernroider, 2017; Box & Pottas, 2014; Herath & Rao, 2009a, 2009b; Ifinedo, 2012, 2014; Rajab & Eydgahi, 2019; Siponen et al., 2014). Moody et al. (2018) zijn in hun onderzoek gestart met ontwikkelen van een uniform model. Onderzoeken waarin meerdere theorieën in één model worden samengevoegd, zonder wetenschappelijk bewijs dat deze samenvoeging geen ongewenste effecten heeft, zijn om die reden niet gebruikt binnen dit onderzoek.

Als we de verschillende modellen meer in detail bekijken zien we dat het merendeel van de modellen het gedrag of gewenste gedrag, veelal naleving van informatiebeveiligingsbeleid, als afhankelijke factor onderzoekt. De onafhankelijke en/of mediërende en/of modererende factoren zijn zeer veel en divers van aard en de verschillende onderzoeken variëren nog wel eens in de resultaten van vergelijkbare factoren, wat het onderzoek van Sommestad et al. (2014) bevestigt.

IBB als factor komt eveneens in meerdere onderzoeken naar voren (Al-Omari et al., 2012; Bauer & Bernroider, 2017; Bulgurcu et al., 2010; Chua et al., 2018; D'Arcy et al., 2009; Haeussinger & Kranz, 2013; E. H. Park et al., 2018; Y. S. Park et al., 2017; Rocha Flores & Ekstedt, 2016). De binnen deze onderzoeken gehanteerde definitie van IBB kan variëren. Enkele onderzoeken laten IBB zien als mediërende factor, in andere onderzoeken is IBB een onafhankelijke factor, maar binnen de onderzoeken waarin IBB als factor is benoemd wordt deze statistisch aangemerkt als een factor die van invloed is op het gedrag.

De vraag of informatiebeveiligingsbewustzijn een van belang zijnde factor is bij de naleving van informatiebeveiligings- en/of privacybeleid kan dus met ja worden beantwoord, waarmee het uitgangspunt van dit onderzoek is gevalideerd.

*Deelvraag 2*

*Welke gevalideerde methoden zijn er binnen de recente literatuur bekend om het IBB te meten en in hoeverre zijn deze bruikbaar binnen de gezondheidszorg?*

Uit verschillende onderzoeken komt naar voren dat IBB een factor van belang is bij de naleving van informatiebeveiligings- en/of privacybeleid. De wijze waarop IBB binnen genoemde onderzoeken is bepaald, is veelal op basis van een aantal algemene vragen welke op een 5- of 7-punts Likert-schaal worden gescoord. Een wetenschappelijk gevalideerde methode wordt binnen die onderzoeken niet gebruikt.

De bestaande literatuur is nog niet heel rijk als het gaat om gevalideerde methoden voor het meten van IBB. Literatuuronderzoek laat zien dat Kruger and Kearney (2006) zijn gestart met de ontwikkeling van een prototype voor het meten van IBB. Dit prototype is gebaseerd op het KAB model, wat onder andere in de sociale psychologie wordt gebruikt. Voor de ontwikkeling van dit prototype wordt via een top down benadering een waardeboom gecreëerd waarin de drie dimensies kennis (wat weet iemand), houding (wat vindt iemand van een onderwerp) en gedrag (wat doet iemand) zijn opgesplitst naar zes aandachtsgebieden en waar nodig zijn deze zes gebieden nog opgesplitst naar subcategorieën. Duidelijk werd dat niet elke factor in gelijke mate zou bijdragen aan de uiteindelijke meting van het bewustzijnsniveau. Hiertoe zijn belangengewichten aan de factoren toegevoegd. De wijze van meten is via vragenlijsten met in sommige gevallen 3 antwoordmogelijkheden (juist, onjuist, weet niet) en in andere gevallen 2 antwoordmogelijkheden (juist, onjuist). Het prototype van het model is getest bij het regionale kantoor in Australië.

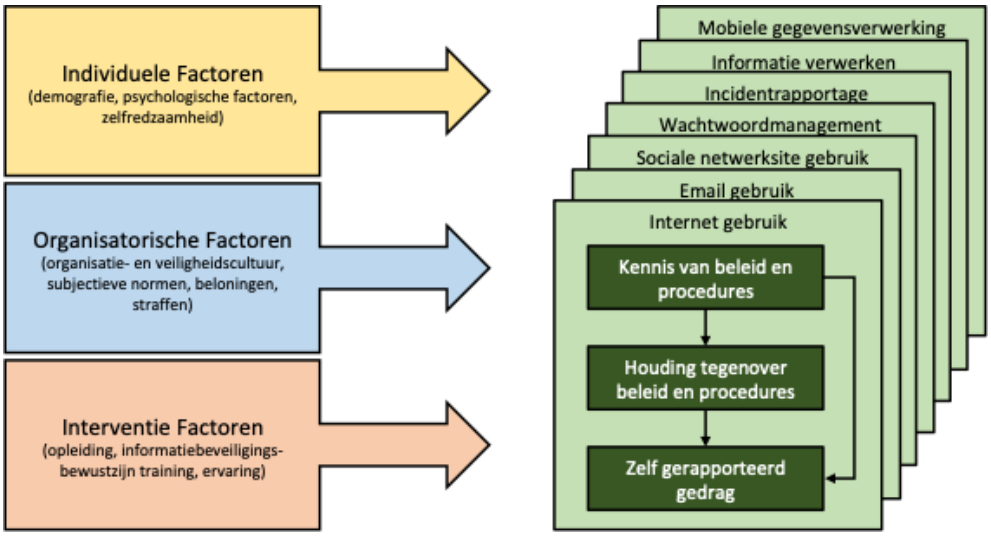
Op basis van dit prototype hebben Kruger et al. (2006) een framework voor de evaluatie van IBB ontwikkeld. Het framework heeft als extra toevoeging dat systeemdata wordt geanalyseerd om het daadwerkelijk beveiligingsgedrag van de medewerkers te bepalen. Het model voor de meting van het IBB wordt vervolgens samengesteld op basis van de enquête- en systeemdata en de wegingsfactoren. Nadat het framework is opgezet, is dit toegepast in een universitaire omgeving conform de voorgestelde aanpak in het framework.

Parsons, McCormac, Pattinson, et al. (2013) ontwikkelden de, eveneens gebruikmakend van aandachtsgebieden en gebaseerd op het KAB model, Human Aspects of Information Security Questionnaire (hierna: HAIS-Q) om het IBB te meten. Om een zo onbevooroordeeld mogelijk instrument te ontwikkelen, is bij de ontwikkeling gebruik gemaakt van zowel kwantitatieve als kwalitatieve onderzoeksmethoden (Parsons, McCormac, Butavicius, et al., 2013), een aanpak die aanbevolen wordt door Karjalainen and Siponen (2011). Bij de ontwikkeling onderkennen zij dat er naast de dimensies kennis en houding meerdere factoren zijn die van invloed zijn op het gedrag. Dit is in overeenstemming met het onderzoek van Vroom and von Solms (2004) en Sommestad et al. (2014). Hiertoe nemen ze in hun ontwikkelde HAIS-Q ook individuele, organisatorische en interventiefactoren op. Een eerste validatie laat positieve resultaten zien.

Verdere validatie en mogelijke uitbreiding van de HAIS-Q heeft plaatsgevonden binnen de onderzoeken van McCormac et al. (2016); McCormac et al. (2017); Parsons et al. (2017); Parsons et al. (2014); Schaeken (2018); Wissen (2017), waarbij het instrument steeds breder is getoetst. Naast het feit dat ook deze onderzoeken positieve resultaten laten zien aangaande het gebruik van de HAIS-Q, worden ook suggesties gedaan voor vervolgonderzoek om het instrument te verbeteren.

Binnen andere onderzoeken zijn eveneens methoden ontwikkeld voor het meten van IBB (Egelman & Peer, 2015; Öğütçü et al., 2015; Rezgui & Marks, 2008; Velki et al., 2014). Deze methoden zijn echter alleen in het eigen onderzoek gevalideerd. Verdere validatie van deze methoden heeft naar mijn weten niet plaatsgevonden.

Concluderend kan gesteld worden dat het aantal gevalideerde methoden voor het meten van IBB zeer gering is, waarbij het meten van IBB gebruikmakend van de HAIS-Q als de meest gevalideerde methode wordt beschouwd. Onderstaande afbeelding geeft de opzet van de HAIS-Q weer.




Afbeelding 2 HAIS Model

Naast een gevalideerd model, is een andere voorwaarde voor bruikbaarheid van een model binnen de gezondheidszorg het kunnen meten van bewustzijn op het gebied van privacy. Uit afbeelding 1 wordt zowel duidelijk dat binnen het model rekening wordt gehouden met de relatie van factoren met de naleving van informatiebeveiligingsbeleid, waarvan de waarde ook onderkend wordt in het onderzoek van Siponen (2001) als dat het model geschikt is om IBB in zijn algemeenheid te meten. Echter het model laat ook zien dat het aandachtsgebied privacy ontbreekt. Parsons et al. (2017) hebben in hun artikel als suggestie voor vervolgonderzoek aangegeven dat de relatie tussen IBB en privacybelangen verder zou kunnen worden onderzocht, door opname van maatregelen van privacybelangen en –gedrag.

Als antwoord op de vraag welke gevalideerde methoden er binnen de recente literatuur bekend zijn om het IBB te meten kan worden gesteld dat de HAIS-Q de meest gevalideerde methode is. Op de vraag of deze methode ook bruikbaar is binnen de gezondheidszorg, is het antwoord dat deze methode een uitermate geschikte basis biedt. Echter het model behoeft uitbreiding met het aspect privacy.

### *Deelvraag 3*

*Is het mogelijk om bestaande methoden voor het meten van IBB door te ontwikkelen en vervolgens te valideren, en zo ja op welke wijze?*

Voor de initiële model ontwikkeling hebben Parsons, McCormac, Butavicius, et al. (2013) gebruik gemaakt van een hybride onderzoeksmethode, waarbij de inductieve, verkennende aanpak is opgenomen die wordt aanbevolen door Karjalainen and Siponen (2011). Hybride om een mix van kwalitatieve en kwantitatieve methoden voor het verzamelen en analyseren van gegevens aan te duiden. Ten behoeve van de ontwikkeling van de informatiebeveiligingsvragenlijst, zijn interviews gehouden met het senior management.

Het resultaat van dit verkennende proces is uiteindelijk de hypothese dat naarmate het kennisniveau van computergebruikers over informatiebeveiligingsbeleid en -procedures toeneemt, hun houding ten opzichte van informatiebeveiligingsbeleid en -procedures verbetert, wat zich zou moeten vertalen in meer risicomijdend gedrag op het gebied van informatiebeveiliging. Dit veranderingsproces wordt ook wel het KAB-model genoemd en een verfijnde en specifieke versie van dit model is een onderdeel van het HAIS-Q.

In de literatuur bestaat meningsverschil aangaande de bruikbaarheid en validiteit van het KAB model. Kollmuss and Agyeman (2002) geven aan dat het model te rationeel is. Baranowski et al. (2003) onderzochten de relevantie van het model op het gebied van gezondheid, en concludeerden dat "de wetenschappelijke ondersteuning van de kenniscomponent van KAB-modellen zwak is" (p. 26S). Volgens McGuire (1969), zoals geciteerd in Parsons, McCormac, Butavicius, et al. (2013), is het probleem met het KAB-model echter niet het theoretische model zelf, maar de manier waarop het model wordt toegepast.

In veel gevallen is het begrip kennis niet duidelijk gespecificeerd (Baranowski et al., 2003). Op basis van de aanbeveling van McGuire (1969) is binnen het theoretische model het begrip kennis eerst geconceptualiseerd als 'kennis van beleid en procedures'. Binnen die verfijnde context zijn verschillende informatiebeveiligingsbeleidsregels herzien en de bevindingen van interviews met het senior management gebruikt om specifieke aandachtsgebieden te ontwikkelen. Deze waren bedoeld om de gebieden van een informatiebeveiligingsbeleid weer te geven die relevant zijn voor werkgevers en computergebruikers en die het meest vatbaar zijn voor niet-naleving. Op deze wijze zijn de zeven aandachtsgebieden geïdentificeerd. Per aandachtsgebied zijn 3 subgebieden ontwikkeld om per subgebied een stelling op elke dimensie van het KAB model (kennis, houding en gedrag) te ontwikkelen. De KAB component van de HAIS-Q bestaat daarmee uit 63 stellingen, elk te scoren op een 5 punt Likert-schaal.

Parsons, McCormac, Butavicius, et al. (2013) hebben vervolgens middels 3 technieken de validiteit en betrouwbaarheid van de onderzoeksonderdelen getest, te weten:

4) Expert toetsing door vragen naar begrip van de termen, de duidelijkheid van de richting en eventuele andere mogelijke misverstanden.
5) Uitvoeren van een cognitieve test met een informatiebeveiliging expert, waarbij een combinatie van hardop denken en mondelinge toetsing wordt toegepast. De expert moest het onderzoek invullen in aanwezigheid van de onderzoekers en alles wat bij de beantwoording in gedachten kwam verbaliseren. Daar waar dit onduidelijk was, zijn aanvullende vragen gesteld.
6) Pilotstudie waarbij de resultaten zijn onderzocht om eventuele resterende problemen op te sporen en de betrouwbaarheid van de belangrijkste onderdelen van het onderzoek vast te stellen. De deelnemers moesten het informatieblad en het toestemmingsformulier lezen en werden vervolgens gevraagd het HAIS-Q in te vullen. De vragenlijst werd online ingevuld. Cronbachs alfa is gebruikt als maatstaf voor de interne consistentie van het onderzoek. Dit verwijst naar de mate waarin de items dezelfde onderliggende constructie meten. Correlatieanalyse is gebruikt om de relatie tussen de items die gebruikt zijn om de drie hoofdconstructies te creëren verder te beoordelen.

McCormac et al. (2016) hebben daarnaast de validiteit en betrouwbaarheid van het model getest door dezelfde meting op 2 momenten uit te voeren en de Cronbachs alfa van beide metingen met elkaar te vergelijken en door te zoeken naar correlatie tussen de resultaten van de twee metingen.

Binnen het onderzoek van Parsons et al. (2017) is de validiteit van de HAIS-Q getoetst door een maatregel voor gedrag te nemen en aan te tonen dat deze correleert met de theoretisch-gerelateerde meting van het IBB. Dit naast een studie onder een groot aantal respondenten.

Andere onderzoeken die de HAIS-Q uitbreiden, wijzigen en/of valideren (Parsons et al., 2014; Parsons, McCormac, Pattinson, et al., 2013; Schaeken, 2018; Wissen, 2017) maken allen gebruik van hybride methodieken zoals gebruikt bij de ontwikkeling van het model. Wissen (2017) geeft in zijn onderzoek aan dat het ten behoeve van de validiteit goed zou zijn om de vragenlijst voorafgaand te toetsen op relevantie voor de organisatie en/of branche van onderzoek. Ook geeft hij aan dat de betrouwbaarheid van het model kan worden vergroot door te kijken naar daadwerkelijk gedrag in plaats van zelf gerapporteerd gedrag. De verhoging van de interne validiteit kan volgens Wissen (2017) bereikt worden door de verschillende vragen uit de HAIS-Q te voorzien van meer context.

Het antwoord op de vraag of het mogelijk is om bestaande methoden voor het meten van IBB door te ontwikkelen en vervolgens te valideren is ja. Op de vraag op welke wijze dit kan geschieden, is het antwoord dat hiervoor een combinatie van methodieken gebruikt kan worden. Voor de uitbreiding van het model met een aandachtsgebied kunnen op basis van documentenstudie en interviews binnen de te onderzoeken branche subgebieden met stellingen per dimensie worden ontwikkeld. Tevens kunnen op deze wijze de bestaande aandachtsgebieden worden getoetst voor toepassing binnen de branche. De uiteindelijke vragenlijst kan worden gevalideerd middels een pilot studie waarbij de resultaten statistisch worden onderzocht.

## Referenties literatuuronderzoek


Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Information security policy compliance: The role of information security awareness.

Baranowski, T., Cullen, K. W., Nicklas, t., Thompshon, D., & Baranowski, J. (2003). Are current health behavioral change models helpful in guiding prevention of weight gain efforts? *Obesity research, 11*(October), 23S-43S.

Bauer, S., & Bernroider, E. (2017). From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 48*(3), 44-68. doi:10.1145/3130515.3130519

Box, D., & Pottas, D. (2014). A Model for Information Security Compliant Behaviour in the Healthcare Context. *Procedia Technology, 16*, 1462-1470. doi:10.1016/j.protcy.2014.10.166

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523-548. doi:10.2307/25750690

Chen, X., Chen, L., Wu, D., & Teng, J. K. L. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management, 55*(8), 1049-1060. doi:10.1016/j.im.2018.05.011

Choi, M., & Song, J. (2018). Social control through deterrence on the compliance with information security policy. *Soft Computing, 22*(20), 6765-6772. doi:10.1007/s00500-018-3354-z

Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. *Telematics and Informatics, 35*(6), 1770-1780. doi:10.1016/j.tele.2018.05.005

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior, 28*(5), 1849-1858. doi:10.1016/j.chb.2012.05.003

D'arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems, 20*(6), 643-658.

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, 20*(1), 79-98. doi:10.1287/isre.1070.0160

Egelman, S., & Peer, E. (2015). *Scaling the security wall: Developing a security behavior intentions scale (sebis).* Paper presented at the Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems.

Evans, M., He, Y., Maglaras, L., & Janicke, H. (2019). HEART-IS: A novel technique for evaluating human error-related information security incidents. *Computers & Security, 80*, 74-89. doi:10.1016/j.cose.2018.09.002

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks, 9*(17), 4667-4679. doi:10.1002/sec.1657

Haeussinger, F., & Kranz, J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behavior.

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.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165. doi:10.1016/j.dss.2009.02.005

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95. doi:10.1016/j.cose.2011.10.007

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69-79. doi:10.1016/j.im.2013.10.001

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), 518-555.
Kim, S. H., Yang, K. H., & Park, S. (2014). An Integrative Behavioral Model of Information Security Policy Compliance. *SCIENTIFIC WORLD JOURNAL, 2014*, 463870-463812. doi:10.1155/2014/463870
Kollmuss, A., & Agyeman, J. (2002). Mind the gap: why do people act environmentally and what are the barriers to pro-environmental behavior? *Environmental education research, 8:3*(August), 239-260.
Kruger, H. A., Drevin, L., & Steyn, T. (2006). *A Framework for Evaluating ICT Security Awareness.* Paper presented at the ISSA.
Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289-296. doi:10.1016/j.cose.2006.02.008
McCormac, A., Calic, D., Parsons, K., Zwaans, T., Butavicius, M., & Pattison, M. (2016). Test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q).
McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior, 69*, 151-156. doi:10.1016/j.chb.2016.11.065
McGuire, W. J. (1969). The nature of attitudes and attitude change. *3*.
Moody, G. D., Siponen, M., Pahnila, S., University of Nevada, L. V., University of, J., & University of, O. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42*(1), 285-285. doi:10.25300/MISQ/2018/13853
Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2015). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83-93. doi:10.1016/j.cose.2015.10.002
Park, E. H., Kim, J., Wiles, L. L., & Park, Y. S. (2018). Factors affecting intention to disclose patients' health information. *Computers & Security*.
Park, Y. S., Park, E. H., & Kim, J. (2017). The role of information security learning and individual factors in disclosing patients' health information. *Computers & Security, 65*, 64-76. doi:10.1016/j.cose.2016.10.011
Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 66*, 40-51. doi:10.1016/j.cose.2017.01.004
Parsons, K., McCormac, A., Butavicius, M., Ferguson, L., Defence, S., Technology Organisation Edinburgh Command Control, C., & Intelligence, D. I. V. (2010). Human Factors and Information Security: Individual, Culture and Security Environment. In.
Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2013, 2013). *The development of the human aspects of information security questionnaire (HAIS-Q)*.
Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165-176. doi:10.1016/j.cose.2013.12.003
Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013). A study of information security awareness in Australian government organisations. *Information Management & Computer Security, 22*(4), 334-345. doi:10.1108/IMCS-10-2013-0078
Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security, 80*, 211-223. doi:10.1016/j.cose.2018.09.016
Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security, 27*(7), 241-253. doi:10.1016/j.cose.2008.07.008
Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security, 59*, 26-44. doi:10.1016/j.cose.2016.01.004
Schaeken, M. (2018). *Information security awareness measuring & social engineering 2.0.* (Thesis). Open Universiteit,
Siponen, M. (2001). Five dimensions of information security awareness. *ACM SIGCAS Computers and Society, 31*(2), 24-29. doi:10.1145/503345.503348
Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies:

An exploratory field study. *Information & Management, 51*(2), 217-224. doi:10.1016/j.im.2013.08.006
Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly, 34*(3), 487-502. doi:10.2307/25750688
Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: a systematic review of quantitative studies. *Information Management & Computer Security, 22*(1), 42-75.
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. doi:10.1016/j.im.2012.04.002
Velki, T., Solic, K., & Ocevcic, H. (2014). *Development of Users' Information Security Awareness Questionnaire (UISAQ)—Ongoing work.* Paper presented at the 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).
Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198. doi:10.1016/j.cose.2004.01.012
Wissen, D. v. (2017). *Meten van informatiebeveiligingsbewustzijn.* (Thesis). Open Universiteit,

# Bijlage A Samenvattingen geschikte publicaties beantwoording deelvraag 1

## D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach

### *Doel van het onderzoek*

Het ontwerpen en empirisch testen van een model, gebaseerd op de algemene afschrikkingstheorie, dat stelt dat gebruikersbewustzijn van beveiligingsmaatregelen (beleid, educatie, training, bewustzijn programma's en monitoring van gebruik) rechtstreeks van invloed is op de perceptie van de gebruiker over de zekerheid en ernst van sancties in geval van misbruik. Dit heeft vervolgens direct invloed op de intentie tot misbruik.

### *Opzet van het onderzoek*

Het uitgevoerde literatuuronderzoek laat zien dat strategieën voor het reduceren van risico's in vier stadia uiteen vallen, te weten: afschrikking, preventie, detectie en herstel, bekend onder de naam 'Cyclus van Beveiligingsacties'. Dit onderzoek richt zich op de eerste stap, het afschrikken, door middel van een mix van procedurele en technische controles. Eerder onderzoek heeft aangetoond dat deze maatregelen effect hebben, maar eerder onderzoek heeft dit niet bekeken vanuit het oogpunt van de gebruiker. Wat is de impact van beveiligingsmaatregelen als de gebruiker zich bewust is van deze maatregelen. De auteurs stellen dat zowel waargenomen kans van de gebruiker op de zekerheid van straf als op de hoogte van de straf invloed hebben op de intentie tot misbruik. Het bewustzijn van elk van de beveiligingsmaatregelen (beleid, educatie, training, bewustzijn programma's en monitoring van gebruik) zal de waargenomen kans van de gebruiker doen stijgen. Voor het meten van de factoren wordt gebruik gemaakt van een enquête, waarbij voor het meten van verschillende constructen scenario's zijn gebruikt. Deze methode is succesvol gebruikt in eerder onderzoek. De literatuur is onderzocht op valide maatregelen waarbij gebruikersbewustzijn of percepties van veiligheidsmaatregelen in aanmerking werden genomen. Bestaande maatregelen zijn echter of geoperationaliseerd op organisatieniveau of zijn geschreven vanuit het perspectief van beveiligingsbeheerders. Daarom zijn voor dit onderzoek originele schalen ontwikkeld die het bewustzijn meten van beveiligingsbeleidsmaatregelen. Een voorlopige versie van het volledige meetinstrument werd getest op duidelijkheid en validiteit. Het empirische onderzoek heeft plaats gevonden met 269 respondenten.

### *Resultaten en conclusies van het onderzoek*

Het onderzoek laat zien dat de waargenomen kans van de gebruiker op de zekerheid van straf geen significant effect heeft op de op de intentie tot misbruik, de waargenomen ernst van de sancties heeft dat effect wel, zelfs een groot effect. Daarnaast laat het onderzoek zien dat bewustzijn van beleid geen effect heeft op de waargenomen zekerheid van sancties, wel op de waargenomen ernst. Educatie, training, bewustzijn programma's en bewustzijn van monitoring van gebruik hebben zowel effect op de waargenomen zekerheid van sancties als op de waargenomen ernst. Controlefactoren blijken ook effect te hebben op de intentie tot misbruik.

Dit onderzoek levert vooruitgang op in de verklaring van de relaties tussen beveiligingsmaatregelen, sanctiepercepties en misbruik. De resultaten suggereren dat gebruikersbewustzijn van beleid, educatie, training, bewustzijn programma's en monitoring van gebruik elk een afschrikwekkend effect hebben op misbruik, en dit effect wordt indirect bereikt door de waargenomen zekerheid en / of strengheid van de sancties. Er zijn ook aanwijzingen dat de invloeden van sanctiepercepties variëren op basis van iemands moraliteitsniveau. Vanuit een theoretisch perspectief introduceert het onderzoek een uitgebreide versie van de algemene afschrikkingstheorie en bevestigt de toepasbaarheid ervan op het informatiebeveiligingsdomein. Deze studie voegt ook toe aan eerdere op afschrikking gebaseerde beoordelingen van beveiligingsmaatregelen door de twee belangrijkste constructen van deze algemene afschrikkingstheorie (waargenomen zekerheid en strengheid van sancties) direct te meten.

### *Suggesties voor verder onderzoek*

Genoemde suggesties voor toekomstig onderzoek zijn:

- Onderzoek de invloeden van verschillende organisatorische kenmerken op misbruikintentie en de effectiviteit van beveiligingsmaatregelen daarbinnen;
- Onderzoek het model opnieuw in een context waarin feitelijk misbruik kan worden gemeten om extra geloofwaardigheid aan het model toe te voegen;
- Doe onderzoek om de verklarende kracht van het model te testen op een groter aantal misbruikgedragingen;
- Onderzoek het model in duidelijk verschillende nationale culturen buiten de Verenigde Staten om het model verder te valideren.

*Relevantie voor het eigen onderzoek*

- Het opgezette model is een uitbreiding van het model uit de voorgaande publicatie door de opname van de factor bewustzijn van verschillende beveiligingsmaatregelen. Het meten van deze factor is gebeurd door de opzet van een eigen meetmethode met 7 punt Likert-schaal.
- Dit onderzoek bekijkt de afhankelijke factor intentie tot informatiesysteem misbruik wat een negatieve factor is ten opzichte van intentie tot naleving van beveiligingsregels. De resultaten moeten dan ook omgekeerd bekeken worden. Resultaten zijn wel in lijn met de voorgaande publicatie.

### Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness

*Doel van het onderzoek*

Het doel van dit onderzoek is om de kennis aangaande de naleving van informatiebeveiligingsregels door werknemers te vergroten door factoren die hierop van invloed zijn te identificeren. Binnen dit onderzoek willen de onderzoekers onder andere inzicht krijgen in de rol van IBB bij het vormgeven van de overtuigingen van een werknemer over de resultaten en de houding ten opzichte van naleving van het informatiebeveiligingsbeleid.

*Opzet van het onderzoek*

Op basis van de 'Theory of Planned Behaviour' is een onderzoeksmodel opgezet dat de intentie van een werknemer om te voldoen aan het informatiebeveiligingsbeleid verklaart. Dit model wordt getoetst door middel van een enquête. De vragen uit de enquête zijn gemaakt op basis van onderzoek in de literatuur en de empirie en vooraf getoetst middels feedback vragen en interviews. De vragen en bijbehorende antwoordschalen zijn in twee pilotgroepen getest, alvorens de enquête door een onderzoeksbureau uit te laten zetten onder een groep van 3150 respondenten van verschillende organisaties.

*Resultaten en conclusies van het onderzoek*

De resultaten van het onderzoek laten zien dat de houding van een werknemer ten opzichte van naleving, samen met de normatieve overtuiging en zelfredzaamheid, bepalend is voor de intentie om te voldoen aan het informatiebeveiligingsbeleid. Als belangrijke bijdrage stellen de onderzoekers dat de houding van een werknemer is beïnvloed door het voordeel van de naleving, de kosten van de naleving en de kosten van niet-naleving, wat overtuigingen zijn over de algemene beoordeling van de gevolgen van de naleving of niet-naleving. Vervolgens stellen de onderzoekers dat deze overtuigingen worden gevormd door de uitkomst van de overtuigingen van de werknemer met betrekking tot de gebeurtenissen die volgen op de naleving of niet-naleving: het voordeel van de naleving wordt gevormd door het intrinsieke voordeel, de veiligheid van de middelen, en beloningen, terwijl de kosten van naleving worden bepaald door de werklast; en de kosten van niet-naleving worden bepaald door de intrinsieke kosten, de kwetsbaarheid van de middelen en de sancties.

Ook is de impact van IBB op de resultaatovertuigingen en de houding van een werknemer ten opzichte van de naleving van het informatiebeveiligingsbeleid onderzocht. De resultaten laten zien dat IBB een positief effect heeft op zowel de houding als de resultaatovertuiging van de werknemer.

*Suggesties voor verder onderzoek*

Genoemde suggesties voor toekomstig onderzoek zijn:

- In dit onderzoek wordt de intentie tot naleving gemeten in plaats van de werkelijke naleving en het IBB wordt gemeten op basis van waarnemingen, daar waar dit ook zou kunnen op een meer objectieve basis. Toekomstig onderzoek zou een studie kunnen betreffen gericht op medewerkers van 1 of enkele organisaties om de daadwerkelijke naleving te meten en het IBB op meer objectieve basis.
- Omdat we hebben vastgesteld dat IBB een belangrijke rol speelt in het gedrag van de medewerkers, is een andere vruchtbare onderzoeksrichting het onderzoeken van de dimensies van IBB. Met name het identificeren van de factoren die leiden tot IBB zou een belangrijke bijdrage leveren aan de academische wereld, aangezien er een leemte is in de literatuur in deze richtlijn. Dergelijk onderzoek zou ook nuttig zijn voor de praktijk, omdat ze die factoren kunnen gebruiken om hun IBB-programma's te formuleren.
- Onderzoekers zouden ook de soorten IBB kunnen onderzoeken die bestaan op verschillende niveaus van de organisatiehiërarchie, aangezien verschillende aspecten van bewustzijn effectiever kunnen zijn in het veranderen van percepties voor werknemers op verschillende niveaus. Terwijl bijvoorbeeld vertegenwoordigers van klanten de gevolgen van een informatiebeveiligingsvraagstuk beter begrijpen in termen van hoe de klantrelaties worden beïnvloed, kunnen de verkoopmanagers dat beter doen in termen van omzetverlies. Dit soort verschillen tussen medewerkers kunnen worden

gebruikt om bewustwordingsprogramma's op maat te maken voor medewerkers op verschillende niveaus in de organisatie.

- Respondenten in deze studie hebben zelf aangegeven dat ze van plan zijn om te voldoen aan de eisen van het informatiebeveiligingsbeleid en het is mogelijk dat sommigen hun ware intenties verborgen hielden omdat zij het niet naleven van de regels als sociaal ongewenst beschouwden. Een manier om deze beperking te verlichten is het gebruik van scenario's (Siponen & Vance, 2010) die een rijkere beschrijving van een hypothetische werknemer geven en indirect vragen stellen over de overtuigingen van de respondent via de situatie van de werknemer in het hypothetische scenario. Een andere beperking van het onderzoek kan zijn dat het de naleving van de voorschriften op een hoog abstractieniveau vastlegt. Het gebruik van scenario's kan helpen om de verschillen aan het licht te brengen in de intentie van een werknemer om zich aan specifieke regels en regelgeving te houden, aangezien scenario's gedetailleerde uitleg kunnen geven over specifiek beleid (d.w.z. wachtwoordbeleid, beleid over internetgebruik, beleid inzake toegang op afstand, enzovoort). Vandaar dat toekomstige onderzoek het nalevingsgedrag van werknemers met deze specifieke beleidsmaatregelen kan onderzoeken door gedetailleerde scenario's te verstrekken.
- In dit onderzoek worden sancties weergegeven als verschillende vormen van sancties die de organisatie aan een werknemer kan opleggen voor het niet naleven van het beleid. Afschrikkingsliteratuur heeft betoogd dat ernst, zekerheid en snelheid belangrijke factoren zijn om te bepalen hoeveel afschrikking een sanctie kan bieden. Aangezien deze factoren niet in aanmerking zijn genomen, kan toekomstig onderzoek onderzoeken hoe de ernst, de zekerheid en de snelheid van de sancties van invloed zijn op de perceptie van de werknemer van de kosten van het niet-nakomen van de verplichtingen van naleving.
- Een onderzoeksrichting zou zijn om de gezamenlijke rol van op gevolgen gebaseerde motivaties en moraliteit/waarden op het nalevingsgedrag van medewerkers te onderzoeken.
- Tot slot richtte dit onderzoek zich op individuele factoren die leiden tot naleving of niet-naleving, maar toekomstig onderzoek zou de impact van organisatorische factoren kunnen onderzoeken, zoals organisatorische sancties (bv. het verliezen van klanten, het voeren van een rechtszaak, het oplopen van financiële schade) of beloningen (bv. het verhogen van de betrouwbaarheid, de reputatie en het goede imago) op de houding van een werknemer ten opzichte van naleving. Een andere uitbreiding van het onderzoek langs deze lijn kan zowel individuele factoren als institutionele factoren omvatten om de intentie tot naleving te verklaren en om het relatieve belang van deze factoren te bestuderen bij het vormgeven van de intentie van een werknemer om te voldoen aan het informatiebeveiligingsbeleid.

*Relevantie voor het eigen onderzoek*

- IBB wordt in dit model als factor benoemd, waarbij het opgebouwd wordt uit het bewustzijn van de medewerker van het informatiebeveiligingsbeleid van de organisatie en het algemene bewustzijn van een medewerker over informatiebeveiliging.
- Het effect van een medewerkers IBB op de intentie tot naleving wordt gedeeltelijk bemiddeld door de houding van de medewerker
- Een medewerkers IBB heeft, zoals in eerdere literatuur aangegeven, een directe significante invloed op de houding van een medewerker ten aanzien van naleving.
- Een medewerkers IBB heeft een negatief effect op de werkbelemmering en een positief effect op de 6 andere factoren die het geloof in een uitkomst beïnvloeden.

### Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Information security policy compliance: The role of information security awareness

*Doel van het onderzoek*

Het doel van dit onderzoek is het verkrijgen van inzicht in de factoren die van invloed zijn op de intentie tot naleving van het informatiebeveiligingsbeleid.

*Opzet van het onderzoek*

Om de hypotheses te testen, hebben de onderzoekers gebruik gemaakt van een enquête, welke is uitgezet bij 2117 willekeurig gekozen werknemers van negen verschillende banken in Jordanië. Deze werknemers zijn werkzaam in verschillende functies en/of afdelingen.

Ten behoeve van de validiteit zijn de enquêtevragen gebaseerd op eerder uitgevoerd en gevalideerd onderzoek. Op basis van feedback van experts zijn de vragen aangescherpt en middels een pilot getest onder 205 respondenten van vier verschillende banken. De enquête is valide en betrouwbaar gebleken.

*Resultaten en conclusies van het onderzoek*

Dit onderzoek is volgens de onderzoekers het eerste onderzoek dat ingaat op de rol van de algemene kennis van gebruikers over informatiebeveiligingskwesties met betrekking tot hun houding ten aanzien van naleving van informatiebeveiligingsregels. Het resultaat suggereert dat de houding van een werknemer ten aanzien van de naleving van het informatiebeveiligingsbeleid kan worden verbeterd door zijn/haar algemene beveiligingsbewustzijn. Wat betreft de kennis en het inzicht van werknemers in technologieën op het gebied van beveiliging, bleek uit het onderzoek dat dit ook een significant positief effect heeft op de houding. Verder suggereren de resultaten dat de kennis van werknemers over beveiligingskwesties en -technologieën hun perceptie van hun eigen prestatievermogen om aan informatiebeveiligingsregels te voldoen, verbetert. Over het algemeen impliceren deze bevindingen dat het creëren van een veiligheidsbewuste cultuur binnen de organisatie de houding en het gedrag van gebruikers zal bepalen om meer veiligheidsbewust te zijn.

*Suggesties voor verder onderzoek*

Gesuggereerd wordt dat toekomstige studies andere organisatorische factoren, zoals de organisatiecultuur, in het bestaande model kunnen opnemen.

*Relevantie voor het eigen onderzoek*

Dit onderzoek toont aan dat IBB van invloed is op de intentie tot naleving van het informatiebeveiligingsbeleid.

### Haeussinger, F., & Kranz, J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behavior

*Doel van het onderzoek*

Het doel van dit onderzoek is om het beperkte onderzoek naar IBB aan te vullen en gaat dieper in op de stelling van Siponen (2000) dat "IBB één van de belangrijkste antecedenten van gedrag is" door de belangrijke, maar onder bestudeerde, bemiddelende rol van IBB in de relatie tussen de antecedenten van IBB en de intentie om te voldoen aan het beveiligingsbeleid te onderzoeken.

*Opzet van het onderzoek*

Om hun model te testen hebben de onderzoekers een enquête uitgevoerd. Respondenten werden gevonden via e-mail en het plaatsen van links met behulp van meerdere distributiekanalen, zoals on- en offline bedrijfsnetwerken, business portals en universitaire alumniverenigingen. De uiteindelijke steekproefomvang bestaat dus uit 475 respondenten.

*Resultaten en conclusies van het onderzoek*

De resultaten van het onderzoek tonen aan dat verschillende institutionele, individuele en omgevingsfactoren die in voorgaand onderzoek als directe antecedenten van veiligheidsgedrag zijn beschouwd, in feite ten minste gedeeltelijk door IBB worden bemiddeld. Dit onderzoek verfijnt dus voorafgaand onderzoek en dient als uitgangspunt voor verder onderzoek naar de rol van IBB op het nalevingsgedrag aangaande informatiebeveiligingsbeleid.

*Suggesties voor verder onderzoek*

Genoemde suggesties voor toekomstig onderzoek zijn:

- De procedure voor het verzamelen van gegevens was geografisch beperkt tot West-Europa. Om de bevindingen te veralgemenen is toekomstig onderzoek nodig om rekening te houden met culturele verschillen, die van bijzonder belang kunnen zijn voor multinationale organisaties.
- Toekomstig onderzoek zou uit kunnen gaan van daadwerkelijk gedrag in plaats van intentie tot gedrag om het model te beoordelen.
- Toekomstig onderzoek zou dieper kunnen ingaan op de "zwarte doos" van trainingsprogramma's voor IBB. Veldexperimenten die het IBB van medewerkers voor en na de trainingsprogramma's analyseren, zouden in dit opzicht een wezenlijke bijdrage kunnen leveren aan ons begrip van de opkomst van IBB van medewerkers.

*Relevantie voor het eigen onderzoek*

Dit onderzoek toont aan dat IBB, zij het bemiddelend, van invloed is op de intentie tot naleving van het informatiebeveiligingsbeleid.

### Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness

*Doel van het onderzoek*

Dit onderzoek heeft als doel om te bepalen hoe organisatorische en individuele factoren elkaar aanvullen bij het vormgeven van de intentie van werknemers om sociale aanvallen tegen het informatiebeveiligingsbeleid te weerstaan.

*Opzet van het onderzoek*

Het onderzoek volgde een 'mixed methods research design', waarin kwalitatieve gegevens werden verzameld om zowel het model van het onderzoek vast te stellen als om een onderzoeksinstrument te ontwikkelen dat werd verspreid onder 4296 organisatorische werknemers van diverse organisaties in Zweden.

*Resultaten en conclusies van het onderzoek*

De resultaten toonden aan dat de houding ten opzichte van het verzet tegen sociale aanvallen de sterkste directe associatie heeft met de intentie om zich te verzetten, terwijl zowel de zelfredzaamheid als de normatieve overtuigingen een zwakke relatie laten zien met de intentie om zich te verzetten. Bovendien toonden de resultaten aan dat transformationeel leiderschap sterk geassocieerd was met zowel de gepercipieerde informatiebeveiligingscultuur als het IBB. Twee bemiddelingstests toonden aan dat houding en normatieve overtuigingen gedeeltelijk het effect van de informatiebeveiligingscultuur op de intentie van werknemers om zich te verzetten tegen sociale aanvallen bemiddelen. Dit suggereert dat zowel houding als normatieve overtuigingen een belangrijke rol spelen in de relatie tussen informatiebeveiligingscultuur en de intentie om weerstand te bieden aan sociale aanvallen. Een derde bemiddelingstest toonde aan dat informatiebeveiligingscultuur het effect van transformationeel leiderschap op de houding van werknemers ten opzichte van het weerstaan van sociale aanvallen volledig verklaart.

*Suggesties voor verder onderzoek*

Genoemde suggesties voor toekomstig onderzoek zijn:

- Onderzoek naar het potentiële matigende effect van zelfwerkzaamheid tussen de intentie en het feitelijke gedrag.
- Ondanks dat het onderzoek identificeerde dat de houding ten opzichte van het weerstaan van sociale aanvallen sterk de gedragsintentie voorspelt, hebben de factoren die variaties in attitudes verklaren een zwakke verklarende kracht. Daarom moet toekomstig onderzoek ofwel andere of meer variabelen bevatten die potentieel sterker bepalend zijn voor de houding ten opzichte van het zich verzetten tegen sociale aanvallen.
- Binnen het onderzoek is niet getest of kenmerken van een bedrijf (bijv. grootte, industrie waarin het bedrijf actief is) verschillen in het model opleveren. Verschillen tussen bedrijven zouden kunnen worden geïdentificeerd op basis van bedrijfskenmerken. De onderzoekers erkennen de potentiële impact van deze factoren en raden daarom aan om ze op te nemen in toekomstige werkzaamheden.

*Relevantie voor het eigen onderzoek*

Dit onderzoek toont aan dat IBB, zij het indirect en zwak, van invloed is op de intentie tot naleving van het informatiebeveiligingsbeleid.

### Bauer, S., & Bernroider, E. (2017). From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization

*Doel van het onderzoek*

Het doel van dit onderzoek is te onderzoeken of naleving van het informatiebeveiligingsbeleid wordt beïnvloed door geaccumuleerde beveiligingsinformatie en informatiebeveiligingsbewustzijn.

*Opzet van het onderzoek*

In deze enkele casestudie binnen het hoofdkwartier van een grote Europese bankorganisatie zijn gegevens verzameld d.m.v. een drietrapsproces waarin semigestructureerde interviews zijn gehouden, een enquête is uitgevoerd om de ontwikkelde onderzoekshypothesen te testen en interactieve presentaties gehouden om de resultaten te bespreken. De kwalitatieve interviews versterkten met name de interne validiteit van de constructies met betrekking tot neutralisatietechnieken en het interne kanaalgebruik voor informatieverwerving.

*Resultaten en conclusies van het onderzoek*

De resultaten tonen aan dat de houding t.a.v. de naleving van het informatiebeveiligingsbeleid, en niet alleen de sociale normen, maar ook de persoonlijke normen met betrekking tot neutralisatietechnieken, allemaal belangrijke variabelen zijn die de kenniskloof die in gerelateerd informatiebeveiligingsonderzoek wordt gerapporteerd, kunnen verkleinen. Naast de nadruk op het belang van uitgebreide normen, die in informatiebeveiligingsbewustzijnsprogramma's moeten worden verantwoord, benadrukken we ook het gebruik van interne en externe kanalen om informatie te verwerven als initiële drijfveren voor bewustwording.

*Suggesties voor verder onderzoek*

Genoemde suggesties voor toekomstig onderzoek zijn:

- De resultaten zijn gevonden in een onderzoek bij het hoofdkantoor van een internationale bank. Het onderzoek zou moeten worden herhaald om het draagvlak voor de bevindingen te versterken.

*Relevantie voor het eigen onderzoek*

Dit onderzoek toont aan dat IBB van invloed is op de intentie tot naleving van het informatiebeveiligingsbeleid. Ook laat dit onderzoek zien dat de intentie tot naleving een goede indicator is voor de daadwerkelijke naleving van het beleid.

### Park, Y. S., Park, E. H., & Kim, J. (2017). The role of information security learning and individual factors in disclosing patients' health information

*Doel van het onderzoek*

Het doel van dit onderzoek is om een concept van gezondheidsinformatiebeveiligingsbewustzijn (hierna: GIBB) en haar componenten op te stellen om vervolgens relaties te identificeren tussen dit bewustzijn en persoonlijke waarden en vast te stellen wat de rol is van de persoonlijke waarden bij de intentie om gezondheidsinformatie te onthullen.

*Opzet van het onderzoek*

Een enquête is gebruikt om gegevens te verzamelen. Het steekproefkader was een steekproef van 123 ondermaatse studenten die zich hadden ingeschreven voor de opleiding tot verpleegkundige aan een grote stedelijke universiteit in Zuid-Korea. De deelnemers zijn representatief voor de algemene populatie van studenten verpleegkunde. Een papieren enquête werd tijdens de les aan de leerlingen uitgedeeld.

*Resultaten en conclusies van het onderzoek*

In dit onderzoek wordt het opgezette model empirisch getest en er blijkt dat drie leercomponenten, te weten algemeen informatiebeveiligingsbewustzijn, bewustzijn aangaande regelgeving inzake de beveiliging van gezondheidsinformatie en bestraffingsbewustzijn van groot belang zijn voor de ontwikkeling van GIBB. We vinden dat GIBB een aanzienlijke invloed heeft op persoonlijke normen en zelfcontrole, die een afschrikkende werking hebben op de intentie om gezondheidsinformatie van patiënten bekend te maken.

*Suggesties voor verder onderzoek*

Genoemde suggesties voor toekomstig onderzoek zijn:

- Andere organisatorische en politieke factoren kunnen van invloed zijn op de intentie van personen om zich aan het beveiligingsbeleid te houden. Deze factoren moeten in toekomstige studies worden onderzocht.
- Het kan ook interessant zijn om de rol van cultuureigenschappen in de verschillende landen te onderzoeken, omdat cultuur van invloed kan zijn op het vrijgeven van patiënten informatie door studenten verpleegkunde.

*Relevantie voor het eigen onderzoek*

Dit onderzoek toont aan dat IBB van invloed is op de intentie tot naleving van het informatiebeveiligingsbeleid. Ook geeft dit onderzoek aan dat het de verpleegkundige student is die patiënt informatie zal onthullen, wat functiedifferentiatie in mijn onderzoek kan rechtvaardigen.

### Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations

*Doel van het onderzoek*

Het doel van dit onderzoek is om te achterhalen wat de impact van de demografische kenmerken van de werknemers is op het bewustzijn en de naleving van het informatiebeveiligingsbeleid.

*Opzet van het onderzoek*

Het onderzoek is uitgevoerd in Maleisië onder Maleisische medewerkers die betrokken zijn bij werktaken die toegang hebben tot de persoonlijke gegevens van hun organisaties en deze gebruiken en/of verwerken via bedrijfsactiviteiten en/of transacties. De gegevens zijn tussen januari en maart 2017 verzameld met behulp van een vragenlijst die via Google Formulier is opgesteld. Er is gebruik gemaakt van een sneeuwballensteekproeftechniek. Het aantal respondenten is 607.

Op basis van de in de literatuur geïdentificeerde factoren werden de volgende demografische gegevens verzameld: geslacht, leeftijd, etniciteit, opleidingsniveau, jaren werkervaring en industrie. Voor het meten van het IBB is gebruik gemaakt van de vragen uit eerder onderzoek.

*Resultaten en conclusies van het onderzoek*

Resultaten laten zien dat leeftijd, bedrijfstak en opleidingsniveau belangrijke gevolgen hebben voor het IBB en de naleving van het informatiebeveiligingsbeleid.

*Suggesties voor verder onderzoek*

Genoemde suggesties voor toekomstig onderzoek zijn:

- De resultaten benadrukken dat bij toekomstig onderzoek de noodzaak aanwezig is om rekening te houden met demografische kenmerken en andere overwegingen, zoals het nemen van risico's, risico afwijkend gedrag en zelfregulerend gedrag.
- Toekomstig onderzoek zou meer variabelen kunnen omvatten zoals het inkomensniveau en de jarenlange ervaring in de omgang met consumentengegevens. Met een beter begrip zouden betere programma's en campagnes kunnen worden geformuleerd om werknemers op te leiden.
- Toekomstig onderzoek kan zich richten op het ontwerpen en testen van educatieve programma's om specifieke groepen werknemers te trainen in informatiebeveiliging en het bewustzijn en de naleving van het privacybeleid.
- Toekomstig onderzoek moet ook het effect van de branche onderzoeken door het gedrag van werknemers in de gegevens intensieve industrie, zoals de gezondheidszorg en de telecommunicatiesector, te vergelijken met data-intensieve industrie, zoals de productiesector.

*Relevantie voor het eigen onderzoek*

Dit onderzoek laat zien dat er meerdere factoren van invloed zijn op het IBB, wat het logisch maakt om verschillende van deze factoren mee te nemen in mijn eigen onderzoek.

### Park, E. H., Kim, J., Wiles, L. L., & Park, Y. S. (2018). Factors affecting intention to disclose patients' health information

*Doel van het onderzoek*

Het doel van dit onderzoek is om factoren te identificeren die van invloed zijn op de intentie, van studenten verpleegkunde, om patiënt informatie te onthullen.

*Opzet van het onderzoek*

Een online enquête is gebruikt om gegevens te verzamelen, waarbij de vragen uit eerder onderzoek zijn gebruikt. Het steekproefkader was een steekproef van 105 studenten die waren ingeschreven voor cursussen verpleegkunde aan een grote universiteit in de VS.

*Resultaten en conclusies van het onderzoek*

De resultaten van het onderzoek laten zien dat GIBB direct van invloed is op de intenties om patiënt informatie te onthullen, terwijl de medische beoordeling bemiddelt in de relatie tussen GIBB en de intenties om te onthullen. Ook vinden we dat GIBB invloed heeft op de zelfredzaamheid, die op haar beurt weer van invloed is op de intenties te onthullen via medische beoordeling.

*Suggesties voor verder onderzoek*

Genoemde suggesties voor toekomstig onderzoek zijn:

- Toekomstige onderzoeken kunnen verder onderzoek doen naar personele, organisatorische en maatschappelijke factoren en hun invloed op afwijkend gedrag in de context van de beveiliging van de gezondheidszorg.

*Relevantie voor het eigen onderzoek*

Dit onderzoek toont aan dat GIBB van invloed is op de intentie tot naleving van het informatiebeveiligingsbeleid. Ook geeft dit onderzoek aan dat het de verpleegkundige student is die patiënt informatie zal onthullen, wat functiedifferentiatie in mijn onderzoek kan rechtvaardigen.

# Bijlage B Samenvattingen geschikte publicaties beantwoording deelvraag 2

## Siponen, M. (2001). Five dimensions of information security awareness.

### *Doel van het onderzoek*

Het schetsen van de verschillende dimensies van het IBB en het onderzoeken van bepaalde belangrijke kwesties rond deze dimensies. Daarnaast worden categorieën (of doelgroepen) in elke dimensie onderscheiden.

### *Opzet van het onderzoek*

Conceptuele analyse is gebruikt als onderzoeksaanpak. Om de dimensies en categorieën die in deze publicatie worden voorgesteld in het licht van deze conceptuele analyse te rechtvaardigen, zijn een aantal praktische voorbeelden gegeven. Het doel is om aan de hand van de voorbeelden een rechtvaardiging te geven voor elke dimensie. Andere, even belangrijke kwesties, zoals de inhoud van veiligheidskwesties in elke dimensie (bv. een lijst van specifieke acties die men al dan niet moet ondernemen), vallen buiten het bestek van dit onderzoek.

### *Resultaten en conclusies van het onderzoek*

Het voortdurend toenemende gebruik van IT en informatisering benadrukt het belang van informatiebeveiliging en in het bijzonder het individuele bewustzijn hiervan. Om in deze behoefte te voorzien, kan het bewustzijn worden verdeeld in vijf dimensies, namelijk: organisatorische, algemeen publieke, socio-politieke, computer ethische en institutionele educatie. De algemeen publieke dimensie is nodig om gewone computergebruikers te informeren over de risico's die verbonden zijn aan het gebruik van bijvoorbeeld het internet. Wat de laatste dimensie betreft, moeten onderwijsinstellingen het onderwijs in computerethiek parallel met het technisch onderwijs ontwikkelen, naast het bespreken van onderwerpen die verband houden met het bewustzijn van informatiebeveiliging. Binnen elke dimensie hebben de verschillende doelgroepen verschillende soorten informatie nodig. Relevante kwesties en doelstellingen moeten worden overwogen, deels om veiligheidsredenen en ethische redenen, en deels om de middelen te maximaliseren. Organisaties zoals beroepsorganisaties en onderwijsinstellingen moeten de teugels in handen nemen om een dergelijk proces in goede banen te leiden.

### *Suggesties voor verder onderzoek*

Genoemde suggesties voor toekomstig onderzoek zijn:

- Het onderzoeken wat eigen specifieke doelstellingen voor doelgroepen kunnen zijn, gebaseerd op een zorgvuldige afweging van de meest relevante zaken die van belang zijn voor de doelgroep.

### *Relevantie voor het eigen onderzoek*

- De dimensie organisatie laat zien dat het van nut kan zijn om bij onderzoek naar IBB onderscheid te maken in verschillende groepen medewerkers binnen de organisatie. Voor mijn onderzoek betekent dit voornamelijk onderscheid tussen de verschillende functies die gebruik kunnen maken van de ‘breaking-the-glass’ optie. Ook is het wellicht verstandig om de groep te onderscheiden die alle patiënt data mogen zien op basis van het hebben van een behandelovereenkomst zonder daarvoor gebruik te hoeven maken van een ‘breaking-the-glass’ optie, zoals zorgadministratiemedewerkers, privacy officer, functionaris gegevensbescherming en mogelijke anderen.

## Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness.

### *Doel van het onderzoek*

Het doel van dit onderzoek is om verslag uit te brengen over de ontwikkeling van een prototype model voor het meten van het bewustzijn inzake informatiebeveiliging in een internationaal mijnbouwbedrijf.

### *Opzet van het onderzoek*

De methodologie die is gebruikt om het meetinstrument te ontwikkelen is gebaseerd op technieken ontleend aan het domein van de sociale psychologie, die stelt dat de geleerde predisposities om op een gunstige of ongunstige manier te reageren op een bepaald object drie componenten hebben, te weten affect, gedrag en cognitie. Deze drie componenten zijn als basis gebruikt en het model is ontwikkeld op drie gelijkwaardige dimensies, namelijk wat iemand weet (kennis); hoe hij/zij zich voelt over het onderwerp (houding); en wat hij/zij doet (gedrag). Om een meetinstrument te ontwikkelen en de daadwerkelijke metingen uit te voeren, is de onderzoeker geconfronteerd met twee verschillende uitdagingen: wat te meten en hoe te meten.

Als belangrijkste vereiste wat te meten is het globaal IBB voor de organisatie benoemd. Om dit te realiseren is via een top down benadering een waardeboom gecreëerd waarin elk van de drie dimensies is opgesplitst naar zes aandachtsgebieden en waar nodig zijn deze zes gebieden nog opgesplitst naar subcategorieën. Duidelijk werd dat niet elke factor in gelijke mate zou bijdragen aan de uiteindelijke meting van het bewustzijnsniveau. Een andere kwestie die moest worden gemeten, was dan ook het belang van de factoren die een bijdrage leveren aan de uiteindelijke bewustzijnsniveaumeting. Hiertoe zijn belangengewichten aan de factoren gehangen per regio.

De wijze van meten is via vragenlijsten met in sommige gevallen 3 antwoordmogelijkheden (juist, onjuist, weet niet) en in andere gevallen 2 antwoordmogelijkheden (juist, onjuist).

Het prototype van het model is getest bij het regionale kantoor in Australië.

### *Resultaten en conclusies van het onderzoek*

Het model maakt gebruik van een eenvoudig gegevensverzamelingsproces en wegingssysteem en biedt, in combinatie met bepaalde multicriteria probleemoplossingstechnieken, een kwantitatieve meting van het IBB. Het is gebaseerd op de gezonde principes van duurzaamheid, verfijning en wetenschappelijke validiteit en kan gebruikt worden als basis voor een meer omvattend en verfijnd meetsysteem.

### *Suggesties voor verder onderzoek c.q. verbetering van het prototype*

Genoemde suggesties voor toekomstig onderzoek zijn:

- Ontwikkeling van een uitgebreide en volledige vragenbank. Aanbevolen wordt om enige kwaliteitstijd te besteden aan een diepgaander onderzoek naar dit aspect van het model. Het model kan alleen succesvol zijn als de ''juiste'' vragen worden gesteld om de juiste gegevens als input voor het model te verkrijgen;
- Maak gebruik van een 5- of 7-punts Likert-schaal om vragen te evalueren;
- Het proces van het verzamelen van informatie en het proces van het toekennen van gewichten moet worden ontwikkeld tot een, bij voorkeur, webgebaseerd instrument dat vanuit een centraal punt wordt gecontroleerd en vervolgens ter beschikking wordt gesteld van de regio's. Het is van essentieel belang dat het verzamelen van informatie en het toewijzen van gewichten wordt gecontroleerd. Toepassing van het instrument in andere regio’s is van belang, zodat meer gegevens het inzicht in het model en het kader zullen vergroten en kunnen leiden tot verdere verbeteringen;
- Praktische gegevens uit een systeem kunnen (moeten) worden gebruikt als extra input voor het model om gedragsfactoren te testen. Dergelijke gegevens zouden betrouwbaarder (niet subjectief of menselijk afhankelijk) zijn en gemakkelijk te verkrijgen zonder gebruik te maken van de werktijd van het personeel om (langere) vragenlijsten in te vullen.

*Relevantie voor het eigen onderzoek*

- De publicatie beschrijft een uitgebreide methode waarmee een prototype model voor het meten van het IBB is opgezet. De gebruikte vragenlijst voor het vergaren van informatie, welke geen onderdeel is van de publicatie, is opgezet voor en met deze specifieke organisatie. Het model is daarmee niet direct bruikbaar voor een andere organisatie.
- Het model en de resultaten hebben voldaan aan de vooraf gestelde verwachtingen, wat kan betekenen dat de gebruikte methodiek voor het vaststellen van het model en daarmee het model als waardevol kunnen worden beschouwd. Het model is echter een prototype en daarmee niet uitgebreid gevalideerd voor het meten van IBB binnen elke andere organisatie.

### Kruger, H. A., Drevin, L., & Steyn, T. (2006). *A Framework for Evaluating ICT Security Awareness.*

#### *Doel van het onderzoek*

Het doel van deze publicatie is het beschrijven van een framework, opgebouwd op basis van het prototypemodel van Kruger and Kearney (2006), waarmee IBB kan worden gemeten.

#### *Opzet van het onderzoek*

Als basis voor het op te zetten framework wordt het prototype van Kruger and Kearney (2006) gebruikt. Verschillende aspecten, technieken en benaderingen binnen dit framework zijn vergelijkbaar met de gebruikte binnen die studie.

De eerste stap in het framework is om in samenspraak met de stakeholders en gebruikmakend van de 'Value Focused Approach' (hierna: VFA) van Keeney (1994) aandachtsgebieden te identificeren in het domein van IBB. De VFA bestaat uit een viertal stappen om te komen tot een netwerk dat de onderlinge verbanden tussen alle doelstellingen laat zien. Het netwerk kan dan worden gebruikt om oorzaak-gevolgrelaties af te leiden en om beslissingskansen te genereren.

Een volgende stap in het framework is de uitvoering van metingen bij medewerkers op kennis, houding en gedrag op basis van de vastgestelde aandachtsgebieden, middels een enquête.

Parallel aan deze stap wordt systeemdata geanalyseerd om het daadwerkelijk beveiligingsgedrag van de medewerkers te bepalen. Dit is een extra toevoeging ten opzichte van het prototype van Kruger and Kearney (2006), wat het model betrouwbaarder maakt. Bij het bepalen welke systeemdata te vergaren en analyseren, wordt aangegeven dat hierbij 3 zaken van belang zijn, te weten: 1. Het moet technisch haalbaar zijn de data te vergaren en analyseren, 2. de data moet relevantie hebben aangaande de vastgestelde aandachtsgebieden en 3. het vergaren van de data moet passen binnen de ethische kaders waar de organisatie mee te maken heeft.

Een volgende stap in het framework is het samenstellen van een model op basis van de enquête- en systeemdata en wegingsfactoren, zodat het niveau van IBB kan worden gemeten. Het model en de uitgevoerde berekeningen zijn gebaseerd op aspecten en technieken zoals weergegeven in de publicatie van Kruger and Kearney (2006).

Nadat het framework is opgezet is dit toegepast in een universitaire omgeving conform de voorgestelde aanpak in het framework.

#### *Resultaten en conclusies van het onderzoek*

Om ervoor te zorgen dat programma's voor beveiligingsbewustzijn waarde toevoegen aan een organisatie en tegelijkertijd een bijdrage leveren aan het gebied van informatiebeveiliging is het noodzakelijk om een gestructureerde aanpak te volgen om het effect ervan te bestuderen en te meten. In deze publicatie is een framework besproken om, volgens een gestructureerde aanpak, IBB te kunnen meten. Het framework biedt bij de toepassing ruimte om discussie te voeren over de identificatie van de aandachtsgebieden. Tijdens het onderzoek zijn korte notities over het gebruik van systeem gegenereerde gegevens die kunnen helpen bij het bepalen van het beveiligingsgedrag, gepresenteerd.

De vooruitgang en de bevindingen van het onderzoek zijn bemoedigend. Het is de bedoeling om verder te gaan met een vervolgstudie van de resterende fasen van het voorgestelde framework.

#### *Suggesties voor verder onderzoek*

Genoemde suggesties voor toekomstig onderzoek zijn:

- Het voortzetten van een, op moment van publicatie lopende, diepgaande studie naar de beschikbaarheid, toepasbaarheid en het gebruik van systeem gegenereerde gegevens om het model te versterken;
- Het genereren van maatregelen die de factoren van de geïdentificeerde aandachtsgebieden vertegenwoordigen;
- Het ontwikkelen van een definitief model, gebruikmakend van de juiste management science technieken om metingen en aanbevelingen te genereren die betrouwbaar en valide zijn.

*Relevantie voor het eigen onderzoek*

- De publicatie beschrijft een gestructureerde aanpak om te komen tot een, voor een specifieke organisatie opgezet, model voor het meten van IBB. Doordat de aanpak voortborduurt op een eerder gepubliceerde methode en beide in verschillende organisaties naar tevredenheid zijn toegepast, is er een basis voor validatie gelegd.
- De voorgestelde aanpak maakt, voor het vaststellen van het IBB, gebruik van daadwerkelijke data aangaande het gedrag van medewerkers. Binnen mijn eigen onderzoek wil ik ook gebruik maken van daadwerkelijke data om vast te stellen of medewerkers het afgesproken beleid naleven. Binnen mijn onderzoek wil ik mij weliswaar richten op een zeer specifiek onderdeel van naleving van informatiebeveiligingsbeleid, maar deze aanpak is daar juist zeer geschikt voor omdat het een op de organisatie toegespitst model oplevert. De vraag is alleen of vaststelling van een model binnen één organisatie ook bruikbaar is binnen vergelijkbare organisaties in de branche. Hier doet het onderzoek geen uitspraken over.

### Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study.

*Doel van het onderzoek*

Het doel van het onderzoek is om de IBBsniveaus van instellingen voor hoger onderwijs in de Verenigde Arabische Emiraten te onderzoeken.

Het onderzoek richt zich daartoe op de volgende twee belangrijke onderzoeksvragen:

1. Wat zijn de huidige uitdagingen en bedreigingen ten aanzien van informatiebeveiliging voor universiteiten in de context van een ontwikkelingsland?
2. Wat zijn de niveaus van IBB van beleidsmakers en medewerkers in het hoger onderwijs in relatie tot deze uitdagingen en bedreigingen?

*Opzet van het onderzoek*

Voor de uitvoering van het onderzoek is een interpretatieve casestudy-benadering gehanteerd. Binnen het onderzoek is gebruik gemaakt van een combinatie van kwantitatieve (enquêtes) en kwalitatieve (interviews, documentatie en observatie) technieken.

De enquête is vooraf getest en uitgezet bij een steekproefpopulatie van 45 medewerkers, waarvan er 43 een ingevulde vragenlijst hebben geretourneerd. Deze enquêtes zijn gecodeerd en geanalyseerd. Interviews zijn gehouden met 7 informatiebeveiligingsfunctionarissen. Gedurende het gehele onderzoek zijn observaties gedaan, vooral om te ontdekken wat mensen doen in plaats van wat ze zeggen dat ze doen. Daarnaast zijn een aantal documenten, zoals systeemlogboeken, rapporten, systeemhandleidingen, trainingshandleidingen, informatiebeveiligingsbeleid verzameld en geanalyseerd ter ondersteuning van de onderzoeksresultaten.

*Resultaten en conclusies van het onderzoek*

De belangrijkste uitdaging waar de universiteit voor staat, wordt weerspiegeld in de tegenstrijdige eisen van een onderwijsmodel dat ontleend is aan het westen en de conservatieve omgeving, geworteld in diepe culturele en religieuze overtuigingen, rond de universiteit. Dreigingen zijn over het algemeen vergelijkbaar met die in ontwikkelde landen, waar de universiteit de oorzaak van de dreigingen als extern ervaart. Maatregelen tegen de optredende risico's worden niet goed toegepast of komen niet tot uiting in de activiteiten en praktijken van de universiteit, die eerder een reactieve dan een proactieve aanpak neigt te hanteren.

Het niveau van het IBB is laag. Hiervoor worden meerdere redenen aangedragen, waaronder het leggen van nadruk op externe en technische bedreigingen, het ontbreken van doelstellingen, beleid en procedures en het gebrek aan training, handleidingen en auditprocedures. Binnen de universiteit is geen visie op informatiebeveiliging en ook geen eenduidig aanspreekpunt. Een andere reden voor het gebrek aan IBB is de aard van de arbeidscontracten, het overgrote deel van de werknemers (meer dan 80%) wordt ingehuurd op uitzendbasis. Voor veel Informatiebeveiligingsmanagers- en medewerkers is dit niet bevorderlijk voor langdurige en voortdurende activiteiten zoals informatiebeveiligingsplanning en -opleiding.

*Suggesties voor verder onderzoek*

Er worden aanbevelingen gedaan om het IBB te vergroten, maar ook om te komen tot een wederzijds begrip van de informatiebeveiliging binnen de context van deze specifieke universiteit.

*Relevantie voor het eigen onderzoek*

- Het onderzoek kijkt naar de uitdagingen en dreigingen voor een organisatie in een specifieke branche. Binnen mijn onderzoek wil ik ook kijken naar een bedreiging die, in de gekozen vorm, specifiek voor de (ziekenhuis)zorg geldt.
- De gebruikte onderzoeksopzet om de mate van IBB te bepalen is zeer uitgebreid en divers, wat de betrouwbaarheid ten goede komt. In mijn onderzoek wil ik op zoek gaan naar de oorzaken van het gebruik van een bepaalde procedure, waarbij een dergelijk uitgebreid onderzoek hier naar alle

waarschijnlijkheid een duidelijk antwoord op zal geven, inclusief de mate van onterecht gebruik en het mogelijk onvoldoende zijn van het bewustzijn als oorzaak.

- De mate van IBB wordt niet uitgedrukt in een cijfer en zodoende maakt deze methode het niet mogelijk om groepen objectief met elkaar te vergelijken. Hoe IBB wordt gedefinieerd is van belang hoe en wat te meten.

### Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2013, 2013). *The development of the human aspects of information security questionnaire (HAIS-Q).*

*Doel van het onderzoek*

Het doel van dit onderzoek was om de ontwikkeling en initiële betrouwbaarheids- en validiteitstoetsing van de HAIS- Q te schetsen en om vast te stellen of er een positief verband bestaat tussen de kennis van de respondenten over beleid en procedures, de houding ten opzichte van beleid en procedures en hun zelf gerapporteerde gedrag bij het gebruik van een werkcomputer.

*Opzet van het onderzoek*

De Human Aspects of Information Security Questionnaire (HAIS-Q) wordt ontwikkeld met behulp van een hybride inductieve, verkennende aanpak. met als doel het evalueren van informatiebeveiligingsrisico's veroorzaakt door medewerkers binnen organisaties. De resultaten van 500 Australische medewerkers zijn vervolgens gebruikt om de betrouwbaarheid van het HAIS-Q te onderzoeken, evenals de relaties tussen kennis van beleid en procedures, houding ten opzichte van beleid en procedures en gedrag bij het gebruik van een werkcomputer.

*Resultaten en conclusies van het onderzoek*

De resultaten wijzen op significante, positieve relaties tussen alle variabelen. Zowel kwalitatieve als kwantitatieve resultaten geven echter aan dat de directe invloed van kennis van beleid en procedures veel minder bepalend is voor de variantie in zelf gerapporteerd gedrag dan de houding ten opzichte van beleid en procedures.

*Suggesties voor verder onderzoek*

Genoemde suggesties voor toekomstig onderzoek zijn:

- In toekomstig onderzoek kunnen individuele, organisatorische en interveniërende factoren worden onderzocht en kan worden nagegaan of deze factoren een statistisch significant effect hebben op het gedrag van de werknemers en dus op de beveiliging van de informatiesystemen van een organisatie.
- In toekomstige studies kan ook het HAIS-Q verder worden ontwikkeld. Zo kunnen bijvoorbeeld alternatieve maatstaven voor kennis, houding en gedrag worden verkregen om de construct-validiteit van het HAIS-Q te beoordelen.
- De vragenlijst kan in toekomstig onderzoek ook worden toegepast op werknemers binnen bekende organisaties, waardoor het feitelijke beleid en de procedures en methoden van training binnen de organisatie kan worden beoordeeld en hoe deze van invloed zijn op de antwoorden die door de werknemers worden gegeven.

*Relevantie voor het eigen onderzoek*

- Binnen dit onderzoek wordt een methode beschreven voor de ontwikkeling van een methode welke ook gebruikt kan worden voor de uitbreiding van dezelfde methode.
- De suggesties voor vervolgonderzoek geven een indicatie van factoren die onderzocht kunnen worden, waarvan ik binnen mijn onderzoek verschillende individuele factoren wil toetsen.
- Het onderzoek geeft aan hoe de validiteit van het instrument verder getoetst kan worden. Een van de methoden is het gebruik van daadwerkelijk gedrag in plaats van zelf gerapporteerd gedrag. Binnen mijn onderzoek wil ik kijken of ik dit kan toepassen.

### Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). A study of information security awareness in Australian government organisations.

*Doel van het onderzoek*

Het doel van dit onderzoeksproject was tweeledig. Het eerste doel was het ontwikkelen en testen van een vragenlijst om te bepalen in hoeverre medewerkers zich bewust zijn van risico's, van tekortkomingen in informatiebeveiliging. Het tweede doel was om een holistisch inzicht te krijgen in de mate van IBB, gedefinieerd door de dimensies kennis, houding en gedrag van medewerkers van 3 Australische overheidsorganisaties.

*Opzet van het onderzoek*

Met behulp van een enquêtetool zijn houdingen, kennis en gedrag getest op 8 aandachtsgebieden. Deze aandachtsgebieden zijn belang, principes en regels van informatiebeveiligingsbeleid, wachtwoordmanagement, email- en internetgebruik, het rapporteren van beveiligingsincidenten, gevolgen van gedrag en training. De enquête werd ingevuld door 203 deelnemers uit de 3 organisaties. Dit is aangevuld met interviews met het senior management van deze organisaties.

*Resultaten en conclusies van het onderzoek*

De resultaten van dit onderzoek laten zien dat het IBB van de medewerkers binnen alle 3 de organisaties over het algemeen voldoende was. De antwoorden op kennisvragen kregen over het algemeen een hogere score dan de antwoorden op vragen over houding en gedrag. Opvallende bevindingen waren:

- Veel medewerkers hadden geen of onvoldoende kennis van een aantal aspecten van draadloze technologie.
- Binnen organisatie B zou wellicht de opleiding aangaande informatiebeveiliging moeten verbeteren en alle organisaties moeten hun werknemers voorlichten over het gebruik van sociale netwerksites.
- De meeste werknemers verklaarden dat ze hun wachtwoorden nooit met anderen zouden delen en dat ze nooit niet-zakelijke software of muziek- of video-inhoud van het internet zouden downloaden op hun werkcomputers. Meer moeite hebben de medewerkers met het clean-desk beleid en het melden van beveiligingsincidenten. Ook het gebruik van een USB-stick om bestanden tussen werk en privé over te brengen gebeurt.
- Uit interviews met het senior management bleek dat de managers een goed inzicht hadden in het IBB van hun medewerkers en dat ze goed begrepen wat goed informatiebeveiligingsmanagement in het algemeen was. Zij erkenden echter ook enkele punten van zorg, zoals de behoefte aan meer opleiding in het juiste gebruik van sociale netwerksites tijdens het werk.

*Suggesties voor verder onderzoek*

Genoemde suggesties voor toekomstig onderzoek zijn:

- Onderzoek om de betrouwbaarheid vast te stellen door de vragenlijst door een groter aantal deelnemers te laten invullen, zodat de relatie tussen de constructen en specifieke items kan worden onderzocht om er zeker van te zijn dat ze het beoogde gebied nauwkeurig meten. De relatie tussen factoren kan ook verder in detail worden onderzocht om een model van de menselijke aspecten van informatiebeveiliging te ontwikkelen.
- Onderzoek de effectiviteit van verschillende trainings- en risicocommunicatiemogelijkheden door gebruik te maken van de vragenlijst die in dit onderzoek is ontwikkeld in een pre-test/post-test methodologie. De auteurs zijn bijvoorbeeld van plan de in deze publicatie gepresenteerde vragenlijst te verfijnen, zodat deze kan worden gebruikt als basis voor het benchmarken van de stand van zaken van informatiebeveiliging in verschillende sectoren.

*Relevantie voor het eigen onderzoek*

- De gedragsvormen die de motivatie voor dit onderzoek vormen, zijn gedragingen die geen technische expertise vereisen en niet worden geassocieerd met de intentie om de organisatie of haar middelen te schaden. Deze gedragingen zijn verantwoordelijk voor veel menselijke fouten en omdat uit de literatuur blijkt dat menselijke fouten de meest voorkomende oorzaak zijn van informatiebeveiligingsschendingen, staan deze gedragingen centraal in de vragenlijst. Het gedrag wat

ik in mijn onderzoek wil bekijken kan ook in deze categorie vallen en zodoende is de gebruikte methodiek interessant. Een extra reden waarom de methodiek interessant is, is het feit dat de resultaten uit de vragenlijst ondersteund worden door de resultaten uit de interviews en vice versa.

- De opzet van de methodiek voor het meten van IBB is vergelijkbaar met die uit eerder bekeken publicaties, zij het dat binnen die publicaties in samenspraak met het management de aandachtsgebieden zijn bepaald en zijn voorzien van wegingsfactoren. Of en zo ja hoe dat binnen dit onderzoek is gebeurd, wordt niet duidelijk. In andere publicaties wordt ook gebruik gemaakt van systeemdata om de betrouwbaarheid te verhogen. Binnen deze publicatie gebeurt dit middels interviews, dit zou een extra toevoeging kunnen zijn voor de creatie van een model om bewustzijn te meten. Wellicht kan ik deze onderzoeksmethodieken binnen mijn onderzoek combineren om de betrouwbaarheid van de resultaten van mijn onderzoek te waarborgen.
- IBB wordt bekeken in termen van kennis, houding en gedrag en impliciet de interactie tussen deze gebieden. Niet uitgesproken verwachtingen zijn dat als de kennis hoog is, dit effect heeft op de houding. Dit lijkt niet direct uit het onderzoek naar voren te komen. Houding en gedrag lijken daarentegen wel een relatie te hebben. Deze relaties kan ik in mijn onderzoek expliciet benoemen in de vorm van hypotheses.

### Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q).

*Doel van het onderzoek*

Het doel van dit onderzoek is tweeledig. Het eerste doel is het ontwikkelen van een empirisch gevalideerd instrument, de Human Aspects of Information Security Questionnaire (hierna: HAIS-Q), om te kunnen beoordelen in hoeverre de informatiesystemen van een organisatie kwetsbaar zijn voor bedreigingen als gevolg van het risicogedrag van medewerkers. Het tweede doel is het onderzoeken van de relatie tussen kennis van beleid en procedures, houding ten opzichte van beleid en procedures en gedrag bij het gebruik van een werkcomputer.

*Opzet van het onderzoek*

Als basis voor de te ontwikkelen HAIS-Q dient het onderzoek van Parsons, McCormac, Pattinson, et al. (2013). Het binnen dat onderzoek gehanteerde iteratieve proces heeft uiteindelijk de hypothese opgeleverd dat naarmate de kennis van de computergebruikers over het beleid en de procedures op het gebied van informatiebeveiliging toeneemt, hun houding ten opzichte van het beleid en de procedures inzake informatiebeveiliging verbetert, wat zich zou moeten vertalen in meer risicomijdend informatiebeveiligingsgedrag. Dit veranderingsproces wordt ook wel het KAB-model genoemd (Kruger & Kearney, 2006) en een verfijnde en specifieke versie van dit model is één onderdeel van de ontwikkelde HAIS-Q. De bestaande kritiek op het KAB-model wordt besproken en de onderzoekers concluderen dat het model kan worden gebruikt zolang de factoren correct worden gedefinieerd.

Conform de methode genoemd in het onderzoek van Parsons, McCormac, Pattinson, et al. (2013) worden een zevental aandachtsgebieden onderkend, elke met 3 sub-gebieden. Per sub-gebied wordt één stelling geformuleerd specifiek voor de dimensie kennis, één voor houding en één voor gedrag, leidend tot 63 stellingen. De respondent kan elke stelling scoren op een 5-punt Likert-schaal.

De bovenstaande relatie tussen kennis, houding en gedrag wordt volgens de onderzoekers ook beïnvloed door vele factoren op het gebied van de individuele persoon, de organisatie en interventie. De HAIS-Q bevat daarom specifieke meetpunten voor verschillende factoren (zo worden organisatorische factoren gemeten via de organisatie- en veiligheidscultuur, subjectieve normen, beloningen en straffen). De beoordeling van de invloed van deze factoren op de KAB en de verschillende aandachtsgebieden maken echter deel uit van een groter project, dat buiten het bestek van deze publicatie valt.

In lijn met de gekozen inductieve, verkennende aanpak wordt de onderzoeksmethodologie van deze publicatie in drie fasen gepresenteerd. De eerste is de validiteitsfase, die bedoeld is om de validiteit en betrouwbaarheid van de HAIS-Q vast te stellen. De tweede fase is een pilotstudie, die is uitgevoerd om de betrouwbaarheid van de HAIS-Q verder te verfijnen en te onderzoeken. Deze beide fasen leverden het eerste bewijs van de validiteit en betrouwbaarheid van het HAIS-Q en rechtvaardigden de uitvoering van de derde fase, de hoofdstudie.

De deelnemers zijn gevraagd eerst de informatiefolder door te lezen en toestemming te geven voor het gebruik van de verzamelde gegevens om daarna de HAIS-Q in te vullen.

*Resultaten en conclusies van het onderzoek*

De in dit onderzoek gepresenteerde gegevens ondersteunen het ontwikkelde model en de daarbij behorende vragenlijst. Ook ondersteunen de gegevens de hypothese dat er een positieve relatie bestaat tussen de kennis van de respondenten over beleid en procedures, hun houding ten opzichte van beleid en procedures en hun zelf gerapporteerde gedrag bij het gebruik van een werkcomputer.

De resultaten geven aan dat de kennis van de deelnemers over beleid en procedures en hun houding ten opzichte van beleid en procedures een belangrijke verklaring is voor de verschillen in het zelf gerapporteerde gedrag van de deelnemers. Een interessante conclusie van dit onderzoek is dat de kennis van het beleid en de procedures van een medewerker veel meer invloed heeft gehad op de houding ten

opzichte van het beleid en de procedures dan op het zelf gerapporteerde gedrag. Dit suggereert dat het effect van kennis op gedrag wordt gemedieerd door de houding ten opzichte van beleid en procedure.

Een andere belangrijke conclusie is dat generieke trainingen, alleen gericht op kennis, minder effectief zullen zijn dan trainingen binnen de context, gericht op het verbeteren van zowel de kennis van als het inzicht in beleid en procedures.

*Suggesties voor verder onderzoek*

Genoemde suggesties voor toekomstig onderzoek zijn:

- Onderzoek de individuele, organisatorische en interventie factoren en bepaal of deze factoren een statistisch significant effect hebben op het gedrag van de medewerkers en dus op de veiligheid van de informatiesystemen van een organisatie.
- Ontwikkel de HAIS-Q verder in lijn met de validatierichtlijnen van Straub, Boudreau, and Gefen (2004). Zo zullen bijvoorbeeld alternatieve maatstaven van kennis, houding en gedrag ons in staat stellen om de construct-validiteit van de HAIS-Q te beoordelen.
- Implementeer de vragenlijst bij medewerkers binnen bekende organisaties, zodat beoordeeld kan worden wat het werkelijke beleid, procedures en trainingsmethoden binnen de organisatie zijn en hoe deze van invloed zijn op de antwoorden van de medewerkers.

*Relevantie voor het eigen onderzoek*

- De afhankelijke factor binnen dit onderzoek is het gewenste gedrag wat gemeten wordt door vragen te stellen aan de respondent aangaande zijn/haar gedrag. Het onderzoek stelt dat houding invloed heeft op gedrag en kennis invloed heeft op zowel houding als gedrag. Daarnaast wordt ook de invloed van vele andere factoren onderkend en verschillende hiervan worden ook meegenomen in de vragenlijst, alleen wordt niet gekeken naar hun statistische significantie. Dit model biedt een goede basis voor wat ik wil onderzoeken, echter wil ik, op één specifiek aandachtsgebied, gebruik maken van daadwerkelijke data, wat afwijkt van deze methodiek. Ook het specifieke aandachtsgebied is geen onderdeel van de 7 aandachtsgebieden in dit onderzoek. De vraag is of ik op vergelijkbare wijze een aandachtsgebied kan toevoegen dat voor de (ziekenhuis)zorg een zeer relevant aandachtsgebied is.
- De binnen dit onderzoek gehanteerde aandachtsgebieden zullen moeten worden geverifieerd op bruikbaarheid binnen de gezondheidszorg, zodat het onderzoek breder kan worden getrokken dan alleen de kennis, houding en gedrag op het gebied van gebruik van de ‘breaking-the-glass’ optie.

### Velki, T., Solic, K., & Ocevcic, H. (2014). *Development of Users' Information Security Awareness Questionnaire (UISAQ)—Ongoing work.*

#### *Doel van het onderzoek*

Het doel van het onderzoek in deze publicatie is de ontwikkeling van een betrouwbaar universeel instrument waarmee de mate van IBB van de gebruikers van het informatiesysteem kan worden gemeten, zo algemeen mogelijk, namelijk de Information Security Awareness Questionnaire (UISAQ).

#### *Opzet van het onderzoek*

In het kader van dit onderzoek hebben de auteurs de UISAQ gecreëerd, bestaande uit 4 delen met in totaal 37 items verzameld uit verschillende beveiligingsrichtlijnen en resultaten van eerdere studies. Elk item is een stelling in de UISAQ die een factor presenteert, gemeten op een 5-punts schaal. De 4 delen van de UISAQ zijn de volgende:

- 20 items die het potentieel risicovolle gedrag van computergebruikers meten;
- 6 items die het niveau van het IBB van de gebruiker meten;
- 5 items die het niveau van het geloof van de gebruiker over informatiebeveiliging meten;
- 6 vragen die de kwaliteit en veiligheid van wachtwoorden onderzochten.

De vragenlijst is uitgezet bij 135 studenten van 3 verschillende faculteiten van een universiteit in Kroatië.

#### *Resultaten en conclusies van het onderzoek*

De ontwikkeling van de vragenlijst bestond uit het selecteren van geschikte items waarvoor werd verondersteld dat het niveau van potentieel risicovol gedrag van computergebruikers, de mate van IBB, het geloof van gebruikers in veiligheid of de kwaliteit van de wachtwoorden werd gemeten. Met behulp van beschrijvende statistieken, factoranalyse en betrouwbaarheidsanalyse is getest of de geselecteerde items een goede maat zijn voor het veronderstelde construct.

Resultaten voor het eerste deel van de UISAQ laten zien dat er 3 items zijn die niet bijdragen en dat de overige 17 items opgedeeld zouden moeten worden in 3 sub-schalen. Resultaten tonen aan dat alle items van deel 2 bijdragen, zonder dat de toevoeging van sub-schalen noodzakelijk is. Voor deel 3 laten de resultaten zien dat 2 items moeten worden verwijderd omdat deze de interne consistentie schenden. Resultaten laten zien dat de items uit deel 4 van de UISAQ bijdragen.

Uit de resultaten blijkt dat UISAQ een goed en betrouwbaar instrument kan worden voor het meten van het IBB van gebruikers.

#### *Suggesties voor verder onderzoek*

Als toekomstig werk zullen de auteurs het verzamelen van gegevens herhalen door ze te analyseren en op die manier de UISAQ zo vaak als nodig is te verbeteren om zo goed als mogelijk een vragenlijst te ontwikkelen. Het einde van het ontwikkelingsproces zou de internationale validatie van deze vragenlijst moeten zijn.

#### *Relevantie voor het eigen onderzoek*

De informatie in deze publicatie is te summier, vragenlijsten zijn niet aanwezig en de publicatie betreft een eerste validatie van een ontwikkeld model. Zodoende is deze publicatie op dit moment niet relevant voor mijn eigen onderzoek.

### Egelman, S., & Peer, E. (2015). *Scaling the security wall: Developing a security behavior intentions scale (sebis).*

#### *Doel van het onderzoek*

Het ontwikkelen van een nieuwe schaal voor het beoordelen van het computerbeveiligingsgedrag van eindgebruikers: de Security Behavior Intenties Scale (SeBIS).

#### *Opzet van het onderzoek*

Voor de ontwikkeling van de schaal is gebruik gemaakt van de procedure van Netemeyer, Bearden, and Sharma (2003), bestaande uit de volgende 4 stappen:

1. Construct definitie en inhoudsdomein: Duidelijk definiëren van de constructie die de schaal wil meten.
2. Het genereren en beoordelen van meetpunten: Het creëren van een pool van kandidaat-vragen om deze vragen vervolgens te evalueren om niet significante vragen te verwijderen.
3. Het ontwerpen en uitvoeren van studie om de schaal te ontwikkelen en te verfijnen: Explorerende factor analyse uitvoeren om het aantal vragen te verminderen en latente constructies te onderzoeken om zo een model te bouwen.
4. Definitief maken van de schaal: Het uitvoeren van een bevestigende factor analyse om te bevestigen dat de schaal past bij het beoogde model, gevolgd door een betrouwbaarheidsanalyse.

#### *Resultaten en conclusies van het onderzoek*

Stap 1 en 2 hebben geleid tot een vragenlijst van 30 vragen welke middels een studie geëvalueerd zijn. Dit heeft geresulteerd in het verwijderen van 6 vragen, resulterend in een vragenlijst van 24 vragen. Met de verzamelde gegevens in een studie onder 500 deelnemers is een explorerende factor analyse uitgevoerd. Resultaat is een vragenlijst met 16 vragen, opgedeeld in 4 factoren. Deze vragenlijst is in een studie uitgezet onder een andere groep van 500 respondenten. De uitgevoerde bevestigende factor analyse en de betrouwbaarheidsanalyse geven aan dat deze vragenlijst de juiste vragen en factoren bevat.

De uiteindelijke SeBIS (Security Behavior Intentions Scale) bestaat uit 16 items, die op een unieke manier in kaart worden gebracht op vier factoren: beveiliging van de apparatuur (sluitsystemen met behulp van wachtwoorden, PIN-codes, enz.), het genereren van wachtwoorden (aanmaken en gebruiken van wachtwoorden), proactieve bewustwording en het bijwerken van de software (zorgen dat de software up-to-date is).

#### *Suggesties voor verder onderzoek*

Genoemde suggesties voor toekomstig onderzoek zijn:

- Onderzoek de psychometrie om een voorspellend model te bouwen;
- Voer studies uit om de SeBIS-resultaten van bedrijven en thuisgebruikers met elkaar te vergelijken;
- Voer een experiment uit om te onderzoeken hoe de sub-schalen van de SeBIS correleren met het werkelijke beveiligingsgedrag, aangezien het nu alleen intenties meet.

#### *Relevantie voor het eigen onderzoek*

De informatie in deze publicatie is te summier, vragenlijsten zijn niet aanwezig en de publicatie betreft een eerste validatie van een ontwikkeld model. Zodoende is deze publicatie op dit moment niet relevant voor mijn eigen onderzoek.

### Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness.

*Doel van het onderzoek*

Het doel van dit onderzoek is om de richting van de relatie tussen het bewustzijn van de individuen ten aanzien van informatiebeveiliging en hun gedrag ten aanzien van het gebruik van informatie- en communicatietechnologieën te achterhalen en het cruciale belang van de sub-factoren die deze relatie definiëren, aan te tonen.

*Opzet van het onderzoek*

In het onderzoek worden 4 onafhankelijke schalen gedefinieerd om het beveiligingsgedrag en het IBB van gebruikers te beoordelen, te weten:

- Risky Behavior Scale (RBS): meet de risicograad ten opzichte van het gedrag;
- Conservative Behavior Scale (CBS): meet hoe voorzichtig de gebruiker is bij het gebruik van een informatietechnologie en informatiesystemen;
- Exposure to Offence Scale (EOS): meet de blootstelling aan een cyberbeveiligingsincident als gevolg van eigen gedrag;
- Risk Perception Scale (RPS): meet de mate van gevaar of risico dat een gebruiker ziet in verband met informatietechnologie of informatiesystemen.

Op basis van de genoemde doelen van het onderzoek en de ontwikkelde schalen hebben de onderzoekers een viertal hypotheses opgesteld die zij middels een enquête willen toetsen. De vragen in de enquête zijn opgesteld in samenwerking met deskundigen en bestaan uit de volgende 5 delen:

1. Vragen die de demografische gegevens van de respondenten verzamelen;
2. Vragen met betrekking tot gebruikersprofielen;
3. Vragen met betrekking tot risicovol gedrag;
4. Vragen met betrekking tot het gedrag van respondenten ten aanzien van informatiebeveiliging en bedreigingen;
5. Vragen met betrekking tot de mate waarin gebruikers zich blootstellen aan cybercriminaliteit.

Vragen worden gemeten op een 5-punts Likert-schaal en zijn uitgezet onder een steekproef van studenten, academici en administratief personeel van een universiteit in Turkije.

*Resultaten en conclusies van het onderzoek*

Het doel van deze studie was om vast te stellen wat individuen denken en doen met betrekking tot informatietechnologieën en hun bewustwording over gerelateerde kwesties, hun gedrag en gedeeltelijk hun kennisniveau.

Resultaten laten zien dat er significante verschillen zijn tussen de academici, de administratieve medewerkers en de studenten in de RBS-, CBS- en RPS-scores. De verhouding van het gebruik van risicovolle informatietechnologie bij studenten is hoger dan bij de andere groepen. Deze bevinding toont aan dat studenten kwetsbaarder zijn voor risico's. Bovendien zijn de scores van studenten voor blootstelling aan criminaliteit ook hoger dan de andere groepen. In de CBS-scores konden geen significante verschillen worden gevonden. De groep met het laagste gemiddelde in RPS-score is de administratieve staf.

Volgens de resultaten is het zo dat hoe meer de respondenten bedreigingen waarnemen, hoe meer hun gedrag beschermend wordt. Er is een positieve relatie gevonden tussen CBS en RPS. Ook is er een positieve relatie tussen RBS en EOS; naarmate het gebruik van risicovolle technologieën toeneemt, neemt ook de verhouding tussen blootstelling aan criminaliteit en negatieve ervaringen toe. Er werd een positief verband gevonden tussen de responsieve RBS en hun dreigingsperceptie. Naarmate het gebruik van technologie toeneemt, worden individuen meer blootgesteld aan criminaliteit en nemen naast hun dreigingsperceptie ook hun dreigingsperceptie toe.

Hoewel er geen significant verschil is tussen de RBS-scores van de groep die een veiligheidstraining heeft gevolgd en de score van de groep die een dergelijke training niet heeft gevolgd, is de CBS-score van de eerste groep hoger dan de score van de tweede groep. Deze bevinding toont duidelijk aan dat een dergelijke training het bewustzijn van de individuen verhoogt.

Een andere belangrijke resultaat is dat respondenten cybercriminaliteit niet aan een autoriteit melden omdat ze niet weten met wie ze contact moeten opnemen. Ook wordt geconstateerd dat de bewustwording op dit punt laag is.

Een van de belangrijkste bevindingen van dit onderzoek is dat hoe hoger het opleidingsniveau, hoe hoger het IBB. Het blijkt dat het opleidingsniveau of het volgen van een training in informatiebeveiliging het risiconiveau in het gedrag van de gebruikers vermindert.

*Suggesties voor verder onderzoek*

Genoemde suggesties voor toekomstig onderzoek zijn:

- Verder onderzoek zou baat kunnen hebben bij een concentratie op verschillende gebruikersgroepen op basis van dezelfde voorgestelde vier schalen.
- Herhaling van het onderzoek met een grotere populatieomvang en in verschillende organisatorische domeinen om de toepasbaarheid van het onderzoeksmodel te verhogen en nieuwe inzichten te verzamelen die gebruikt kunnen worden om nieuwe inhoud voor de informatievoorziening op maat te maken.

*Relevantie voor het eigen onderzoek*

- Het onderzoek geeft geen duidelijk model voor het meten van IBB, de vragen ontbreken en de getoetste hypotheses hebben vooral betrekking op effecten van bepaalde gebeurtenissen. Dit sluit niet goed aan bij mijn onderzoeksvraag.
- Het onderdeel wat goed aansluit is dat binnen dit onderzoek verschillende groepen met elkaar worden vergeleken, iets wat ik ook binnen mijn onderzoek wil doen.
- De ontwikkelde methode is alleen getoetst binnen 1 universiteit in Turkije en daarmee onvoldoende gevalideerd.

### McCormac, A., Calic, D., Parsons, K., Zwaans, T., Butavicius, M., & Pattison, M. (2016). Test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q).

*Doel van het onderzoek*

Het doel van dit onderzoek is om te bepalen of de HAIS-Q zowel externe betrouwbaarheid als interne consistentie heeft.

*Opzet van het onderzoek*

Dit onderzoek beschouwt in eerste instantie verschillende methoden die ontwikkeld zijn voor het meten van IBB, waarbij zij zich uiteindelijk richten op het testen van de betrouwbaarheid en interne consistentie van de HAIS-Q omdat deze op het moment van het onderzoek het meest uitgebreid is getest.

In het kader van dit onderzoek werden twee enquêtes uitgevoerd, waarbij dezelfde steekproef van deelnemers werd gebruikt. Hierdoor konden de resultaten van de eerste test (T1) en de hertest (T2) worden vergeleken.

*Resultaten en conclusies van het onderzoek*

Om de interne consistentie van de HAIS-Q te meten, werden de alfacoëfficiënten van de Cronbach op T1 en T2 vergeleken. Zowel de scores voor kennis, houding, zelf gerapporteerd gedrag en IBB op T1 en T2 als de scores voor de zeven aandachtsgebieden op T1 en T2, laten een minimale variatie zien in de geschatte interne consistentie tussen de twee tijdsintervallen.

Betrouwbaarheid wordt beoordeeld door te kijken naar de correlatie tussen de resultaten van T1 en die van T2. De resultaten leveren voldoende bewijs dat de HAIS-Q een stabiele maatstaf is.

Deze studie heeft aangetoond dat de HAIS-Q, een maatstaf voor IBB, extern betrouwbaar en intern consistent is.

*Suggesties voor verder onderzoek*

Genoemde suggesties voor toekomstig onderzoek zijn:

- Het zou nuttig zijn om na te gaan waarom bepaalde deelnemers hun gedrag veranderden na het voltooien van de HAIS-Q en waarom anderen dat niet deden;
- Door het test-hertestonderzoek met een bekende organisatie uit te voeren, zouden we beter in staat zijn om te beoordelen wat er tussen T1 en T2 gebeurt. Eventuele tussenliggende trainingen of organisatorische veranderingen kunnen worden gecontroleerd en verantwoord;
- Uitvoeren van verdere validiteits- en betrouwbaarheidsbeoordelingen van de HAIS-Q in verschillende landen om de effecten van eventuele culturele verschillen te meten.

*Relevantie voor het eigen onderzoek*

- Deze publicatie bespreekt verschillende methodieken voor het meten van bewustzijn en hun waarde, dit sluit aan bij mijn eigen conclusies van de gelezen publicaties, wat inhoudt dat de HAIS-Q en de daarvoor gebruikte methodiek het best past bij mijn eigen onderzoek.
- Bestudering van eerdere publicaties heeft aangetoond dat de methodiek voor ontwikkeling van de HAIS-Q en de uiteindelijke HAIS-Q bruikbaar kunnen zijn voor mijn onderzoek. Met deze extra positieve validatie van de methodiek wordt deze meer betrouwbaar. Echter, zoals de onderzoekers zelf aangeven is de methodiek vooral binnen Australië gevalideerd.

### Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies.

*Doel van het onderzoek*

Het doel van dit onderzoek is om de construct-validiteit van de HAIS-Q, als een effectief instrument voor het meten van IBB, verder vast te stellen.

*Opzet van het onderzoek*

De construct validiteit wordt getoetst door het uitvoeren van 2 studies.

In de eerste studie wordt de convergente validiteit van de HAIS-Q beoordeeld, door een maatregel voor gedrag te nemen en aan te tonen dat deze correleert met de theoretisch-gerelateerde meting van het IBB. De maatregel die genomen wordt is het uitvoeren van een empirisch phishingexperiment, wat gezien wordt als een gedragsmaatregel om bewustzijn te verhogen, gevolgd door de meting van het IBB door invulling van de HAIS-Q. Respondenten waren 112 studenten in Australië.

In de tweede studie is de HAIS-Q door 531 werkende Australiërs ingevuld. Voorafgaand aan de data-analyse werden de antwoorden van de deelnemers onderzocht op tekenen van non-responsiviteit van de inhoud, wat helpt bij het identificeren van antwoorden die zonder de nodige zorgvuldigheid zijn gegeven. Dit omvatte bijvoorbeeld deelnemers die op alle vragen hetzelfde antwoord gaven. Op basis hiervan werden 26 antwoorden uitgesloten, wat resulteerde in een definitieve steekproef van 505 werkende Australiërs.

*Resultaten en conclusies van het onderzoek*

Binnen de eerste studie laten de resultaten zien dat er een medium significante positieve correlatie is gevonden tussen de totale IBB score en de phishingprestatie. De relatie was nog sterker toen het focusgebied voor e-mailgebruik van de HAIS-Q werd onderzocht. De resultaten leveren bewijs voor de construct validiteit van de HAIS-Q, aangezien deelnemers die hogere scores hadden op de HAIS-Q ook betere phishingprestaties hadden. Dit betekent dat de HAIS-Q aspecten van informatiebeveiliging gerelateerd gedrag kan voorspellen.

De resultaten van de factoranalyse van de tweede studie, waar de HAIS-Q is getest binnen een grote populatie respondenten, ondersteunen de construct validiteit van de HAIS-Q.

*Suggesties voor verder onderzoek*

Genoemde suggesties voor toekomstig onderzoek zijn:

- Verricht in de toekomst onderzoek naar de ontwikkeling en validering van aanvullende elementen om het hoofd te bieden aan evoluerende bedreigingen, waaronder het internet der dingen, cloud computing en Bring Your Own Device beleid;
- De relatie tussen IBB en privacybelangen moet verder worden onderzocht, door opname van maatregelen van privacybelangen en -gedrag, evenals andere maatregelen van individuele en organisatorische factoren, om hun relatie met het bewustzijn van medewerkers te evalueren;
- Om het vermogen om respondenten die op een maatschappelijk wenselijke of onzorgvuldige manier reageren verder uit te filteren te verbeteren, kan een IBB sociale-wenselijkheidsschaal worden opgenomen in de HAIS-Q. Deze schaal bestaat uit een set van uitspraken, specifiek voor de aandachtsgebieden binnen de HAIS-Q die volstrekt onnodig informatiebeveiligingsgedrag vertegenwoordigen;
- Toekomstige onderzoek kan gegevens uit andere regio's verzamelen, die meer inzicht zullen geven in de generaliseerbaarheid van de HAIS-Q als een geldige en betrouwbare maatstaf voor IBB.

*Relevantie voor het eigen onderzoek*

- Bestudering van eerdere publicaties heeft aangetoond dat de methodiek voor ontwikkeling van de HAIS-Q en de uiteindelijke HAIS-Q bruikbaar kunnen zijn voor mijn onderzoek. Met deze extra positieve validatie van de methodiek wordt deze meer betrouwbaar;

- De aanbevelingen voor verder onderzoek onderkennen ook het feit dat de huidige HAIS-Q nog niet alle relevante gebieden van IBB afdekt. De auteurs geven aan dat zij in de toekomst de vragenlijst willen uitbreiden. Dit betekent dat ik dit ook binnen mijn onderzoek kan doen, zodat aansluiting bij de (ziekenhuis)zorg thema's gevonden kan worden. Wellicht is een modulaire vragenlijst mogelijk waarbij de onderzoeker alleen die onderdelen onderzoekt die relevant zijn voor zijn/haar organisatie.

### McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness.

*Doel van het onderzoek*

Het hoofddoel is het onderzoeken van de relatie tussen het IBB van individuen en de individuele verschillen in factoren, namelijk leeftijd, geslacht, persoonlijkheid en risicobereidheid.

*Opzet van het onderzoek*

De factoren worden verzameld door middel van de eerder ontwikkelde HAIS-Q vragenlijst. Deze is ingevuld door 505 respondenten die werken in Australië.

*Resultaten en conclusies van het onderzoek*

Resultaten laten zien dat oudere volwassenen een hoger IBB hebben in vergelijking met jongere volwassenen, wat in eerder onderzoek ook geconstateerd is. Met betrekking tot geslacht werd een klein significant verschil gevonden, waarbij vrouwen hogere scores behaalden in vergelijking met mannen.

Regressieanalyses zijn uitgevoerd om de impact van persoonlijkheid, individuele verschillen en de neiging tot het nemen van risico's op het IBB te onderzoeken. Ten eerste bleek dat meer bewuste, aangename en open individuen en individuen met een neiging tot het nemen van minder risico's hogere scores van IBB hadden, in relatie tot de persoonlijkheid. Verder bleek uit regressieanalyses dat consciëntieusheid, aangenaamheid, risicobereidheid en emotionele stabiliteit een belangrijke verklaring vormden voor de verschillen in IBB. Deze bevindingen sluiten gedeeltelijk aan bij eerder onderzoek.

*Suggesties voor verder onderzoek*

Genoemde suggesties voor toekomstig onderzoek zijn:

- Toekomstig onderzoek zou de relatie tussen IBB en individuele verschillen in elk van de zeven aandachtsgebieden kunnen onderzoeken;
- Gezien het feit dat consciëntieusheid en vriendelijkheid de meeste verschillen in bewustzijn verklaren, rechtvaardigen deze factoren verder onderzoek. Bijzondere facetten binnen consciëntieusheid en aangenaamheid zouden in toekomstig onderzoek in aanmerking kunnen worden genomen;
- Gezien de beperkte reikwijdte van dit onderzoek, kunnen ook andere factoren worden opgenomen, bijvoorbeeld het vertrouwen van een individu in computers en de frequentie waarmee hij toegang heeft tot het internet;
- Leeftijdsverschillen in IBB moeten ook verder onderzocht worden, gezien het feit dat er een significante relatie bestond tussen leeftijd en IBB;
- Hoewel interventie en organisatorische factoren, zoals trainingsprogramma's en de beveiligingscultuur van de organisatie niet binnen het bestek van dit onderzoek vielen, is het waarschijnlijk dat dergelijke factoren een belangrijke rol spelen bij het beïnvloeden van individueel beveiligingsgedrag;
- Toekomstig onderzoek zou ook kunnen kijken naar de potentiële wisselwerking tussen de veiligheidscultuur en individuele verschilfactoren.

*Relevantie voor het eigen onderzoek*

- Deze publicatie is een uitbreiding van eerder onderzoek van dezelfde auteurs, waarbij extra factoren die van invloed kunnen zijn op gedrag worden onderzocht. Dit betreft een extra validatie van de HAIS-Q, maar wederom binnen Australië.
- De onderzochte factoren maken inzichtelijk dat deze methodiek ook gebruikt kan worden om groepen onderling te vergelijken op basis van individuele factoren. Binnen mijn onderzoek wil ik de verschillende functies met elkaar vergelijken, met deze methodiek is dit dus mogelijk.

## Van Wissen, D. (2017). Measuring Information Security Awareness.

### *Doel van het onderzoek*

Bepalen van de betrouwbaarheid en validiteit van de HAIS-Q, alsook te bepalen hoe de HAIS-Q in de praktijk presteert.

### *Opzet van het onderzoek*

De betrouwbaarheid van de HAIS-Q wordt getoetst middels een statistische analyse, meting van de Cronbach alfa, op de verkregen data uit de enquête onder 58 respondenten. De validiteit van de vragenlijst wordt bepaald door het voeren van een kwalitatief onderzoek middels interviews met zes deskundigen.

Om te bepalen hoe de HAIS-Q in de praktijk presteert, wordt het gehele meetproces doorlopen opdat sterke en zwakke eigenschappen van de meting worden ervaren. Door deze te noteren en een analyse uit te voeren van de vragen, interviews en feedbackvragen wordt bepaald hoe de HAIS-Q presteert.

### *Resultaten en conclusies van het onderzoek*

Op basis van de statistische analyse wordt gesteld dat de interne betrouwbaarheid van de HAIS-Q hoog is. De hoogte doet vermoeden dat er sprake is van redundantie in de vragen. Vanuit de feedback binnen de organisatie wordt aangegeven dat de kans op sociaal wenselijk antwoorden aanwezig is. Echter geeft men ook aan hier geen probleem te verwachten zolang de anonimiteit binnen het onderzoek is gewaarborgd.

Op basis van een analyse van de antwoorden van de geïnterviewden aangaande de inhoudsvaliditeit is geconcludeerd dat veel van de vragen uit de vragenlijst nuttig of essentieel worden bevonden. Echter er wordt ook aangegeven dat er onderwerpen onderbelicht blijven en/of niet van toepassing zijn. Conclusie is dat de vragenlijst niet universeel bruikbaar is en vooraf getoetst moet worden aan gangbare beleidsregels binnen de organisatie of branche van onderzoek.

De opdeling van de vragenlijst naar dimensies en focus area's wordt nuttig gevonden, omdat met de uitkomsten gericht gestuurd kan worden op verbetering. De feedback van respondenten geeft aan dat het aantal vragen acceptabel is, de hoeveelheid tijd die het kost om de enquête in te vullen positief wordt ervaren, de vragen duidelijk zijn maar niet altijd van toepassing. De resultaten van de enquête zijn in twee verschillende vormen teruggekoppeld, welke beide nuttig worden bevonden. Conclusie is dat de HAIS-Q door de vaste vragenlijst en eenvoudige opzet een zeer praktisch meetinstrument is.

### *Suggesties voor verder onderzoek*

Genoemde suggesties voor toekomstig onderzoek zijn:

- Onderzoek of sociaal wenselijk antwoorden kan worden herkend of voorkomen;
- Onderzoek of HAIS-Q kan worden heringericht, zonder dat steeds drie vragen achter elkaar over hetzelfde onderwerp worden gesteld;
- Maak goed gebruik van de alternatieve vorm als vragen in een andere vorm terugkeren, om daarmee te testen op betrouwbaarheid;
- Onderzoek of HAIS-Q als generieke vragenlijst in andere omgevingen dan Organisatie X wel volledig toepasbaar is. Als blijkt dat HAIS-Q in meer omgevingen moet worden aangepast voor een correcte meting, beschouw HAIS-Q dan als de basis voor een goed meetinstrument en niet als de totaaloplossing;
- Overweeg de vragen van HAIS-Q te voorzien van meer context, zodat ze voor respondenten ondubbelzinnig zijn;
- Heroverweeg negatief geformuleerde vragen ten gunste van de leesbaarheid;
- Overweeg extra antwoordopties, bijvoorbeeld "niet van toepassing" of "weet ik niet";
- Onderhoud HAIS-Q, door de focus area's als modules te beschouwen die kunnen worden toegevoegd, verwijderd of vernieuwd. Overweeg de vragenlijst uit te breiden met onderwerpen zoals social engineering of opslag van data. Voeg eventueel een versienummering toe;
- Ga vertrouwelijk om met resultaten van een meting naar informatiebeveiligingsbewustzijn;

- Onderzoek of de weegfactoren uit de methode van Kruger & Kearney meerwaarde hebben bij toepassing van HAIS-Q.

*Relevantie voor het eigen onderzoek*

- Ook dit onderzoek laat zien dat de HAIS-Q een betrouwbare manier is om het IBB te toetsen;
- Voorafgaand aan de toepassing is het noodzakelijk om de vragenlijst te toetsen tegen staand beleid van de organisatie en/of de branche;
- Bekijken in hoeverre het mogelijk is om de betrouwbaarheid van de vragenlijst te toetsen door vergelijking van daadwerkelijk gedrag met de ingevulde vragenlijsten;
- Om de validiteit van de vragenlijst te verhogen, meet ik wat ik wil meten, onderzoeken of het te gebruiken enquête instrument aangevuld kan worden met informatieballonnen voor verdere context bij een vraagstelling.
- Onderzoeken of het mogelijk is om de vragenlijst ad random in elkaar te zetten, zodat vragen aangaande een focus area elkaar niet direct opvolgen. Vragen aangaande eenzelfde focus area zijn net verschillend aan elkaar door de dimensie waarop zij betrekking hebben, hierbij kan de informatieballon uit het vorige punt helpen om de context beter weer te geven.

### Schaeken, M. (2018). Information security awareness measuring & social engineering 2.0.

#### *Doel van het onderzoek*

Het doel van dit onderzoek is het creëren van een alternatief verbeterd HAIS-Q op basis van gevalideerd onderzoek en het valideren van de relaties tussen de kennis van werknemers over beleid en procedures, hun houding ten opzichte van beleid en procedures en hun zelf gerapporteerde gedrag bij het gebruik van een computer of ander ICT-materiaal zoals een smartphone.

#### *Opzet van het onderzoek*

In dit onderzoek wordt gekozen voor een gemengde strategie, waarbij kwalitatieve en kwantitatieve methoden die achtereenvolgens worden uitgevoerd, worden gecombineerd.

Met een vanuit de literatuur gevalideerde methode voor het meten van IBB is een verkenning uitgevoerd om algemene contextinformatie te verkrijgen en de standaard HAIS-Q vragen te herzien. Deze inductieve verzamelde informatie werd gebruikt om de oorspronkelijke vragen aan te passen aan de context en de nieuwste SE2.0-aanvallen en verdedigingsmechanismen.

De ontstane gestructureerde vragenlijst van het HAIS-Q is in een online enquête aangeboden aan alle medewerkers die met digitale informatie werken in ziekenhuizen in het Vlaams sprekende deel van België, in de veronderstelling dat de verkregen steekproef de populatie zal vertegenwoordigen. De verkregen resultaten van de enquête worden statistisch geanalyseerd.

#### *Resultaten en conclusies van het onderzoek*

De resultaten van dit onderzoek tonen aan dat het verbeterde HAIS-Q een geldig en betrouwbaar instrument is om het IBB in Belgische ziekenhuizen te meten.

#### *Suggesties voor verder onderzoek*

Genoemde suggesties voor toekomstig onderzoek zijn:

- In vervolgonderzoek zou de invloed van het aspect cultuur en cultuurvariabelen verder onderzocht kunnen worden, net als het privacyaspect.
- Vervolgonderzoek binnen ziekenhuizen zou kunnen worden uitgevoerd door gebruik te maken van een intelligente chatbot die beschikbaar is via een app op een mobiele telefoon in plaats van een online survey.

#### *Relevantie voor het eigen onderzoek*

- Het onderzoek is wederom een validatie van het de HAIS-Q waardoor deze meer bruikbaar wordt voor mijn onderzoek.
- De gebruikte methodiek binnen dit onderzoek kan ik eveneens gebruiken voor mijn eigen onderzoek, aangezien ik de vragenlijst wil verbeteren en uitbreiden om vervolgens te valideren.
- Genoemde suggestie voor vervolgonderzoek sluit aan bij mijn vraagstelling.

## Bijlage II Interviewprotocol en vragen interview ontwikkeling nieuw HAIS-Q

1. Inleiding (5 minuten)
   a. Dank voor deelname
   b. Gelegenheid tot het stellen van vragen door geïnterviewde
   c. Doornemen interviewopzet
   d. Toestemming vragen voor het opnemen van het interview

2. Introductie van geïnterviewde (5 minuten)
   a. Kunt u uw functie binnen de organisatie beschrijven?
   b. Wat is uw rol of relatie met het werkveld informatiebeveiliging en privacy?
   c. Bent u bekend met de geldende wet- en regelgeving op het gebied van informatiebeveiliging en privacy binnen de gezondheidszorg?
   d. Bent u bekend met de methoden waarop in de gezondheidszorg naleving van wet- en regelgeving is vorm gegeven?

3. Ervaringen geïnterviewde met informatiebeveiligingsincidenten en/of datalekken (5 minuten)
   a. Wat zijn uw ervaringen met informatiebeveiligingsincidenten?
   b. Wat zijn uw ervaringen met datalekken?

4. Oorzaken informatiebeveiligingsincidenten en/of datalekken (5 minuten)
   a. Wat zijn naar uw mening oorzaken van informatiebeveiligingsincidenten?
   b. Wat zijn naar uw mening oorzaken van datalekken?
   c. Is er naar uw weten binnen de gezondheidszorg aandacht voor de factor mens in het voorkomen van informatiebeveiligingsincidenten en/of datalekken?

5. HAIS-Q, beginnend met uitleg over de HAIS-Q en het model (20 minuten)
   a. Zijn de genoemde aandachtsgebieden en subgebieden naar uw mening relevant voor het meten van informatiebeveiligingsbewustzijn binnen de gezondheidszorg?
   b. Missen er naar uw mening aandachtsgebieden in deze vragenlijst?

6. Privacy als aandachtsgebied (15 minuten)
   a. Heeft het naar uw mening toegevoegde waarde om privacy als aandachtsgebied toe te voegen aan de vragenlijst voor het meten van informatiebeveiligingsbewustzijn?
   b. Wat zijn naar uw mening relevante subgebieden binnen het aandachtsgebied privacy in relatie tot naleving van geldend privacybeleid?

7. Afronding
   a. Dank voor deelname (5 minuten)
   b. Vraag geïnterviewde feedback op het interview
   c. Geef geïnterviewde uitleg over het verloop van het verdere onderzoek, inclusief het 2$^{e}$ interview

## Bijlage III Interviewprotocol en vragen interview validatie bestaande HAIS-Q

1. Inleiding (5 minuten)
   a. Dank voor deelname
   b. Gelegenheid tot het stellen van vragen door geïnterviewde
   c. Doornemen interviewopzet
   d. Toestemming vragen voor het opnemen van het interview

2. Introductie van geïnterviewde, bij 1e interview (5 minuten)
   a. Kunt u uw functie binnen de organisatie beschrijven?
   b. Wat is uw rol of relatie met het werkveld informatiebeveiliging en privacy?
   c. Bent u bekend met de geldende wet- en regelgeving op het gebied van informatiebeveiliging en privacy binnen de gezondheidszorg?
   d. Bent u bekend met de methoden waarop in de gezondheidszorg naleving van wet- en regelgeving is vorm gegeven?

3. Validiteit ontwikkelde vragenlijst (20 minuten)
   a. Is het gelukt om van alle vragen aan te geven of u deze essentieel, nuttig maar niet essentieel of niet noodzakelijk vindt?
   b. Zijn de vragen naar uw mening helder in de context van de gezondheidszorg?
   c. Meet de vragenlijst naar uw mening het informatiebeveiligingsbewustzijn?
   d. Is de vragenlijst naar uw mening compleet?
   e. Wat zijn naar uw mening sterke kanten van de vragenlijst?
   f. Wat zijn naar uw mening zwakke kanten van de vragenlijst?

4. Verwachting bruikbaarheid vragenlijst (10 minuten)
   a. Denkt u dat medewerkers in de gezondheidszorg bereid zouden zijn de vragenlijst in te vullen?
   b. Denkt u dat medewerkers in de gezondheidszorg de vragenlijst waarheidsgetrouw zullen invullen?
   c. Levert de vragenlijst naar uw mening bruikbare informatie op voor een organisatie in de gezondheidszorg?

5. Toevoegingen vragenlijst (5 minuten)
   a. Denkt u dat het toegevoegde waarde heeft om vragen op individueel niveau toe te voegen aan de vragenlijst en zo ja, waarom?
   b. Denkt u dat het toegevoegde waarde heeft om vragen op organisatie niveau toe te voegen aan de vragenlijst en zo ja, waarom?
   c. Denkt u dat het toegevoegde waarde heeft om vragen op interventie niveau toe te voegen aan de vragenlijst en zo ja, waarom?

6. Afronding (5 minuten)
   a. Dank voor deelname
   b. Vraag geïnterviewde feedback op het interview
   c. Geef geïnterviewde uitleg over het verloop van het verdere onderzoek

# Bijlage IV Informatieblad Interviewrondes

Binnen dit onderzoek zijn 3 interviewrondes gehouden. Bij de agenda uitnodiging voor elk interview is een informatieblad meegestuurd, wat inzicht geeft in de doelstelling van het onderzoek in zijn geheel en de opzet van het interview waar de uitnodiging betrekking op heeft specifiek.

Onderstaand het generieke deel van het informatieblad en daarna de specifieke onderdelen die per uitnodiging verschillen.

## Generieke onderdelen informatieblad

**1. Titel van het afstudeeronderzoek**

De Human Aspects of Information Security Questionnaire (HAIS-Q): Doorontwikkeling met het aspect privacy

**2. Naam, functie, contactgegevens onderzoeker en begeleider**

Onderzoeker: Petra Verbeek

Functie: Student masteropleiding Business Process Management & ICT, Open Universiteit

Contactgegevens: 06 – 19 26 67 07, p.verbeek@nwz.nl

Begeleider: Prof. Dr. L. Bijlsma (lex.bijlsma@ou.nl); Dr. L.W. Rutledge (lloyd.rutledge@ou.nl)

**3. Beschrijving afstudeeronderzoek**

Met de ontwikkelingen van informatie- en communicatietechnologie en de daardoor verdergaande digitalisering van de samenleving, zijn informatiebeveiliging en privacy steeds belangrijkere onderwerpen. Regulering vindt plaats vanuit de overheid en vaak staan de regels waar organisaties aan moeten voldoen op gespannen voet met het gebruikersgemak wat eindgebruikers willen ervaren.

Binnen de keten van zorgverlening, waaronder ziekenhuizen, zijn zorgverleners voor het uitoefenen van hun taak in hoge mate afhankelijk van de informatie die opgeslagen wordt in de verschillende systemen. Ook hier is het inregelen van afdoende informatiebeveiligingsmaatregelen, opdat de privacy van de patiënt geborgd wordt, in combinatie met de werkbaarheid voor de zorgverlener vaak een groot probleem. Het goed inregelen en toepassen van maatregelen blijkt vaak, om verschillende redenen, problematisch met als gevolg dat er informatiebeveiligingsincidenten optreden, mogelijk met ongewenste publiciteit ten gevolg. De omvang van deze incidenten, bijvoorbeeld het gebruik van ‘breaking-the-glass’ procedures, is zodanig hoog dat het vermoeden bestaat dat de interventies zeer regelmatig niet voldoen aan wet- en regelgeving. De Autoriteit Persoonsgegevens meldt in haar jaarverslag 2018 20.881 gerapporteerde datalekken, waarvan 29% in de sector gezondheid en welzijn (Autoriteit Persoonsgegevens, 2019b). Ook dit is een indicatie dat nog niet alle maatregelen zorgvuldig worden nageleefd of juist zijn geïmplementeerd. Een recent onderzoek van de AP binnen een ziekenhuis heeft aangetoond dat de beveiliging van patiëntendossiers niet op orde was, leidend tot een zeer hoge boete (Autoriteit Persoonsgegevens, 2019a, 2019c).

De complexiteit van de zorgprocessen en de urgentie van de beschikbaarheid van informatie om de zorgtaken uit te voeren maakt dat de maatregelen ten behoeve van informatiebeveiliging en privacy in bijvoorbeeld het ziekenhuisinformatiesysteem een combinatie zijn van technische restricties en organisatorische procedures uit te voeren door medewerkers. Verschillende onderzoeken laten zien dat juist deze menselijke factor vaak oorzaak is van beveiligingsincidenten en daarmee een kritieke factor binnen de informatiebeveiliging is (Evans et al., 2016; Parsons et al., 2010; Schultz, 2005). De mate van informatiebeveiligingsbewustzijn (hierna: IBB) van de medewerkers wordt daarmee een belangrijk onderdeel voor het mitigeren van risico’s binnen de informatiebeveiliging.

Het doel van dit onderzoek is om te bepalen hoe het IBB van medewerkers geloofwaardig en correct te meten, waarbij alle relevante onderdelen voor de gezondheidszorg onderdeel van de meting zijn.

Uitgangspunt is dat meer informatiebeveiligingsbewuste medewerkers minder incidenten tot gevolg hebben.

## Specifiek onderdelen informatieblad

Onderstaande worden de specifieke onderdelen van het informatieblad beschreven. Dit betreft de interviewopzet die per interviewronde afwijkt.

**4a. Interviewopzet interview ontwikkeling**

- Het interview wordt bij voorkeur door de onderzoeker in persoon uitgevoerd. Indien dit door (corona) omstandigheden niet mogelijk is, wordt het interview via Microsoft Teams afgenomen;
- Het interview wordt afgenomen bij leden van het senior management en bij experts in het werkgebied van informatiebeveiliging en privacy;
- Het betreft een semigestructureerd interview wat de onderzoeker de mogelijkheid geeft om door te vragen waar zij dat noodzakelijk vindt om het doel van het onderzoek te bereiken;
- De geïnterviewde hoeft geen voorbereidingen te treffen;
- De geïnterviewde werkt op vrijwillige basis mee aan het onderzoek en kan op elk moment ervoor kiezen niet langer mee te werken;
- Het interview vindt plaats in vertrouwen, wat inhoudt dat de naam en functie van de geïnterviewde niet gepubliceerd wordt;
- Het interview duurt maximaal anderhalf uur;
- Het interview wordt met toestemming opgenomen, zodat het getranscribeerd kan worden;
- De transcriptie van het interview wordt gebruikt om een kwalitatieve analyse uit te voeren om antwoord te verkrijgen op de vraag welke aandachtsgebieden van de bestaande vragenlijst het senior management relevant vindt voor de meting van het informatiebeveiligingsbewustzijn. Daarnaast moet deze analyse inzicht verschaffen in mogelijke subgebieden binnen het aandachtsgebied privacy.

**4b. Interviewopzet interview validatie**

- Het interview wordt bij voorkeur door de onderzoeker in persoon uitgevoerd. Indien dit door (corona) omstandigheden niet mogelijk is, wordt het interview via Microsoft Teams afgenomen;
- Het interview wordt afgenomen bij leden van het senior management en bij experts in het werkgebied van informatiebeveiliging en privacy;
- Het betreft een semigestructureerd interview wat de onderzoeker de mogelijkheid geeft om door te vragen waar zij dat noodzakelijk vindt om het doel van het onderzoek te bereiken;
- De geïnterviewde krijgt ter voorbereiding op het interview de (vertaalde) vragenlijst die als basis dient voor de meting van informatiebeveiligingsbewustzijn, aangevuld met het nieuw ontwikkelde aandachtsgebied privacy. De geïnterviewde wordt gevraagd om vooraf per vraag aan te geven of zij deze 1. Essentieel, 2. Nuttig maar niet essentieel OF 3. Niet noodzakelijk vinden;
- De geïnterviewde werkt op vrijwillige basis mee aan het onderzoek en kan op elk moment ervoor kiezen niet langer mee te werken;
- Het interview vindt plaats in vertrouwen, wat inhoudt dat de naam en functie van de geïnterviewde niet gepubliceerd wordt;
- Het interview duurt maximaal één uur;
- Het interview wordt met toestemming opgenomen, zodat het getranscribeerd kan worden;
- De transcriptie van het interview wordt gebruikt om een kwalitatieve analyse uit te voeren om antwoord te verkrijgen op de vraag of de samengestelde vragenlijst valide is volgens senior management en experts.

**4c. Cognitieve test experts en zorgprofessionals**

- De cognitieve test wordt door de onderzoeker in persoon uitgevoerd;
- De cognitieve test wordt afgenomen bij experts in het werkgebied van informatiebeveiliging en privacy en bij een tweetal zorgprofessionals;

- De cognitieve test vraagt van de deelnemer dat de ontwikkelde vragenlijst in bijzijn van de onderzoeker wordt ingevuld, waarbij de deelnemer hardop zijn gedachten uitspreekt. De onderzoeker heeft hierbij de mogelijkheid om op basis van de antwoorden en/of haar observaties additionele vragen te stellen om verduidelijking te verkrijgen aangaande de gedachten en interpretaties van de deelnemer;
- De deelnemer hoeft geen voorbereidingen te treffen voor de test;
- De deelnemer werkt op vrijwillige basis mee aan het onderzoek en kan op elk moment ervoor kiezen niet langer mee te werken;
- De cognitieve test vindt plaats in vertrouwen, wat inhoudt dat de naam en functie van de deelnemer niet gepubliceerd wordt;
- De cognitieve test duurt maximaal anderhalf uur;
- De cognitieve test wordt met toestemming opgenomen, zodat het getranscribeerd kan worden;
- De transcriptie van de test wordt gebruikt om een kwalitatieve analyse uit te voeren om antwoord te verkrijgen op de vraag of de samengestelde vragenlijst valide is volgens experts en zorgprofessionals.

## Bijlage V Originele HAIS-Q (vertaald)

| Dimensies | Kennis | Houding | Gedrag |
|---|---|---|---|
| **Aandachtsgebied: Wachtwoord management** | | | |
| Gebruik van hetzelfde wachtwoord | Het is aanvaardbaar om mijn sociale media wachtwoorden te gebruiken voor mijn werkaccounts | Het is veilig om hetzelfde wachtwoord voor mijn sociale media accounts en werkaccounts te gebruiken | Ik gebruik verschillende wachtwoorden voor mijn sociale media accounts en mijn werkaccounts |
| Delen van wachtwoorden | Ik mag mijn werkwachtwoorden delen met collega's | Het is een slecht idee om mijn werkwachtwoorden te delen, zelfs als een collega erom vraagt | Ik deel mijn werkwachtwoorden met collega's |
| Gebruik van een sterk wachtwoord | Een mix van letters, cijfers en symbolen en een lengte van minimaal 8 karakters is noodzakelijk voor werkwachtwoorden | Het is veilig om een werkwachtwoord te hebben met alleen maar letters | Voor mijn werkwachtwoorden maak ik gebruik van een combinatie van letters, cijfers en symbolen en een lengte van minimaal 8 karakters |
| **Aandachtsgebied: Email gebruik** | | | |
| Klikken op links in e-mails van bekende afzenders | Ik mag op links in e-mails klikken van mensen die ik ken | Het is altijd veilig om op links te klikken in e-mails van mensen die ik ken | Ik klik niet altijd op links in e-mails ook al is deze afkomstig van iemand die ik ken |
| Klikken op links in e-mails van onbekende afzenders | Ik mag niet op een link in een e-mail van een onbekende afzender klikken | Er kan niets slechts gebeuren als ik op een link in een e-mail van een onbekende afzender klik | Als een e-mail van een onbekende afzender interessant lijkt, klik ik op een link in de e-mail |
| Openen van bijlagen in e-mails van onbekende afzenders | Ik mag e-mailbijlagen van onbekende afzenders openen | Het is riskant om een e-mailbijlage van een onbekende afzender te openen | Ik open geen e-mailbijlagen als de afzender mij onbekend is |
| **Aandachtsgebied: Internetgebruik** | | | |
| Downloaden van bestanden | Ik mag alle soorten bestanden naar mijn werkcomputer downloaden als ze me helpen om mijn werk te doen | Het kan riskant zijn om bestanden op mijn werkcomputer te downloaden | Ik download alle bestanden op mijn werkcomputer die me zullen helpen om de klus te klaren |
| Benaderen van dubieuze websites | Terwijl ik aan het werk ben, moet ik bepaalde websites niet bezoeken | Ook al heb ik toegang tot een website op het werk, betekent dat niet dat het een veilige website is | Als ik op het werk toegang heb tot het internet, bezoek ik elke website die ik wil bezoeken, zowel voor werk als privé doeleinden |
| Informatie online invoeren | Ik mag alle informatie op een website invoeren als dat me helpt bij het uitvoeren van mijn werk | Als het me helpt om mijn werk te doen, maakt het niet uit welke informatie ik op een website zet | Ik beoordeel de veiligheid van websites en het soort informatie dat gevraagd wordt in te voeren, alvorens deze informatie in te voeren |
| **Aandachtsgebied: Sociale media gebruik** | | | |
| Sociale media privacy instellingen | Ik moet regelmatig de privacy-instellingen op mijn sociale media-accounts controleren | Het is een goed idee om mijn sociale media privacy-instellingen regelmatig te herzien | Ik bekijk mijn sociale media privacy-instellingen niet regelmatig. |
| Rekening houden met gevolgen | Ik kan niet ontslagen worden voor iets wat ik op sociale media plaats | Het maakt niet uit of ik dingen op sociale media plaats die ik normaal gesproken niet in het openbaar zou zeggen | Ik plaats niets op sociale media voordat ik nadenk over eventuele (negatieve) gevolgen voor mijzelf en anderen |
| Plaatsen van informatie over werk | Ik kan posten wat ik wil over mijn werk op sociale media | Het is riskant om bepaalde informatie over mijn werk op sociale media te plaatsen | Ik plaats alles wat ik wil over mijn werk op sociale media |
| **Aandachtsgebied: Mobiele apparaten** | | | |
| Fysieke beveiliging van mobiele apparaten | Als ik in een openbare ruimte werk, moet ik mijn laptop altijd bij me houden | Als ik in een café werk, is het veilig om mijn laptop een minuutje onbeheerd achter te laten | Als ik in een openbare ruimte werk, laat ik mijn laptop onbeheerd achter |

| Dimensies | Kennis | Houding | Gedrag |
|---|---|---|---|
| Versturen van gevoelige informatie via wifi | Ik mag gevoelige werkbestanden of mails versturen via een openbaar Wi-Fi-netwerk | Het is riskant om gevoelige werkbestanden of mails te versturen via een openbaar Wi-Fi-netwerk | Ik verstuur soms gevoelige werkbestanden of mails via een openbaar Wi-Fi-netwerk |
| Over de schouder meekijken | Als ik aan een gevoelig document werk, moet ik ervoor zorgen dat onbevoegden niet op mijn laptopscherm kunnen meekijken | Het is riskant om gevoelige werkbestanden of mails op een laptop te openen als onbevoegden op mijn scherm kunnen meekijken | Ik controleer of onbevoegden niet op mijn laptop scherm kunnen meekijken als ik aan een gevoelig document werk |
| **Aandachtsgebied: Informatieverwerking** | | | |
| Het weggooien van gevoelige afdrukken | Gevoelige afdrukken kunnen op dezelfde manier worden weggegooid als niet-gevoelige afdrukken | Het weggooien van gevoelige afdrukken door ze bij het afval te leggen is veilig | Wanneer gevoelige afdrukken moeten worden weggegooid, zorg ik ervoor dat ze versnipperd of vernietigd worden |
| Het plaatsen van verwijderbare media | Als ik een USB-stick op een openbare plaats vind, moet ik hem niet op mijn privé of werkcomputer aansluiten | Als ik een USB-stick op een openbare plaats vind, kan er niets ergs gebeuren als ik hem op mijn privé of werkcomputer aansluit | Ik zou een USB-stick die ik op een openbare plaats heb gevonden niet in mijn privé of werkcomputer steken |
| Achterlaten van gevoelige informatie | Ik mag 's nachts afdrukken met gevoelige informatie op mijn bureau laten liggen | Het is riskant om ’s nachts afdrukken met gevoelige informatie op mijn bureau te laten liggen | Ik laat afdrukken die gevoelige informatie bevatten op mijn bureau liggen als ik er niet ben |
| **Aandachtsgebied: Melden van incidenten** | | | |
| Melden van verdacht gedrag | Als ik iemand zich verdacht zie gedragen op mijn werkplek, moet ik dat melden | Als ik iemand negeer die verdacht handelt op mijn werk, kan er niets ergs gebeuren | Als ik iemand verdacht zou zien handelen op mijn werkplek, zou ik er iets aan doen |
| Negeren van slecht veiligheidsgedrag van collega's | Ik mag niet voorbijgaan aan het slechte veiligheidsgedrag van mijn collega's | Er kan niets ergs gebeuren als ik slecht veiligheidsgedrag van een collega negeer | Als ik merk dat mijn collega de veiligheidsregels negeert, zou ik geen actie ondernemen |
| Melden van alle incidenten | Het is optioneel om beveiligingsincidenten te melden | Het is riskant om beveiligingsincidenten te negeren, ook al denk ik dat ze niet belangrijk zijn | Als ik een beveiligingsincident zou opmerken, zou ik het melden |

# Bijlage VI Resultaten enquête validiteit

| Wachtwoordmanagement | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Sub | zelfde wachtwoord | | | wachtwoord delen | | | sterkte wachtwoord | | | |
| Vraag | WWM0 | WWM3 | WWM6 | WWM1 | WWM4 | WWM7 | WWM2 | WWM5 | WWM8 | |
| | kennis | houding | gedrag | kennis | houding | gedrag | kennis | houding | gedrag | |
| A | 2 | 2 | 1 | 1 | 2 | 2 | 0 | 1 | 2 | 13 |
| B | 2 | 2 | 1 | 1 | 2 | 2 | 2 | 1 | 1 | 14 |
| C | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 18 |
| D | 0 | 0 | 2 | 0 | 2 | 2 | 2 | 0 | 2 | 10 |
| E | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 18 |
| F | 2 | 2 | 0 | 2 | 0 | 1 | 1 | 2 | 2 | 12 |
| G | 1 | 1 | 2 | 2 | 1 | 2 | 1 | 1 | 2 | 13 |
| H | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 17 |
| I | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 2 | 17 |
| J | 1 | 1 | 2 | 2 | 2 | 2 | 1 | 1 | 1 | 13 |
| K | 2 | 2 | 1 | 2 | 0 | 2 | 1 | 1 | 1 | 12 |
| Totaal | 17 | 18 | 17 | 18 | 17 | 21 | 16 | 14 | 19 | |

| eMail gebruik | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Sub | links bekende | | | links onbekend | | | openen bijlagen | | | |
| Vraag | EM0 | EM3 | EM6 | EM1 | EM4 | EM7 | EM2 | EM5 | EM8 | |
| | kennis | houding | gedrag | kennis | houding | gedrag | kennis | houding | gedrag | |
| A | 1 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 16 |
| B | 1 | 2 | 1 | 1 | 2 | 1 | 2 | 1 | 2 | 13 |
| C | 1 | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 15 |
| D | 1 | 1 | 1 | 2 | 0 | 1 | 0 | 2 | 2 | 10 |
| E | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 18 |
| F | 1 | 2 | 1 | 1 | 1 | 0 | 1 | 2 | 2 | 11 |
| G | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 16 |
| H | 1 | 2 | 1 | 2 | 2 | 2 | 1 | 2 | 2 | 15 |
| I | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 18 |
| J | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 18 |
| K | 2 | 2 | 0 | 1 | 1 | 2 | 1 | 2 | 2 | 13 |
| Totaal | 15 | 19 | 14 | 19 | 18 | 18 | 17 | 21 | 22 | |

| Internet gebruik | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Sub | downloaden files | | | dubieuze websites | | | online info invoeren | | | |
| Vraag | IG0 | IG3 | IG6 | IG1 | IG4 | IG7 | IG2 | IG5 | IG8 | |
| | kennis | houding | gedrag | kennis | houding | gedrag | kennis | houding | gedrag | |
| A | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 17 |
| B | 2 | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 1 | 16 |
| C | 2 | 2 | 2 | 1 | 2 | 2 | 1 | 1 | 2 | 15 |
| D | 1 | 0 | 2 | 2 | 1 | 1 | 2 | 0 | 2 | 11 |
| E | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 17 |
| F | 2 | 2 | 0 | 2 | 2 | 2 | 2 | 1 | 2 | 15 |
| G | 1 | 2 | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 15 |
| H | 2 | 2 | 2 | 1 | 2 | 1 | 2 | 1 | 1 | 14 |
| I | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 18 |
| J | 1 | 2 | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 13 |
| K | 2 | 2 | 1 | 0 | 2 | 2 | 2 | 2 | 2 | 14 |
| Totaal | 19 | 20 | 17 | 15 | 20 | 18 | 21 | 16 | 19 | |

| Sociale Media | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Sub | privacy settings | | | consequentie posten | | | posten over werk | | | |
| Vraag | SM0 | SM3 | SM6 | SM1 | SM4 | SM7 | SM2 | SM5 | SM8 | |
| | kennis | houding | gedrag | kennis | houding | gedrag | kennis | houding | gedrag | |
| A | 1 | 2 | 1 | 2 | 0 | 2 | 2 | 2 | 2 | 14 |
| B | 2 | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 16 |
| C | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 18 |
| D | 0 | 0 | 0 | 0 | 0 | 2 | 1 | 2 | 1 | 6 |
| E | 2 | 2 | 1 | 2 | 1 | 2 | 2 | 2 | 2 | 16 |
| F | 2 | 1 | 2 | 2 | 0 | 2 | 2 | 0 | 1 | 12 |
| G | 1 | 1 | 1 | 2 | 1 | 2 | 2 | 2 | 1 | 13 |
| H | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 18 |
| I | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 17 |
| J | 1 | 2 | 1 | 0 | 2 | 2 | 2 | 2 | 2 | 14 |
| K | 2 | 2 | 0 | 0 | 0 | 2 | 2 | 1 | 2 | 10 |
| Totaal | 17 | 16 | 13 | 15 | 12 | 22 | 21 | 19 | 19 | |

| Mobiele apparaten | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Sub | achterlaten laptop in | | | gebruik open wifi | | | shoulder surfing | | | |
| Vraag | MA0 | MA3 | MA6 | MA1 | MA4 | MA7 | MA2 | MA5 | MA8 | |
| | kennis | houding | gedrag | kennis | houding | gedrag | kennis | houding | gedrag | |
| A | 2 | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 16 |
| B | 1 | 1 | 1 | 2 | 2 | 2 | 1 | 2 | 2 | 14 |
| C | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 18 |
| D | 2 | 1 | 1 | 1 | 2 | 1 | 2 | 1 | 2 | 13 |
| E | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 18 |
| F | 2 | 0 | 0 | 2 | 1 | 2 | 1 | 2 | 2 | 12 |
| G | 2 | 1 | 1 | 2 | 1 | 1 | 1 | 2 | 1 | 12 |
| H | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 18 |
| I | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 17 |
| J | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 18 |
| K | 0 | 0 | 0 | 2 | 1 | 2 | 1 | 1 | 2 | 9 |
| Totaal | 19 | 14 | 14 | 21 | 19 | 20 | 18 | 20 | 20 | |

| Informatieverwerking | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Sub | weggooien gevoelige | | | omgang met | | | achterlaten gevoelige | | | |
| Vraag | IV0 | IV3 | IV6 | IV1 | IV4 | IV7 | IV2 | IV5 | IV8 | |
| | kennis | houding | gedrag | kennis | houding | gedrag | kennis | houding | gedrag | |
| A | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 1 | 2 | 16 |
| B | 2 | 1 | 2 | 2 | 2 | 2 | 1 | 2 | 1 | 15 |
| C | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 18 |
| D | 0 | 0 | 2 | 2 | 0 | 1 | 1 | 2 | 0 | 8 |
| E | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 18 |
| F | 2 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 2 | 10 |
| G | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 1 | 16 |
| H | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 18 |
| I | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 2 | 16 |
| J | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 18 |
| K | 0 | 1 | 2 | 0 | 2 | 0 | 1 | 2 | 0 | 10 |
| Totaal | 17 | 17 | 21 | 19 | 18 | 17 | 17 | 19 | 18 | |

| Melden incidenten | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Sub | verdachte individuen | | | slecht veiligheidsgedrag | | | melden van beveiligings | | | |
| Vraag | MEL0 | MEL3 | MEL6 | MEL1 | MEL4 | MEL7 | MEL2 | MEL5 | MEL8 | |
| | kennis | houding | gedrag | kennis | houding | gedrag | kennis | houding | gedrag | |
| A | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 17 |
| B | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 1 | 2 | 16 |
| C | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 18 |
| D | 2 | 1 | 2 | 2 | 0 | 0 | 0 | 1 | 2 | 10 |
| E | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 17 |
| F | 1 | 0 | 2 | 1 | 0 | 2 | 0 | 0 | 2 | 8 |
| G | 2 | 2 | 1 | 2 | 1 | 1 | 1 | 2 | 1 | 13 |
| H | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 16 |
| I | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 18 |
| J | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 18 |
| K | 2 | 1 | 2 | 0 | 0 | 2 | 1 | 0 | 2 | 10 |
| Totaal | 20 | 15 | 21 | 18 | 15 | 19 | 16 | 16 | 21 | |

| Individuele vraagscores | |
|---|---|
| 0 | Niet noodzakelijk |
| 1 | Nuttig maar niet essentieel |
| 2 | Essentieel |

**Somscore vragen**

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

**Somscore deelnemer**

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

## Bijlage VII Doorontwikkelde HAIS-Q

Onderstaande vindt u de doorontwikkelde HAIS-Q op basis van de documentstudie, gehouden interviews en enquêteresultaten. Ook is aangegeven welke contextinformatie is meegegeven bij de enquête voor de pilotgroep en de cognitieve test. Behouden items en teksten zijn groen gekleurd, aangepaste teksten zijn oranje gekleurd en toegevoegde items en teksten zijn rood gekleurd. Verwijderde subgebieden zijn onder het aandachtsgebied beschreven met reden van verwijdering. Daarnaast staat daar, voor zover nodig, toelichting voor mogelijke wijzigingen binnen subgebieden.

De enquête is voorafgegaan door een welkomsttekst en een drietal voorbeeldvragen, welke onderstaande zijn weergegeven.

| **Welkomsttekst** |
|---|
| Beste collega,<br><br>Informatiebeveiliging en privacy zijn in de zorg thema's die steeds vaker op de agenda staan en waar ook in het nieuws vaker aandacht aan wordt besteed. Denk bijvoorbeeld aan ransomware aanvallen of datalekken waar patiëntdossiers onterecht worden ingezien. Rode draad in veel van deze berichten is de rol van de medewerker, wat weet hij/zij en hoe acteert hij/zij in de dagelijkse praktijk, ofwel hoe informatiebeveiligingsbewust zijn medewerkers in de zorgsector.<br><br>Het informatiebeveiligingsbewustzijn van een medewerker wordt bepaald door de kennis van deze medewerker over beleid op het gebied van informatiebeveiliging en privacy, zijn/haar houding ten opzichte van dit beleid en uiteraard of hij/zij zich wel of niet aan het beleid conformeert in zijn/haar dagelijkse gedrag.<br><br>Deze enquête bevat stellingen over uw kennis, uw houding en uw gedragingen aangaande verschillende aandachtsgebieden van informatiebeveiliging en privacy.<br><br>De enquête is opgebouwd rondom de verschillende onderwerpen en aandachtsgebieden. Binnen elk aandachtsgebied wordt u 1 stelling aangaande uw kennis voorgelegd, gevolgd door 1 stelling aangaande uw houding en het aandachtsgebied wordt afgesloten door 1 stelling aangaande uw daadwerkelijke gedrag. Daarna worden u stellingen voorgelegd over een ander aandachtsgebied.<br><br>Per voorgelegde stelling wordt aan u gevraagd in hoeverre u het met een stelling (helemaal) eens of (helemaal) oneens bent. Indien u bij een kennisvraag niet weet wat het beleid is, geeft u aan wat u denkt dat het beleid is. **Er zijn geen goede of foute antwoorden, het is vooral belangrijk dat u waarheidsgetrouw antwoordt**.<br><br>Nadat alle aandachtsgebieden zijn doorlopen worden nog enkele algemene vragen aan u gesteld, waaronder uw functie en uw leeftijd. Deze vragen zijn optioneel van aard en dienen extra analyse doeleinden. Als laatste worden er wat vragen gesteld over de enquête zelf en is er ruimte voor het geven van feedback aangaande de enquête.<br><br>De enquête wordt anoniem afgenomen, waarbij het de verwachting is dat u 20 tot 30 minuten nodig zult hebben om alle stellingen te doorlopen.<br><br>Op voorhand dank voor uw medewerking!!<br><br>Petra Verbeek |

| **Voorbeeldstellingen** | | | |
|---|---|---|---|
| Autorijden en alcohol Hieronder vindt u 3 voorbeeldstellingen over het aandachtsgebied Autorijden en alcohol. De eerste stelling gaat over uw kennis (weet u wat de regel is), de tweede stelling gaat over uw houding (wat vindt u van de regel) en de derde stelling gaat over uw gedrag (volgt u de regel wel of niet). Alle aandachtsgebieden in deze enquête zijn vergelijkbaar opgebouwd, elk aandachtsgebied 3 stellingen. Er zijn daarbij geen foute of goede antwoorden, alleen eerlijke antwoorden. De stellingen kunnen erg op elkaar lijken omdat zij allen over hetzelfde aandachtsgebied gaan maar met een andere nuance. | | | |
| | **Kennis** | **Houding** | **Gedrag** |
| Voorbeeldstellingen | KENNIS: Als ik 3 biertjes op heb mag ik nog autorijden | HOUDING: Als ik 3 biertjes op heb kan ik nog autorijden | GEDRAG: Als ik 3 biertjes op heb ga ik nog autorijden |

| **Aandachtsgebied: Authenticatiemiddelen** | | | |
|---|---|---|---|
| Om toegang te krijgen tot applicaties met daarin gegevens, maar bijvoorbeeld ook tot ruimtes met middelen, moet je je als persoon authentiseren. Een zeer bekende manier van authenticatie is de combinatie van gebruikersnaam en wachtwoord, maar heden ten dage worden ook vaak andere middelen ingezet, zoals bijvoorbeeld een personeelspas of vingerafdruk. Weet u wat de regels zijn over omgang met deze middelen en wat vindt u daarvan? En nog belangrijker wat doet u in uw dagelijkse praktijk? Volgend vindt u voor 3 aandachtgebieden binnen het onderwerp 'authenticatiemiddelen' stellingen over uw kennis, uw houding en uw gedrag. Lees elke stelling goed door alvorens antwoord te geven. | | | |
| | **Kennis** | **Houding** | **Gedrag** |
| Gebruik van hetzelfde wachtwoord | Het is acceptabel om hetzelfde wachtwoord te gebruiken voor particuliere toepassingen als voor zakelijke toepassingen | Ik ervaar het als veilig om hetzelfde wachtwoord zowel privé als zakelijk te gebruiken | Ik gebruik dezelfde wachtwoorden voor particuliere toepassingen als voor zakelijke toepassingen |
| Delen van authenticatiemiddelen | Ik mag mijn wachtwoorden (of andere authenticatiemiddelen zoals pasje) delen met mijn collega's als dat nodig is voor het werk | Ik vind het een slecht idee om mijn wachtwoorden (of andere authenticatiemiddelen zoals pasje) te delen, zelfs als een collega erom vraagt | Ik heb wel eens een wachtwoord (of ander authenticatiemiddel zoals een pasje) met een collega gedeeld |
| Registratie van wachtwoorden | Ik mag geen wachtwoorden registreren tenzij dit op een veilige wijze kan, zoals in een wachtwoordenkluis | Ik ben van mening dat ik mijn wachtwoorden veilig kan registreren, ook zonder het gebruik van een wachtwoordenkluis | Ik registreer mijn wachtwoorden alleen in een wachtwoordenkluis en niet op een andere wijze (papier, computerbestand, telefoon etc.) |

Het subgebied ‘Gebruik van een sterk wachtwoord’ is technisch goed af te dwingen, waardoor dit onderwerp minder relevant is. Dit is ook teruggekomen uit de enquêtes. Zodoende is er vergelijkbaar met het onderzoek van Schaeken (2018) gekozen om een ander onderwerp op te nemen, te weten registratie van wachtwoorden, zoals in het beleid is aangegeven.

| **Aandachtsgebied: Email gebruik** | | | |
|---|---|---|---|
| Email als communicatiemiddel wordt veelvuldig door medewerkers gebruikt binnen en buiten de organisatie. Het is een snelle en makkelijke manier om vragen te stellen, opdrachten uit te zetten of mensen te informeren. Ook is het een laagdrempelige wijze om contacten te leggen met nog onbekende personen. Een gemiddelde medewerker ontvangt al gauw 10 tot 30 mails op een dag, sommige medewerkers nog vele malen meer. Deze mails kunnen links naar interessante websites of elders opgeslagen informatie bevatten. Daarnaast worden er ook talrijke bestanden heen en weer gestuurd via de mail om verschillende redenen, variërend van plaatjes en filmpjes tot allerlei office bestanden. Bent u zich bewust van de regels die uw organisatie op dit onderwerp hanteert en zo ja, bent u het daar dan mee eens? En wat doet u in de praktijk? Volgend vindt u voor 3 aandachtgebieden binnen het onderwerp 'eMail gebruik' stellingen over uw kennis, uw houding en uw gedrag. Lees elke stelling goed door alvorens antwoord te geven. | | | |
| | **Kennis** | **Houding** | **Gedrag** |
| eMails van bekende afzenders | Instructies, bijlages en links in mails van bekende afzenders mag ik altijd opvolgen, openen of op klikken | Ik denk dat het altijd veilig is om bijlages te openen, op links te klikken of instructies op te volgen als deze staan in een mail van een bekende afzender | Als ik in een mail van een bekende afzender instructies, bijlages of links krijg, open ik deze altijd |
| Klikken op links in e-mails van ONbekende afzenders | Ik mag niet op een link in een e-mail van een onbekende afzender klikken | Er kan niets slechts gebeuren als ik op een link in een e-mail van een onbekende afzender klik | Als een e-mail van een onbekende afzender interessant lijkt, klik ik op een link in de e-mail |
| Openen van bijlagen in e-mails van onbekende afzenders | Ik mag e-mailbijlagen van onbekende afzenders openen | Het is riskant om een e-mailbijlage van een onbekende afzender te openen | Ik open geen e-mailbijlagen als de afzender mij onbekend is |

Vanwege de opkomst van spearfishing mails naast fishing mails, is het subgebied ‘eMails van bekende afzenders’ uitgebreid met het onderdeel instructies. Binnen de case-organisatie is dit al regelmatig voorgekomen. De onderzoeker heeft een eMail gehad, zogenaamd van de voorzitter van de Raad van Bestuur, om geld over te maken.

| **Aandachtsgebied: Internetgebruik** | | | |
|---|---|---|---|
| Vandaag de dag kunnen we ons geen wereld meer voorstellen zonder internet. Als we iets willen kopen of informatie over een onderwerp zoeken gaan we even 'googelen'. Alles kun je vinden op het internet en daarmee is dat een rijke bron aan informatie. Volgend vindt u voor 3 aandachtgebieden binnen het onderwerp 'internetgebruik' stellingen over uw kennis, uw houding en uw gedrag. Lees elke stelling goed door alvorens antwoord te geven. | | | |
| | **Kennis** | **Houding** | **Gedrag** |
| Downloaden van bestanden | Ik mag alle soorten bestanden naar mijn werkcomputer downloaden als ze me helpen om mijn werk te doen | Het kan riskant zijn om bestanden op mijn werkcomputer te downloaden | Ik download alle bestanden op mijn werkcomputer die me zullen helpen om de klus te klaren |

| | Kennis | Houding | Gedrag |
|---|---|---|---|
| Benaderen van dubieuze websites | Terwijl ik aan het werk ben, moet ik bepaalde websites niet bezoeken | Ook al heb ik toegang tot een website op het werk, betekent dat niet dat het een veilige website is | Als ik op het werk toegang heb tot het internet, bezoek ik elke website die ik wil bezoeken, zowel voor werk als privé doeleinden |
| Informatie online invoeren | Ik mag alle informatie op een website invoeren als dat me helpt bij het uitvoeren van mijn werk | Als het me helpt om mijn werk te doen, maakt het niet uit welke informatie ik op een website zet | Ik beoordeel de veiligheid van websites en het soort informatie dat gevraagd wordt in te voeren, alvorens deze informatie in te voeren |

**Aandachtsgebied: Sociale media gebruik**

Het aangaan en onderhouden van contacten gaat heel makkelijk met behulp van allerlei social media sites zoals Facebook, Twitter, LinkedIn, Instagram, Google+, YouTube, etc. Via deze kanalen is het ook heel makkelijk om informatie over mensen te vinden, hoe staan ze in het leven, wat doen ze zoal en wie kennen ze. De meeste mensen die op social media zitten vinden het ook leuk of fijn om op deze laagdrempelige wijze zaken te delen, zowel privé als zakelijk. Het aantal connecties dat iemand heeft kan zelfs veel aanzien wekken. Volgend vindt u voor 3 aandachtgebieden binnen het onderwerp 'sociale media gebruik' stellingen over uw kennis, uw houding en uw gedrag. Lees elke stelling goed door alvorens antwoord te geven.

| | Kennis | Houding | Gedrag |
|---|---|---|---|
| Accepteren van vriendverzoeken | Het is acceptabel om op sociale netwerk sites alle vriendschapsverzoeken te accepteren | Ik denk dat het weinig kwaad kan om alle vriendschapsverzoeken op sociale netwerk sites te accepteren | Ik accepteer alle vriendschapsverzoeken op sociale netwerk sites |
| *Rekening houden met gevolgen* | *Ik kan niet ontslagen worden voor iets wat ik op sociale media plaats* | *Op sociale media kan ik ook zaken plaatsen die ik normaal gesproken niet in het openbaar zou zeggen* | *Ik plaats niets op sociale media voordat ik nadenk over eventuele (negatieve) gevolgen voor mijzelf en anderen* |
| *Plaatsen van informatie over werk* | *Ik kan posten wat ik wil over mijn werk op sociale media* | *Het is riskant om bepaalde informatie over mijn werk op sociale media te plaatsen* | *Ik plaats alles wat ik wil over mijn werk op sociale media* |

Het subgebied ‘Sociale media privacy instellingen’ is vanwege de lage relevantie op alle dimensies in navolging op het onderzoek van Schaeken (2018) vervangen door het subgebied ‘Accepteren van vriendverzoeken’, mede omdat dit relevant is bij Social Engineering wat meer dan eens is genoemd in de interviews als missend aandachtsgebied.

**Aandachtsgebied: Mobiele apparaten**

Laptops zijn al langere tijd beschikbaar en worden in het werk ook steeds meer gangbaar. Met de komst van tablets en smartphones en de daarbij behorende apps heeft het mobiele werken een vogelvlucht genomen. Er is bijna geen medewerker meer die niet op één of andere manier gebruik maakt van een mobiel apparaat voor zijn of haar werk. Heel gemakkelijk, maar is het ook altijd veilig? Volgend vindt u voor 3 aandachtgebieden binnen het onderwerp 'mobiele apparaten' stellingen over uw kennis, uw houding en uw gedrag. Lees elke stelling goed door alvorens antwoord te geven.

| | Kennis | Houding | Gedrag |
|---|---|---|---|
| Fysieke beveiliging van mobiele apparaten | Als ik in een openbare ruimte werk, moet ik mijn mobiele apparatuur altijd bij me houden | Als ik in een café werk, kan ik mijn laptop en/of telefoon op tafel laten liggen terwijl ik een drankje ga halen | Als ik in een openbare ruimte werk, laat ik mijn laptop en/of mobiele telefoon nooit op mijn werkplek achter als ik naar het toilet ga |
| Versturen van gevoelige informatie via wifi | Ik mag gevoelige werkbestanden of mails versturen via een openbaar Wi-Fi-netwerk | Het is riskant om gevoelige werkbestanden of mails te versturen via een openbaar Wi-Fi-netwerk | Ik verstuur soms gevoelige werkbestanden of mails via een openbaar Wi-Fi-netwerk |
| Over de schouder meekijken | Als ik aan een gevoelig document werk, moet ik ervoor zorgen dat onbevoegden niet op mijn laptopscherm kunnen meekijken | Het is riskant om gevoelige werkbestanden of mails op een laptop te openen als onbevoegden op mijn scherm kunnen meekijken | Ik controleer of onbevoegden niet op mijn laptop scherm kunnen meekijken als ik aan een gevoelig document werk |

Binnen dit aandachtsgebied zijn enkele aanpassingen in de vragen gedaan voor een beter begrip.

**Aandachtsgebied: Informatieverwerking**

Informatie is overal, zowel digitaal als op papier. Afhankelijk van het soort informatie is het meer of minder belangrijk hoe zorgvuldig iemand hier mee om gaat. Meestal kunnen we ons daar ook wel een voorstelling van maken, maar gaan we daar dan ook op die manier mee om? Volgend vindt u voor 3 aandachtgebieden binnen het onderwerp 'informatieverwering' stellingen over uw kennis, uw houding en uw gedrag. Lees elke stelling goed door alvorens antwoord te geven.

| | Kennis | Houding | Gedrag |
|---|---|---|---|
| Het weggooien van gevoelige afdrukken | Afdrukken met gevoelige informatie mogen op dezelfde wijze worden weggegooid als afdrukken zonder gevoelige informatie | Het weggooien van gevoelige afdrukken door ze in de prullenbak te gooien is veilig | Ik maak onderscheid in het weggooien van afdrukken met en zonder gevoelige informatie |
| Het plaatsen van verwijderbare media | Als ik een USB-stick op een openbare plaats vind, moet ik hem niet op mijn privé of werkcomputer aansluiten | Als ik een USB-stick op een openbare plaats vind, kan er niets ergs gebeuren als ik hem op mijn privé of werkcomputer aansluit | Ik zou een USB-stick die ik op een openbare plaats heb gevonden niet in mijn privé of werkcomputer steken |
| Clear screen / clean desk | Het is toegestaan mijn scherm niet te vergrendelen en gevoelige informatie achter te laten als ik mijn werkplek verlaat | Ik vind het riskant om gevoelige informatie, papier of digitaal, op mijn werkplek achter te laten als ik afwezig ben | Het komt voor dat ik bij het verlaten van mijn werkplek mijn scherm niet vergrendel of gevoelige informatie op mijn werkplek laat liggen |

Binnen het subgebied ‘Het weggooien van gevoelige afdrukken’ is wat tekstnuance toegepast voor betere duiding van begrippen. Daarnaast is het subgebied ‘Achterlaten van gevoelige informatie’ uitgebreid zodat ook het open laten staan van het scherm hieronder te scharen valt. Daarnaast is een gezondheidsorganisatie over het algemeen een continu bedrijf, wat maakt dat er geen onderscheid is tussen nacht en dag.

**Aandachtsgebied: Melden van incidenten**

Op allerlei gebied kunnen zich incidenten voordoen, zo ook op het gebied van informatiebeveiliging en privacy. Dit onderdeel gaat over het melden van incidenten en/of het aanspreken van collega's op gedrag. Weet jij wat je wel of niet moet melden en wanneer dat van je wordt verwacht? Vindt jij het jouw verantwoordelijkheid om dit te doen en zo ja, hoe doe je dat in de werkelijkheid? Volgend vindt u voor 3 aandachtgebieden binnen het onderwerp 'melden van incidenten' stellingen over uw kennis, uw houding en uw gedrag. Lees elke stelling goed door alvorens antwoord te geven.

| | Kennis | Houding | Gedrag |
|---|---|---|---|
| Melden van verdacht gedrag | *Als ik iemand zich verdacht zie gedragen op mijn werkplek, moet ik dat melden* | *Ik denk niet dat er iets ergs zal gebeuren als ik iemand negeer die verdacht handelt op mijn werk* | *Als ik iemand verdacht zou zien handelen op mijn werkplek, zou ik er iets aan doen (melden of aanspreken)* |
| Negeren van slecht veiligheidsgedrag van collega's | *Ik mag niet voorbijgaan aan het slechte veiligheidsgedrag van mijn collega's* | Ik vind het niet mijn verantwoordelijkheid om collega’s aan te spreken als zij slecht veiligheidsgedrag vertonen | *Als ik merk dat mijn collega de veiligheidsregels negeert, attendeer ik hem/haar daar op* |
| Melden van alle incidenten | *Het is optioneel om beveiligingsincidenten (incl. datalekken) te melden* | *Het melden van beveiligingsincidenten (incl. datalekken) helpt om de informatieveiligheid te verhogen* | *Als ik een beveiligingsincident zou opmerken, zou ik het melden* |

Binnen het aandachtsgebied ‘Melden van incidenten’ heeft vooral veel tekstnuancering plaatsgevonden, opdat de vragen beter begrepen worden. Ten aanzien van het subgebied ‘Negeren van slecht veiligheidsgedrag van collega’s’ is gedurende de interviews aangegeven dat de verwachting bestaat dat de medewerkers het aanspreken van collega’s niet ziet als hun verantwoordelijkheid, maar als de verantwoordelijkheid van de leidinggevende. Ook is de gedragsvraag omgedraaid van een negatieve naar een positieve vraag en is de term ‘actie’ verder geduid. Bij het subgebied ‘Melden van alle incidenten’ is de term datalekken toegevoegd omdat dit een herkenbaar en veel voorkomend incident is binnen de gezondheidszorg.

**Omgang met privacygevoelige informatie**

Privacy is een HOT onderwerp, dit geldt binnen de gezondheidszorg uiteraard voor onze patiënten maar daarnaast ook voor onze medewerkers. Privacygevoelige gegevens worden geadministreerd binnen daarvoor ontworpen systemen zoals een EPD of een personeelssysteem. De toegang daartoe is over het algemeen goed gereguleerd op basis van 'need to know' principes. Echter, privacygevoelige informatie zit ook in de medewerkers en soms hebben medewerkers meer toegang binnen systemen dan zij sec nodig hebben om hun werk te doen. Wat mag en kan nu wel en hoe gaan wij daar in de praktijk mee om? Volgend vindt u voor 3 aandachtgebieden binnen het onderwerp 'omgang met privacygevoelige informatie' stellingen over uw kennis, uw houding en uw gedrag. Lees elke stelling goed door alvorens antwoord te geven.

| | Kennis | Houding | Gedrag |
|---|---|---|---|
| Privacy gevoelige gegevensverzamelingen buiten de applicaties | Voordat ik een eigen privacygevoelige gegevensverzameling voor studie/werk/onderzoek aanleg, | Het kan geen kwaad om een privacygevoelige gegevensverzameling voor mijn werk/studie/onderzoek aan te | Voor mijn studie/werk/onderzoek haal ik soms privacygevoelige gegevens uit een applicatie en sla |

| | | | |
|---|---|---|---|
| | moet ik dit laten toetsen door de privacy officer | leggen op een locatie buiten de applicatie of op mijn privé computer | deze op buiten de applicatie of op mijn privé computer |
| Afdrukken van privacy gevoelige informatie | Het is niet acceptabel om privacygevoelige informatie af te drukken als ik dat ook digitaal kan raadplegen | Voor mijn werk vind ik het makkelijker om privacygevoelige informatie af te drukken i.p.v. gebruik te maken van de computer | Ik druk nooit privacygevoelige informatie af |
| In publieke gelegenheden praten over patiënten en/of medewerkers | Ik mag in een publieke ruimte praten over patiënten of medewerkers zolang ik dat anoniem doe | Ik vind het geen goed idee om in een publieke ruimte over patiënten of medewerkers, ook niet als dat anoniem is | Als ik over patiënten of medewerkers praat, let ik op waar ik ben en doe ik dat altijd anoniem |
| Inzien van persoonsgegevens van patiënten en/of medewerkers | Ik mag alleen persoonsgegevens van patiënten en/of medewerkers raadplegen als dat voor mijn werk noodzakelijk is | Ik heb een geheimhoudingsplicht dus ik mag persoonsgegevens van iedereen raadplegen ook al is dat niet nodig voor mijn werk | Ik bekijk alleen gegevens van patiënten of medewerkers wanneer dat nodig is om mijn werk te kunnen doen |