Hoe iBewust zijn medewerkers van Nederlandse gemeenten?

Een methodiek om kennis, houding en gedrag op het gebied van informatiebeveiliging bij medewerkers van Nederlandse gemeenten te meten

Auteur	Youri Lammerts van Bueren
Studentnummer	851447002
Presentatiedatum	19 november 2015

What is the information security awareness of employees of Dutch municipalities?

A methodology for measuring knowledge, attitude and behavior in the field of information security among employees of Dutch municipalities

Auteur	Youri Lammerts van Bueren
Studentnummer	851447002
Presentatiedatum	19 november 2015
Masteropleiding	Business Process Management & IT
Faculteit	Management, Science & Technology
Instelling	Open Universiteit
Cursuscode	T9232B
Begeleidingscommissie	
Afstudeerbegeleider	dr. ir. Harald Vranken
2e begeleider/lezer	dr. ir. Arjan Kok
Examinator	dr. ir. Harald Vranken

Inhoudsopgave

Samenvatting

Informatie is een belangrijke kapitaalfactor van een organisatie. Medewerkers spelen een cruciale rol in het beschermen van deze informatie. In hoeverre zij het gewenste gedrag hierbij vertonen hangt in belangrijke mate af van hun informatiebeveiligingsbewustzijn. Er is momenteel een beperkt aantal methodieken voorhanden waarmee het informatiebeveiligingsbewustzijn gemeten kan worden. Uit een onderzoek bij een Zweedse overheidsinstelling blijkt dat medewerkers ander (ongewenst) gedrag vertonen terwijl zij kennis hebben van het gedrag van hen verlangd wordt. De vraag die opdoemt is of die onderzoekresultaten representatief zijn voor de Nederlandse overheid en specifiek voor Nederlandse gemeenten. Op 29 november 2013 is namelijk tijdens de Buitengewone Algemene Ledenvergadering van de Vereniging voor Nederlandse Gemeenten (VNG) besloten dat gemeenten structureel aan het informatiebeveiligingsbewustzijn moeten werken. In de praktijk speelt dan de vraag op welke wijze het informatiebeveiligingsbewustzijn kan worden gemeten om hierop te sturen.

Om dit te onderzoeken is de eerste stap het bepalen op welke wijze het informatiebeveiligingsbewustzijn kan worden gemeten bij medewerkers van Nederlandse gemeenten. De probleemstelling van dit onderzoek was:

> *Op welke wijze kan het informatiebeveiligingsbewustzijn van medewerkers bij Nederlandse gemeenten en bijbehorend gedrag worden gemeten met een gevalideerde methodiek?*

Dit met als doel om te komen tot een methodiek die correct, volledig en effectief is.

De opzet van het onderzoek bestond uit een literatuuronderzoek gevolgd door een empirisch onderzoek. In de fase van het literatuuronderzoek was het doel om te komen tot een referentiemodel waarmee het informatiebeveiligingsbewustzijn kon worden gemeten. Tijdens deze onderzoeksfase stonden drie deelvragen centraal:

1. Welke methoden zijn beschikbaar voor het meten van het informatiebeveiligingsbewustzijn en bijbehorend gedrag?
2. Welk informatiebeveiligingsbeleid en welke informatiebeveiligingsnormen vormen de inhoudelijke uitgangspunten voor de methode om het informatiebeveiligingsbewustzijn en bijbehorend gedrag te meten bij medewerkers van Nederlandse gemeenten?
3. Welke onderzoeken met welke onderzoeksresultaten zijn er bij Nederlandse gemeenten gedaan op het gebied van het informatiebeveiligingsbewustzijn en naleving van het informatiebeveiligingsbeleid?

De literatuurstudie leverde, conform onderzoeksdoel, een referentiemodel. Dit model is gebaseerd op het model van Kruger en Kearney (2006). Het meet inhoudelijk de 10 belangrijkste gedragsrisico's op basis van de 10 gouden regels uit de campagne iBewustzijn Overheid (2014b). Met dit model is het mogelijk om het informatiebeveiligingsbewustzijn (kennis, houding en gedrag) te meten bij medewerkers van Nederlandse gemeenten.

Het resultaat uit de literatuurstudie maakte het noodzakelijk om de probleemstelling aan te scherpen ten behoeve van het empirisch onderzoek. Hierdoor kwam de focus vervolgens kwam te liggen op de validatie van het referentiemodel. De probleemstelling werd:

In hoeverre is de ontwikkelde methodiek uit de literatuurstudie, waarmee het informatiebeveiligingsbewustzijn en bijbehorend gedrag van medewerkers bij Nederlandse gemeenten kan worden gemeten, correct, volledig én effectief?

De deelvragen die centraal stonden in de empirische onderzoeksfase waren:

1. In hoeverre is de ontwikkelde methodiek volledig, waarbij het de 10 belangrijkste gedragsrisico's meet?
2. In hoeverre is de ontwikkelde methodiek correct opgezet?
3. In hoeverre is de ontwikkelde methodiek effectief, waarbij rekening wordt gehouden met de aspecten haalbaarheid, begrijpelijkheid en bruikbaarheid?

Voor de eerste twee onderzoeksvragen zijn vier semi-gestructureerde interviews gehouden met deskundigen op het vlak van informatiebeveiliging binnen de Nederlandse overheid c.q. gemeenten. Hierbij is gesproken met:

- een afvaardiging van de Informatiebeveiligingsdienst voor gemeenten (IBD);
- de voorzitter van de domeingroep awareness van het Centrum Informatiebeveiliging en Privacybescherming (CIP-overheid);
- met betrokkenen die de campagne iBewustzijn Overheid hebben opgezet;
- de CISO van de gemeente Edam-Volendam.

Om te onderzoeken in hoeverre de methodiek effectief is, is de methodiek op beperkte schaal toegepast door middel van een survey. Dit is gedaan bij een negental medewerkers van drie kleine tot middelgrote gemeenten. Deze negental medewerkers, die geen specifieke IT-kennis hadden, vormden een dwarsdoorsnee van een Nederlandse gemeente. De survey meette het gedrag van medewerkers, waarbij het ging om gedrag zonder kwaadwillende intenties. Dit gedrag laat zich namelijk goed meten door middel van een survey.

Ten aanzien van de volledigheid is geconstateerd dat de belangrijkste gedragsrisico's afgeleid konden worden uit een vijftal belangrijke ontwikkelingen: tijd- en plaatsonafhankelijk werken, samenwerken met andere organisaties, digitalisering, open databehandeling en een mogelijk perceptieverschil tussen generaties inzake de informatiebeveiliging.
Vanuit deze ontwikkelingen zijn de belangrijkste gedragsrisico's bepaald, die in grote lijn overeen kwamen met de gedragsrisico's die waren opgenomen in het referentiemodel en aan de deskundigen waren voorgelegd ter validatie. Bij het meten van het informatiebeveiligingsbewustzijn is het raadzaam om gegevens vast te leggen van medewerkers omtrent functie, leeftijd, loonklasse en dergelijke. Hiermee kan het informatiebeveiligingsbewustzijn vanuit verschillende invalshoeken worden geanalyseerd.

Met betrekking tot de correctheid is geconstateerd dat de gedragsrisico's van toepassing zijn op medewerkers van Nederlandse gemeenten. Op basis van de interviews met deskundigen is het model qua opbouw aangepast waarbij de gedragsrisico's worden afgeleid uit de risico's van de organisatie. Deze opbouw bevordert de interne validiteit van het model, waardoor inzichtelijk wordt of het model meet wat het beoogt te meten. De surveyvragen die vervolgens per gedragsrisico het informatiebeveiligingsbewustzijn meten, moeten hierbij gericht zijn op de dimensies kennis, houding én gedrag. De kennisvragen meten hierbij of medewerkers weten wat van hen verwacht wordt en wat de gevolgen zijn als zij ander gedrag vertonen. De surveyvragen dienen gesloten vragen

te zijn met een meerpuntsschaal om het informatiebeveiligingsbewustzijn te kunnen kwantificeren.

Het onderzoek inzake de effectiviteit van de methodiek leverde kaders op voor het opstellen van een survey. Deze kaders lijken de begrijpelijkheid en haalbaarheid van de voorgelegde survey positief te beïnvloeden. Dit is relevant voor de betrouwbaarheid van de antwoorden die medewerkers geven op de surveyvragen.

Het onderzoek heeft antwoord gegeven op de centrale onderzoeksvraag. Het heeft geleid tot een model waarbij het model van Kruger en Kearney (2006) is uitgebreid en verrijkt met kaders. Hierdoor kan het informatiebeveiligingsbewustzijn worden gemeten bij medewerkers van Nederlandse gemeten. Deze methodiek is dusdanig ontwikkeld dat het flexibel (herbruikbaar) en niet statisch van aard is. Deze flexibiliteit houdt in dat de methodiek eenvoudig aangepast kan worden. De opzet van de methodiek houdt rekening met concrete specifieke organisatie-eigenschappen alsmede veranderende (c.q. andere) gedragsrisico's in verband met nieuwe (IT-)ontwikkelingen over de tijd heen. Deze flexibiliteit draagt er aan bij dat het model ook gebruikt kan worden door andere (overheids)organisaties dan alleen Nederlandse gemeenten.

1. Inleiding

Informatie(middelen) vormen de 'lifeblood' van een organisatie. Daarom is het belangrijk om deze te beschermen (Kruger, Drevin, & Steyn, 2006). Dit gebeurt door het treffen van maatregelen. Organisaties focussen zich hierbij hoofdzakelijk op organisatorische (beleidsmatige) en technische maatregelen. Hierbij hebben zij minder aandacht voor de menselijke factor, terwijl menselijk gedrag als cruciale factor wordt beschouwd voor de effectiviteit van het informatiebeveiligingsbeleid (Kruger et al., 2006; Aytes & Conolly, 2003; Dodge Jr., Carver, & Ferguson, 2007; Hagen, Albrechtsen, & Hovden, 2008; Siponen & Karjalainen, 2011).

Het niet naleven van het informatiebeveiligingsbeleid en bijbehorende procedures door medewerkers is een grote zorg voor elke organisatie (Siponen & Karjalainen, 2011). Hoe effectief de getroffen informatiebeveiligingsmaatregelen zijn, hangt af van of een ieder het gedrag vertoont en begrijpt wat van hem verwacht wordt (Kruger & Kearney, 2006). Het vertonen van gedrag dat in strijd is met het beleid kan leiden tot informatiebeveiligingsincidenten. Door een reeks van informatiebeveiligingsincidenten bij Nederlandse overheden, waaronder de DigiNotar-crisis in 2011, is de Nederlandse politiek in beweging gebracht om op dit vlak in te grijpen. Op landelijk niveau is daardoor veel aandacht ontstaan voor de informatiebeveiliging bij de Nederlandse overheid en expliciet voor Nederlandse gemeenten. Dit heeft ertoe geleid dat op 29 november 2013 tijdens de Buitengewone Algemene Ledenvergadering van de Vereniging van Nederlandse Gemeenten (VNG) de resolutie "Informatieveiligheid, randvoorwaarde voor de professionele gemeente" is aangenomen (VNG, 2013a). Deze resolutie geeft aan hoe Nederlandse gemeenten het onderwerp informatiebeveiliging moeten vormgeven. Onderdeel hiervan is dat er structureel gewerkt moet worden aan het informatiebeveiligingsbewustzijn bij medewerkers.

Dat de medewerker een belangrijke factor is ten aanzien van de informatiebeveiliging bij Nederlandse gemeenten wordt bevestigd in het onderzoek van Van der Goes (2012). In zijn onderzoek geeft hij aan dat het informatiebeveiligingsniveau tegen social engineering laag is bij Limburgse gemeenten. Van der Goes geeft aan dat uit zijn literatuuronderzoek blijkt dat maatregelen als bewustzijn, scholing en training hiertegen het effectiefst zijn. Vergelijkbare resultaten kwamen ook uit eerder onderzoek bij een grote Zweedse overheidsinstelling (Koroliov, Turesson, & Brolin, 2009). Deze onderzoekers verklaarden ongewenst gedrag van medewerkers door ineffectieve ontwerpen van security systemen, menselijke beperkingen zoals het geheugen[1], gebrek aan training en scholing en een te laag informatiebeveiligingsbewustzijn. Zij concludeerden daarnaast dat ondanks dat medewerkers bepaalde kennis hadden van informatiebeveiligingsmaatregelen, deze toch niet altijd werden nageleefd. Zij bevolen voor vervolgonderzoek aan om deze discrepantie tussen het kennisniveau en het bijbehorende gedrag te onderzoeken en te verklaren.

Om dit te kunnen onderzoeken dient eerst het informatiebeveiligingsbewustzijn gemeten te worden. Er zijn echter weinig methodieken beschikbaar om het informatiebeveiligings-bewustzijn te meten (Siponen, 2001; Kruger & Kearney, 2006; Koroliov, Turesson, & Brolin, 2009). Daarbij is er géén specifieke methodiek voorhanden om het informatiebeveiligingsbewustzijn bij medewerkers van Nederlandse gemeenten te meten. Ondanks dat de Taskforce Bestuur en Informatieveiligheid Dienstverlening (BID) en het

1 Een complex wachtwoord is moeilijk te onthouden

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) de campagne iBewustzijn Overheid hebben opgezet. Deze campagne heeft als doel om het bewustzijn te stimuleren omtrent informatiebeveiliging bij medewerkers van de Nederlandse overheid, waaronder dus gemeenten. Medewerkers dienen uiteindelijk onbewust bekwaam om te gaan met informatie (Taskforce_BID & Ministerie_BZK, 2014).

Het doel van dit afstudeeronderzoek is om een methodiek te ontwerpen waarmee het informatiebeveiligingsbewustzijn bij medewerkers van Nederlandse gemeenten kan worden gemeten. Dit onderzoek dient in een breder kader geplaatst te worden en heeft een hoger gelegen doel. Dit instrument kan namelijk vervolgens gebruikt worden om de discrepantie in kaart te brengen tussen het informatiebeveiligingsbewustzijnniveau en het feitelijke gedrag dat wordt vertoond door medewerkers (theoretische relevantie). Door dit te doorgronden, is het mogelijk om het informatiebeveiligingsbeleid verder te optimaliseren en informatiebeveiliging succesvol te verankeren in de organisatie. Indien medewerkers namelijk ander gedrag vertonen waardoor technische en organisatorische maatregelen worden omzeild, dan is dit een aanknopingspunt om de effectiviteit van die maatregelen te evalueren. Bij deze evaluatie wordt dan gekeken op welke wijze maatregelen effectief worden ingezet. Hierbij wordt enerzijds gekeken naar de werkbaarheid van de maatregelen en anderzijds naar de wijze waarop de informatie(middelen) effectief worden beschermd vanuit informatiebeveiligingsoogpunt. Hierdoor is het voor gemeenten mogelijk om ‘in control’ te raken op het gebied van informatiebeveiliging (praktische relevantie).

1.1. Onderzoeksdoelstelling

In de inleiding zijn de context, het onderzoeksthema, het topic en de relevantie uitvoerig beschreven, waarbij is aangegeven dat dit onderzoek in een breder kader geplaatst dient te worden. Het concrete doel van dit onderzoek is:

> *Het komen tot een gevalideerde methodiek om het informatiebeveiligingsbewustzijn en bijbehorend gedrag van medewerkers bij Nederlandse gemeenten te kunnen meten.*

Het valideren houdt in dat de methodiek correct, volledig én effectief is. In bijlage 1 zijn begrippen en definities geoperationaliseerd. Hierin is ook het begrip methodiek en model gedefinieerd, die in dit verslag beide met regelmaat worden aangehaald. Een methodiek dient hierbij gezien te worden als een richtlijn tot de oplossing, wat gefaciliteerd wordt door een instrument (in casu een model).

1.2. Probleemstelling

Bij de start van het onderzoek stond de volgende probleemstelling centraal:

> *Op welke wijze kan het informatiebeveiligingsbewustzijn van medewerkers bij Nederlandse gemeenten en bijbehorend gedrag worden gemeten met een gevalideerde methodiek?*

Tijdens de literatuurstudie is onderzocht op welke wijze het informatiebeveiligings-bewustzijn kon worden gemeten en welke methodieken hiervoor beschikbaar zijn. Het resultaat van de literatuurstudie leidde tot een referentiemodel waarmee het informatiebeveiligingsbewustzijn en bijbehorend gedrag van medewerkers bij Nederlandse gemeenten kan worden gemeten. Aansluitend is tijdens het empirische onderzoek deze methodiek onderzocht ter validatie. De probleemstelling van het empirisch onderzoek was:

In hoeverre is de ontwikkelde methodiek uit de literatuurstudie, waarmee het informatiebeveiligingsbewustzijn en bijbehorend gedrag van medewerkers bij Nederlandse gemeenten kan worden gemeten, correct, volledig én effectief?

1.3. Onderzoeksvragen

De onderstaande onderzoeksvragen stonden centraal tijdens de literatuurstudie:

1. Welke methoden zijn beschikbaar voor het meten van informatiebeveiligings-bewustzijn en bijbehorend gedrag?
2. Welk informatiebeveiligingsbeleid en welke informatiebeveiligingsnormen vormen de inhoudelijke uitgangspunten voor de methode om het informatiebeveiligings-bewustzijn en bijbehorend gedrag te meten bij medewerkers van Nederlandse gemeenten?
3. Welke onderzoeken met welke onderzoeksresultaten zijn er bij Nederlandse gemeenten gedaan op het gebied van het informatiebeveiligingsbewustzijn en naleving van het informatiebeveiligingsbeleid?

Na de literatuurstudie volgde het empirisch onderzoek. Tijdens de empirische onderzoeksfase stonden de volgende drie onderzoeksvragen centraal, die gericht waren op het valideren van de ontwikkelde methodiek die het resultaat was van de literatuurstudie:

1. In hoeverre is de ontwikkelde methodiek volledig, waarbij het de 10 belangrijkste gedragsrisico's meet?
2. In hoeverre is de ontwikkelde methodiek correct opgezet?
3. In hoeverre is de ontwikkelde methodiek effectief, waarbij rekening wordt gehouden met de aspecten haalbaarheid, begrijpelijkheid en bruikbaarheid?

1.4. Organisaties ten behoeve van het empirisch onderzoek

Het empirisch onderzoek is in twee fasen uitgevoerd. In de eerste fase zijn deskundigen geïnterviewd die werkzaam zijn binnen het vakgebied van informatiebeveiliging bij overheden (en gemeenten specifiek). Hierbij is het model inhoudelijk gevalideerd. Hiervoor zijn interviews gehouden met:

- de voorzitter van de domeingroep 'Awareness' bij het CIP-overheid (Centrum voor informatiebeveiliging en privacy);
- een afvaardiging van de IBD (Informatiebeveiligingsdienst voor gemeenten);
- de Chief Information Security Officer (CISO) van de gemeente Edam-Volendam
- personen die betrokken waren het opzetten van de campagne iBewustzijn Overheid.

In de tweede fase van het empirisch onderzoek is de methodiek op beperkte schaal in de praktijk getoetst bij een negental medewerkers. Tezamen vormen zij een dwarsdoorsnede van een gemeentelijke organisatie. Deze negen medewerkers zijn werkzaam bij de gemeente Culemborg, Geldermalsen of Tiel. Deze drie gemeenten zijn geografisch gevestigd ten zuiden van de gemeente Utrecht in de omgeving West-Betuwe. Deze drie gemeenten werken in diverse verbanden met elkaar samen en hebben op 9 juli 2015 gezamenlijk een gemeenschappelijke regeling opgericht waarin zij hun bedrijfsvoeringstaken hebben ondergebracht. De gemeente Culemborg en Geldermalsen hebben respectievelijk iets meer dan 27.000 en 26.000 inwoners. De gemeente Tiel heeft omstreeks 41.000 inwoners. Op 1 januari 2015 telde Nederland in totaal 393 gemeenten.

1.5. Leeswijzer

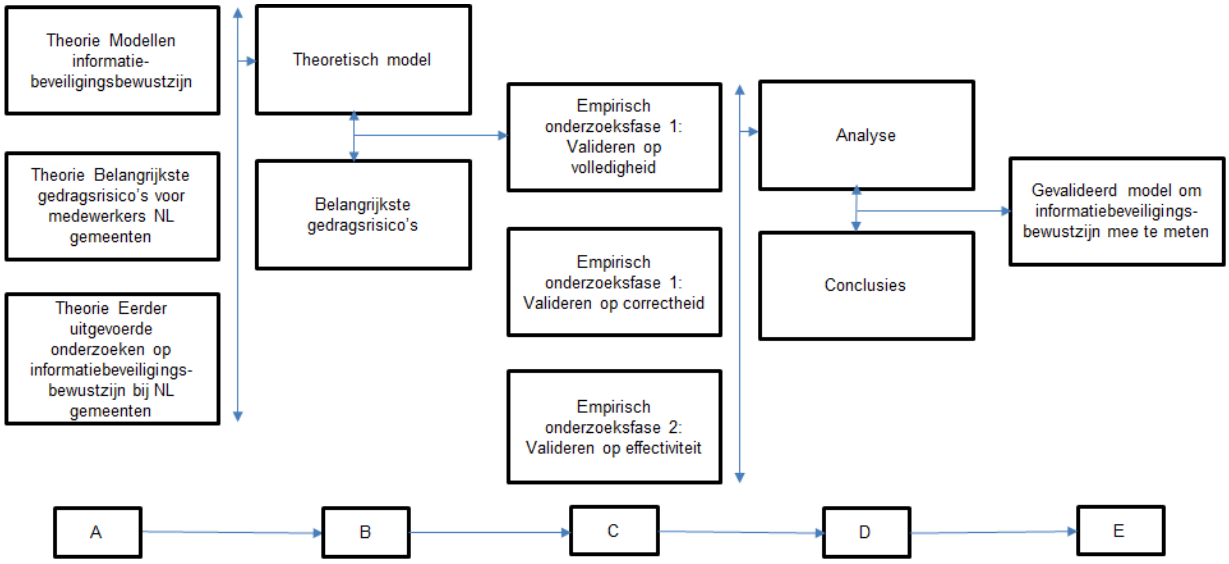
Hoofdstuk 2 beschrijft de onderzoeksaanpak voor de literatuurstudie en het empirisch onderzoek dat uit twee fasen bestaat. De resultaten van de literatuurstudie staan in hoofdstuk 3 en die van het empirisch onderzoek in hoofdstuk 4. De conclusies en aanbevelingen naar aanleiding van het empirisch onderzoek staan in hoofdstuk 5. De reflectie op het product en het proces staan in hoofdstuk 6. De referenties zijn opgenomen in hoofdstuk 7. Een belangrijke bijlage om te benoemen voor de leesbaarheid van dit verslag is bijlage 1, waarin begrippen zijn gedefinieerd zoals informatiebeveiliging, informatiebeveiligingsbewustzijn, correct, volledig, effectief, methodiek.

2. Onderzoeksaanpak

Er hebben twee onderzoeken plaatsgevonden, een literatuurstudie en het empirisch onderzoek. In dit hoofdstuk is de aanpak van beide onderzoeken beschreven.

2.1. Onderzoeksmodel

In figuur 1 is het theoretisch onderzoeksmodel weergegeven.
De literatuurstudie (A) levert een referentiemodel op, dat de belangrijkste gedragsrisico's meet bij medewerkers van Nederlandse gemeenten (B). Dit referentiemodel is in de empirische onderzoeksfase (C) gevalideerd. De validatie vond plaats in twee fasen. De eerste fase richtte zich op in hoeverre het referentiemodel volledig en correct was. De tweede fase richtte zich op de effectiviteit van het referentiemodel door het op beperkte schaal toe te passen. De onderzoeksresultaten en de daaruit voortvloeiende conclusies (D) hebben geresulteerd in het antwoord op de probleemstelling van het onderzoek (E).



Figuur 1 Theoretisch onderzoeksmodel

2.2. Onderzoeksaanpak literatuurstudie

Tijdens de literatuurstudie stond de vraag centraal: 'Op welke wijze kan het informatiebeveiligingsbewustzijn en bijbehorend gedrag van medewerkers bij Nederlandse gemeenten worden gemeten?'. Dit had tot doel om te komen tot een ontwerp[2] van een methodiek voor het meten van het informatiebeveiligingsbewustzijn van medewerkers bij Nederlandse gemeenten.
Om dit te onderzoeken waren drie deelvragen geformuleerd (zie paragraaf 1.3.).
De eerste deelvraag richtte zich op het vinden van bruikbare methodieken. De andere twee deelvragen richtten zich op hetgeen dat inhoudelijk door de methodiek gemeten moest worden. Deze drie deelvragen leidden tezamen tot een methodiek waarmee specifiek het informatiebeveiligingsbewustzijn van medewerkers bij Nederlandse gemeenten gemeten kon worden. Per deelvraag is de toegepaste zoekstrategie uitgewerkt.

2 Ook wel referentiemodel genoemd

Zoekstrategie deelvraag 1
Bij deze deelvraag is gebruik gemaakt van de sneeuwbalmethodiek, waarbij gestart is vanuit het onderzoek van Koroliov et al. (2009). Hiervoor is gekozen omdat in dit onderzoek de aanbeveling werd gedaan om de waargenomen discrepantie tussen kennis en gedrag van medewerkers te onderzoeken. Dit vormde mede de aanleiding van de probleemstelling van dit onderzoek. Via de sneeuwbalmethodiek zijn artikelen geselecteerd welke in de regel stammen uit de periode na 2000. Vanaf deze periode zijn computers en internet breder toegankelijk geworden. Organisaties zijn dit intensiever gaan gebruiken, wat van invloed is op het informatiebeveiligingsbewustzijn. Daarbij is gekeken of in de referentielijst key-woorden voorkwamen die gelieerd waren aan 'framework for information security awareness' en of de publicatie een peer-review heeft gekend. Daarnaast is met dezelfde criteria tevens bij het downloaden van een publicatie gebruik gemaakt van de optie 'users who downloaded this article also downloaded…'

Doordat de sneeuwbalmethodiek op een gegeven moment niet meer leidde tot nieuwe inzichten is via Google Scholar op vergelijkbare wijze gezocht. Tot slot is ook nog met behulp van de 'quick search' in de digitale bibliotheek van de Open Universiteit Nederland naar relevante publicaties gezocht met de termen 'model to measure and evaluate information security awareness'. Dit leidde vrijwel direct tot dezelfde publicaties dan wel tot publicaties die geen nieuwe inzichten gaven. Daarop is besloten het zoeken te beëindigen en de deelvraag te beantwoorden met de gevonden publicaties.

Zoekstrategie deelvraag 2
Doordat deelvraag 2 zich richtte op niet-wetenschappelijke publicaties, is in Google gezocht naar bronnen die informatie gaven over inhoudelijk uitgangspunten die gericht waren op het informatiebeveiligingsbewustzijn bij Nederlandse gemeenten. Gestart werd met de twee zoektermen 'informatiebeveiliging' en 'Nederlandse gemeenten'. Hierbij lag de focus op publicaties na 2011, omdat destijds de DigiNotar-affaire had plaatsgevonden. De DigiNotar-affaire vormde een belangrijke aanleiding op landelijk niveau om informatiebeveiliging naar een hoger plan te tillen binnen de overheid.
Met deze twee zoektermen werden direct bruikbare hits getoond die leidden naar de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' en de Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG, 2013a). Van hieruit is de sneeuwbalmethodiek gebruikt en zijn inhoudelijke uitgangspunten aangetroffen die specifiek voor Nederlandse gemeenten gelden.

Zoekstrategie deelvraag 3
Deze deelvraag had tot doel om de methodiek en de inhoudelijke uitgangspunten aan te scherpen voor de specifieke omgeving (Nederlandse gemeente) en doelgroep (medewerkers). Gezocht is naar onderzoeken vanaf het jaar 2000 om dezelfde reden als genoemd bij de zoekstrategie van deelvraag 1. Hierbij is gestart met het zoeken via Google Scholar met behulp van diverse zoektermen in verschillende combinaties. Er is gezocht met Nederlandse zoektermen aangezien de focus lag op onderzoeken die bij Nederlandse gemeenten waren uitgevoerd. Gezocht is met de zoektermen: informatiebeveiliging; bewustzijn; onderzoek; Nederland; gemeente. Dit leverde geen relevante onderzoeken op behalve dat van Van der Goes (2012). Vervolgens is in Google Scholar met andere (Engelse) zoektermen gezocht om uit te sluiten dat een onderzoek wel is gedaan en in het Engels is beschreven. Gezocht is met de zoektemen: information security awareness; government; employees; Netherlands; en public

organizations. Ook hierbij zijn diverse combinaties geprobeerd. Dit leidde niet tot relevante publicaties.

Aansluitend is op vergelijkbare wijze verder gezocht in de digitale bibliotheek van de Open Universiteit Nederland met de optie 'quick search'. Ook dit leverde geen relevante publicaties op. Tot slot is gezocht in de scriptiedatabase van het vakblad van Platform voor Informatiebeveiliging. Dit leverde qua relevantie alleen het onderzoek op van Neys (2003). Zij heeft onderzocht in hoeverre het gedrag van IT'ers bij de Rabobank ICT bijdraagt aan het niveau van de informatiebeveiliging. Dit is gedaan met behulp van het model van Clarke, genaamd het model van 'normale overtredingen'. Dit model meet niet het informatiebeveiligingsbewustzijn, maar analyseert waarom bepaald gedrag wordt vertoond dat tegenstrijdig is met het beleid. Dit model kan waardevol zijn in onderzoek naar het verklaren waarom bepaald gedrag afwijkt van hetgeen dat in het informatiebeveiligingsbeleid is vastgelegd. Dit model kan niet worden gebruikt voor het meten van het actuele informatiebeveiligingsbewustzijnniveau.

2.3. Onderzoeksaanpak empirisch onderzoek

Op basis van de literatuurstudie is een methodiek ontworpen waarmee het informatiebeveiligingsbewustzijn van medewerkers bij Nederlandse gemeenten kon worden gemeten. In de empirische onderzoeksfase is deze methodiek gevalideerd, wat inhoudt dat is nagegaan of de methodiek correct, volledig en effectief is. Het empirisch onderzoek is in twee fasen verdeeld. In de eerste fase is gekeken in hoeverre de ontwikkelde methodiek correct en volledig was, waarop aansluitend in de tweede fase de methodiek is beoordeeld op effectiviteit. Grofweg kan gesteld worden dat in fase 1 de methodiek werd beoordeeld op de inhoud en in fase 2 op de toepasbaarheid. Deze paragraaf beschrijft per fase de onderzoeksaanpak. Paragraaf 2.3.3. richt zich op de validiteit en betrouwbaarheid van het empirisch onderzoek.

2.3.1. Fase 1 van empirisch onderzoek

In deze onderzoeksfase is het model geverifieerd door inhoudelijke deskundigen op correctheid en volledigheid. Het model is vervolgens voor fase 2 is aangepast om beoordeeld te worden op effectiviteit door medewerkers. Aan de deskundigen is tevens gevraagd een uitspraak te doen over de verwachte bruikbaarheid van de methodiek.

Onderzoeksstrategie

Op kwalitatieve wijze is de methodiek gereviewd door middel van vier semi-gestructureerde interviews met open vragen (zie bijlage 2). Deze interviews zijn afgenomen bij personen die deskundig zijn op het vlak van informatiebeveiliging – specifiek bij overheden en gemeenten. De interviewvragen zijn gekoppeld aan de onderzoeksvragen. Er is gekozen voor een semigestructureerd interview omdat (Vennix, 2006):

- dit de mogelijkheid geeft om per aspect de diepte in te gaan;
- de geïnterviewde uitleg kan geven aan zijn antwoorden;
- dit leidt tot meer overwogen antwoorden dan bij gesloten vragen.

Via een brief (zie bijlage 3) zijn de volgende personen uitgenodigd voor een interview:

- een afvaardiging van twee personen van de Informatiebeveiligingsdienst voor gemeenten (IBD). De IBD is een organisatie die Nederlandse gemeenten ondersteunt en adviseert bij het vormgeven van informatiebeveiliging;

- een deskundige vanuit het Centrum informatiebeveiliging en privacybescherming (CIP-overheid);
- de Chief Information Security Officer (CISO) van de gemeente Edam-Volendam;
- een afvaardiging van drie persoon die hebben gewerkt aan het programma iBewustzijn Overheid. Aan deze personen is aansluitend gevraagd op welke wijze deze campagne tot stand is gekomen aangezien naar aanleiding van de literatuurstudie de bijbehorende 10 gouden regels zijn opgenomen in de methodiek om het informatiebeveiligingsbewustzijn te meten.

Primaire onderzoekgegevens en verantwoording selectie geïnterviewden
De geïnterviewden hebben op basis van hun deskundigheid (kennis en ervaring) de methodiek beoordeeld. Zij zijn geselecteerd voor het interview omdat de IBD, het CIP en de Taskforce BID[3] zich op landelijk niveau actief inzetten voor het verbeteren van de informatieveiligheid en -beveiliging bij overheden (waaronder specifiek gemeenten). De CISO is geselecteerd omdat deze CISO informatiebeveiliging vormgeeft conform de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), die leidend is voor gemeenten (VNG, 2013a). Daarbij heeft deze CISO een traject ingezet om te werken aan het informatiebeveiligingsbewustzijnniveau van 'zijn' medewerkers.

Wijze waarop de gegevens worden geanalyseerd
De interviews zijn uitgewerkt in interviewverslagen (zie bijlagen 4 tot en met 7). De verslagen zijn aan de geïnterviewden voorgelegd ter verificatie voordat deze zijn gebruikt voor de resultatenanalyse. Vervolgens is gekeken waar overeenkomsten en verschillen zitten tussen de gehouden interviews. Bij de analyse is bepaald of en op welke wijze de methodiek moet worden bijgesteld zodat het correct en volledig is, alvorens deze in fase twee van het empirisch onderzoek op effectiviteit wordt getoetst.

Vooruitblik op resultaat
Naar aanleiding van fase 1 is de ontwikkelde methodiek uit de literatuurstudie inhoudelijk beoordeeld op 'in hoeverre de methodiek correct en volledig is'. Op basis hiervan is de methodiek bijgesteld en in fase 2 beoordeeld op effectiviteit (toepasselijkheid).

2.3.2. Fase 2 van empirisch onderzoek
Fase 1 bepaalt in grote mate de wijze waarop het informatiebeveiligingsbewustzijn kan worden gemeten. De betrouwbaarheid van de methodiek wordt grotendeels bepaald door de gegevens die bij de inzet van deze methodiek worden verzameld. Om de validiteit en betrouwbaarheid van de methodiek te versterken zal de methodiek in de praktijk getoetst moeten worden op werking. In verband met de beperking van de onderzoekstijd, is gekozen om de methodiek op beperkte schaal in de praktijk te toetsen. Hierdoor is het mogelijk om een eerste indruk te krijgen van de validiteit en betrouwbaarheid van de methodiek. Hierbij is gekeken in hoeverre de methodiek effectief is. Effectief betekent dat de methodiek bruikbaar is voor de onderzoeker en dat de surveyvragen begrijpelijk zijn voor de medewerkers, en de tijdsduur en hoeveelheid surveyvragen acceptabel zijn voor hen. Dit is van belang omdat dit mede de betrouwbaarheid van de resultaten bepaalt die via de surveyvragen worden opgehaald door de onderzoeker.

[3] Taskforce Bestuur en Informatieveiligheid Dienstverlening (BID) ontwikkelde handvatten voor het verankeren van het informatiebeveiligingsbewustzijn bij overheden, waarbij de resultaten zijn gebundeld in een campagnepakket iBewustzijn Overheid (Blankena, 2015)

Onderzoeksstrategie
Net als in fase 1 en om dezelfde reden, is gebruik gemaakt van een kwalitatief onderzoek door middel van semi-gestructureerde interviews, dit maal echter met gemeentelijke medewerkers. De medewerkers hebben een uitnodigingsbrief ontvangen met de vraag of zij willen deelnemen aan het onderzoek en hoe dit onderzoek verloopt (zie bijlage 8). De medewerkers hebben bij het onderzoek eerst een survey met gesloten vragen ingevuld (zie bijlage 9) alvorens het interview daadwerkelijk startte (zie bijlage 10 voor de interviewvragen). De survey vormt een onderdeel van de methodiek waarmee uiteindelijk het informatiebeveiligingsbewustzijn wordt gemeten. Het interview richtte zich op de begrijpelijkheid en haalbaarheid van de survey.

Onderzoekssetting, primaire onderzoeksgegevens en verantwoording selectie geïnterviewden
Als onderzoeker ben ik werkzaam voor de gemeenten Culemborg, Geldermalsen en Tiel waardoor ik eenvoudig toegang heb tot de gemeentelijke medewerkers om de survey te testen. Per gemeente zijn drie personen geselecteerd waarvan ik weet dat zij bereidwillig zouden zijn om hieraan deel te nemen. In totaal zijn negen personen geselecteerd die qua functies tezamen een dwarsdoorsnede vormen van een gemeentelijke organisatie. Het interview is op locatie van de desbetreffende medewerker afgenomen. De volgende functies zijn geïnterviewd: burgemeester, gemeentesecretaris, adviseur P&O, medewerker Documentaire Informatievoorziening, adviseur informatiemanagement, afdelingsmanager, controller, organisatieadviseur en een communicatiemedewerker.
Voor een adviseur P&O is gekozen, omdat een P&O-adviseur over kennis en ervaring beschikt inzake een cultuur die heerst bij een gemeente. Voor een communicatiemedewerker is gekozen omdat deze extra waarde toevoegt aan het interview doordat zij de specifieke survey mede op begrijpelijkheid kan beoordelen vanuit haar expertise.

De volgorde van de afgenomen interviews is gebaseerd op de beschikbaarheid van deelnemers aan het interview. Gestart is met de gemeentesecretaris. Om er zeker van te zijn dat het gehele interview met bijbehorende survey kon worden afgenomen, is eerst de survey als proef bij een willekeurige collega afgenomen om te kijken hoe lang werd gedaan over het invullen van de survey. Op basis hiervan was helder dat het interview en de complete survey binnen 1,5 uur kon worden afgenomen. Vervolgens bleek uit het interview met de gemeentesecretaris dat de vorm van de survey meer gestructureerd moest worden en niet alle vragen helder waren. Deze aspecten zijn aangepast in de survey en vervolgens gebruikt bij de andere acht interviews.

Wijze waarop de gegevens worden geanalyseerd
Net als in fase 1 zijn de interviews uitgewerkt in interviewverslagen (zie bijlage 11) en aan de geïnterviewden voorgelegd ter verificatie voordat deze zijn gebruikt voor de resultatenanalyse. Ook hierbij zijn vervolgens de resultaten vergeleken op overeenkomsten en verschillen tussen de gehouden interviews. Bij de analyse is bepaald of en op welke wijze de survey moest worden bijgesteld zodat deze effectief kan worden afgenomen.

Vooruitblik op resultaat
Deze interviews beogen om tot een haalbare en begrijpelijke survey voor medewerkers te komen. Doordat bij het interview tevens een vooronderzoek is gedaan naar de betrouwbaarheid van de gegeven antwoorden bij de surveyvragen (hierover meer in

paragraaf 2.3.3.), is de betrouwbaarheid van de methodiek versterkt. Daarnaast doe ik als onderzoeker een uitspraak over de bruikbaarheid van de methodiek en de wijze waarop het informatiebeveiligingsbewustzijn eenvoudig kan worden gemeten. Daarnaast doe ik een uitspraak of de resultaten eenvoudig kunnen worden geanalyseerd – wat het doel en output moet zijn de ontworpen methodiek.

2.3.3. Validiteit en betrouwbaarheid

De validiteit houdt in dat de methodiek meet wat het beoogt te meten. In de literatuurstudie is gezocht naar een wetenschappelijk onderbouwd model. Deze is als basis gebruikt, zodat dit model vervolgens verrijkt kon worden met inhoudelijke uitgangspunten die specifiek voor gemeenten gelden. Door de methodiek vervolgens voor te leggen en te bespreken met vakinhoudelijke deskundigen is de validiteit van de ontworpen methodiek geverifieerd. Onderzoeksvragen 1 en 2 zijn gericht op deze verificatie. De validiteit kan versterkt worden door de resultaten te spiegelen aan resultaten uit aanvullende (observatie)onderzoeken, maar gezien de onderzoekstijd en het niet beschikken over financiële middelen is dit niet gedaan. Na het empirisch onderzoek kan tevens een uitspraak gedaan worden over de generaliseerbaarheid.

De betrouwbaarheid geeft aan of bij herhaling van het onderzoek nagenoeg dezelfde resultaten worden gemeten. Om steeds hetzelfde te meten bij herhaling van onderzoek is het van belang dat het model eenduidig, helder en begrijpelijk is voor de medewerkers bij wie het informatiebeveiligingsbewustzijn wordt gemeten aan de hand van een survey. Onderzoeksvraag 3 gaat hierover. Behalve een survey worden meerdere meettechnieken aanbevolen om de betrouwbaarheid van de resultaten te verhogen (Stanton et al., 2005; Kruger & Kearney, 2006; Ceraolo, 1996; Dodge Jr. et al., 2007). Hierbij kan gedacht worden aan social engineering, analyse van systeemdata, penetratietesten en onaangekondigde phishingmailtesten. Zoals eerder beschreven beschik ik als onderzoeker over een beperkte onderzoekstijdsduur en niet over financiële onderzoeksmiddelen. Een survey is daarbij een geaccepteerde methodiek om gedrag, houding en percepties te meten (Berry & Houston in Da Veiga & Eloff, 2010). Door in fase 2 bij het onderzoek 10 controlevragen in te bouwen per dimensie (kennis, houding en gedrag) die aansluiten op de surveyvragen, wordt een uitspraak gedaan over de betrouwbaarheid van de methodiek. Deze controlevragen meten of het antwoord op de gesloten surveyvraag overeenkomt met het antwoord op de controlevraag. Op deze wijze wordt onder andere gekeken naar sociaal wenselijke antwoorden. De controlevragen worden afwisselend gesteld met open en gesloten vragen (zie bijlage 9, vierde vragenlijst). De controlevragen zijn ingeleid met een concrete korte praktijkcasus (mogelijke praktijksituatie).

Verder is voor de validiteit en betrouwbaarheid gebruik gemaakt van een peer- en collegiale (peer)review in fase 1. Deze reviews waren belangrijk omdat ik als onderzoeker na de literatuurstudie de methodiek op eigen inzicht heb aangescherpt vanuit mijn kennis, ervaring en functie als CISO voor drie gemeenten. Om mogelijke ‘blinde vlekken’ af te dekken waren deze reviews gewenst. Doordat ik CISO ben bij drie gemeenten heb ik voor de tweede fase van het empirisch onderzoek een drietal medewerkers geselecteerd per gemeente, waarvan ik achtte dat zij bereidwillig waren om deel te nemen aan het onderzoek. Het bewust selecteren van medewerkers heeft niet geleid tot een bias (vooringenomenheid bij de deelnemers). Zowel zij als ik hadden daar geen enkel belang bij. Daarbij had deze selectie een positieve bijkomstigheid. Het leidde namelijk tot medewerkers die (voor mij) de tijd namen om aandachtig en zorgvuldig de vragen te beantwoorden uit het onderzoek. Voor het onderzoek was het

overigens niet noodzakelijk om een steekproef te trekken uit alle medewerkers voor deelname, maar was het belangrijk om een groep medewerkers te hebben die een dwarsdoorsnede vormde van de gemeentelijke organisatie (ofwel een representatieve groep).

Tot slot geven Siponen en Karjalainen (2011) aan dat er meerdere targetgroups binnen een organisatie kunnen worden onderscheiden voor het informatiebeveiligings-bewustzijn. De targetgroup voor dit onderzoek zijn de eindgebruikers. De eindgebruikers hoeven hierbij geen voorkennis te hebben van IT en/of Information Security (IS) om specifiek gewenst gedrag te kunnen vertonen. Hierbij wordt het gedrag gemeten waarmee medewerkers geen vooropgezette of kwade intenties hebben. Volgens Stanton, Stam, Mastrangeloe en Jolton (2005) kan dit gedrag geclassificeerd worden in ‘naïve mistakes’ en ‘basic hygiene’. Dit type gedrag bij deze targetgroup kan gemeten worden aan de hand van een survey, omdat medewerkers doorgaans bereidwillig zijn om dit soort gedrag te laten meten (Stanton et al., 2005).

3. Van literatuurstudie naar een methode voor het meten van het informatiebeveiligingsbewustzijn

In de literatuurstudie is gezocht naar een methodiek waarmee het informatiebeveiligingsbewustzijn kan worden gemeten bij medewerkers van Nederlandse gemeenten (zie paragraaf 2.2. voor de onderzoeksaanpak en probleemstelling van deze literatuurstudie). In paragraaf 2.3.3. zijn de resultaten uit de literatuurstudie die van invloed zijn op de validiteit en betrouwbaarheid van dit onderzoek al beschreven. In dit hoofdstuk staan de onderzoeksresultaten beschreven aan de hand van de drie gestelde literatuuronderzoeksvragen. In paragraaf 3.4. staat het resultaat van de literatuurstudie.

3.1. Methodieken voor het meten van informatiebeveiligingsbewustzijn

Tijdens de literatuurstudie zijn voornamelijk veel publicaties gevonden die beschreven waarom het belangrijk is om te werken aan het informatiebeveiligingsbewustzijn. Dit heeft volgens Kruger et al. (2006) te maken met het feit dat informatie de 'lifeblood' vormt van een organisatie en medewerkers een grote rol hebben in het beschermen van deze informatie. Gedragsmaatregelen worden effectiever geacht dan organisatorische en technische maatregelen (Hagen et al., 2008). Het gedrag van medewerkers speelt namelijk een grote rol bij de effectiviteit van de implementatie van technische en organisatorische (procedurele) maatregelen, omdat medewerkers deze maatregelen vaak eenvoudig kunnen omzeilen. Het niet naleven van procedures door medewerkers is een grote zorg voor elke organisatie (Siponen & Karjalainen, 2011). Daarom is het van belang om te meten hoe informatiebeveiligingsbewust medewerkers zijn. Siponen (2001), Kruger & Kearney (2006) en Koroliov et al. (2009) merken op dat er weinig methodieken beschikbaar zijn voor het meten van het informatiebeveiligingsbewustzijn. Gedurende de literatuurstudie zijn verschillende methodieken en technieken gevonden voor het meten van het informatiebeveiligingsbewustzijn, maar ook methodieken die op een hoger 'level' de informatiebeveiliging meten. Hierbij ging het niet alleen om het informatiebeveiligingsbewustzijn bij medewerkers, maar om de totale cultuur die hierbij past. Verder zijn ook elementen gevonden in publicaties die deel dienen uit te maken van een methodiek om het bewustzijn te meten op het vlak van informatiebeveiliging. De volgende vier subparagrafen beschrijven de gevonden resultaten.

3.1.1. Drie methodieken voor meten informatiebeveiligingsbewustzijn

In totaal zijn tijdens de literatuurstudie drie methodieken gevonden voor het meten van het informatiebeveiligingsbewustzijn:

1. Information Security Program Maturity Grid Model (Stacey, 1996);
2. Model van Kruger en Kearney (2006);
3. Framework voor ICT-awareness (Kruger et al., 2006).

Met het Information Security Program Maturity Grid Model model van Stacey (1996) kan de volwassenheid van het informatiebeveiligingsbewustzijn worden gemeten aan de hand van vijf volwassenheidsfasen: onzekerheid, ontwaken, verlichting, wijsheid en welwillendheid. Elke fase kan hierbij een volwassenheidsniveau bereiken op vijf aspecten: management, organisatie, incidentafhandeling, geld en verbetering.
Doordat Stacey het model summier beschrijft én vanuit het oogpunt van software engineering, kunnen wat vraagtekens worden gezet bij de toepasselijkheid van dit model. Vooral omdat Stacey niet beschrijft waarop deze vijf aspecten zijn gebaseerd. Daarnaast worden zaken gemeten op het niveau van het hebben van een Information Security Officer en het beschikbaar stellen van geld, maar geeft het geen waardeoordeel over de inhoudelijke kwaliteiten van de vijf aspecten. Het model geeft geen inzicht in de

waarde en betekenis die men mag toekennen aan het bereiken van een fase. Verder ontbreekt de rol van (c.q. een aspect als) 'medewerkers'. Tot slot, zoals Koroliov et. al (2009) in hun onderzoek al opmerkten, is het model statisch van aard (inflexibel) en houdt het geen rekening met de omgeving en de specifieke eigenschappen van een organisatie. De vragen die volgens Stacey gesteld kunnen worden voor de meting worden als gegeven beschouwd en ook hierbij is onduidelijk waarom deze vragen worden gesteld en geen andere vragen.

Een methodiek die meer flexibiliteit kent en rekening houdt met de specifieke eigenschappen van een organisatie is het model van Kruger en Kearney (2006). Zij hebben het informatiebeveiligingsbewustzijn bij een internationaal mijnbouwbedrijf gemeten dat in meerdere regio's gevestigd was. Hierbij meetten zij kennis, houding en gedrag. Deze drie componenten zijn geleend uit het sociaalpsychologische veld en zijn vaker toegepast bij het evalueren van bewustwordingsprogramma's. Vervolgens wordt per type organisatie bepaald welke risicogebieden kunnen worden onderscheiden en welke men gemeten wil hebben. Per risicogebied worden de factoren en de subfactoren bepaald. Tot slot kent het management waarde toe aan de risicogebieden met behulp van het Analytic Hierarchy Process (AHP). AHP, dat tijdrovend kan zijn, probeert subjectiviteit te voorkomen bij het toekennen van de waardes. Deze toekenning kan belangrijk zijn omdat binnen de ene regio een zwaardere weging aan een risico kan worden toegekend dan bij een andere regio. Het model van Kruger en Kearney (2006) kwantificeert uiteindelijk hetgeen dat wordt gemeten, waardoor het niveau van het informatiebeveiligingsbewustzijn concreet kan worden gemaakt. Hiervoor wordt gebruik gemaakt van een vragenlijst om het gedrag te meten, waarbij de meeste vragen een twee- (waar, niet waar) of driepuntschaal kenden als antwoord (waar, weet niet of niet waar). Het risico van deze schaalindeling is dat medewerkers sociaal wenselijke antwoorden geven. Kruger en Kearney merken hierbij dan ook terecht op dat het raadzaam is om in de praktijk ook aanvullende metingen te verrichten, zodat de betrouwbaarheid van de vragenlijst kan worden bepaald. Het toepassen van georganiseerde social engineering en het inzetten mysterie guests behoren onder andere tot de mogelijkheden.

Daarnaast is het mogelijk om systeemdata te gebruiken. Kruger, Drevin en Steyn (2006) hebben het model van Kruger en Kearney (2006) verrijkt met systeemdata om het informatiebeveiligingsbewustzijn te kunnen meten (Framework voor ICT-awareness). Systeemdata zijn namelijk betrouwbaar en objectiever dan vragenlijsten. Daardoor kunnen objectief gegevens verzameld worden over het gedrag van medewerkers. Denk hierbij bijvoorbeeld aan tijdsbesteding van medewerkers aan het internet. Deze methodiek leidt echter direct tot ethische kwesties omdat deze data volgens Kruger et. al (2006) tot op individueel niveau herleidbaar moeten zijn. Het analyseren van systeemdata op individueel niveau zal handmatig redelijk wat tijd in beslag nemen. Indien de onderzoeker de analyse (gedeeltelijk) geautomatiseerd wil laten plaatsvinden, zal de onderzoeker moeten beschikken over budget om hiervoor specialistische instrumenten in te zetten.

3.1.2. Methodieken voor het meten van de informatiebeveiliging(scultuur)

Naast de drie methodieken zijn ook andere methodieken gevonden die gerelateerd zijn aan het meten van het informatiebeveiligingsbewustzijn.
Silva, Menezes en Costa (2012) hebben een model ontwikkeld dat niet specifiek het informatiebeveiligingsbewustzijn meet, maar informatiebeveiliging als geheel binnen een organisatie. Het model bestaat uit de fasen: structureren, modelleren en evalueren.

Structureren betekent dat er een informatiebeveiligingsbeleid is opgesteld. Modelleren betekent dat indicatoren worden vastgesteld en gewaardeerd om te meten in hoeverre medewerkers compliant zijn aan dit beleid. En evalueren betekent het vergaren van data (ofwel de meting doen) en de analyse doen. Het model kent kanttekeningen, want het is een theoretisch nog niet gevalideerd model. De voorgestelde (te meten) indicatoren (23 stuks) zijn niet allemaal eenvoudig te meten, zoals het onderzoeken hoeveel spyware op de werkstations is geïnstalleerd.

Naast het meten van informatiebeveiliging kan ook de informatiebeveiligingscultuur worden gemeten. Thomson en Solms (2006) hebben hiervoor het Information Security Competence Maturity Model (ISCM) ontwikkeld dat vier cultuurtyperingen onderscheidt. Medewerkers zijn 1) onbewust onbekwaam, 2) bewust onbekwaam, 3) bewust bekwaam of 4) onbewust bekwaam. De vierde typering is het hoogst haalbare en betekent dat informatiebeveiliging een tweede natuur is van medewerkers. De publicatie van Thomson en Solms (2006) geeft helaas niet aan hoé de methode kan worden toegepast. Daarnaast hebben Da Veiga en Eloff (2010) ook een framework ontwikkeld voor het meten van de informatiebeveiligingscultuur, genaamd 'Information Security Culture Framework (ISCF). Dit model meet de complete cultuur op organisatie-, groeps- en individueel niveau en meet per niveau verschillende componenten die het gedrag beïnvloeden. Het ISCF is niet specifiek gericht op het informatiebeveiligingsbewustzijn. Dit model gaat veel breder en dieper dan waar de specifieke onderzoeksvraag op doelt.

3.1.3. Elementen die in de methodiek moeten worden opgenomen

Tijdens de literatuurstudie zijn in de publicaties ook elementen aangetroffen die belangrijk zijn bij het meten van het informatiebeveiligingsbewustzijn. Hiervan kan gesteld worden dat de methodiek rekening moet houden met deze elementen. Siponen (2001) geeft aan dat binnen het informatiebeveiligingsbewustzijn meerdere doelgroepen te onderkennen zijn waarvoor andere aspecten gemeten moeten worden. Dit is gelieerd aan hun werkzaamheden. Zo kan er onderscheid gemaakt worden tussen management en medewerkers, maar ook tussen medewerkers die kennis hebben van IT en medewerkers die dat niet hebben. De doelgroep bepaalt mede *hoe* de methodiek wordt vormgegeven. Aytes en Conolly (2003) hebben een model ontwikkeld waar vanuit kan worden afgeleid *wat* gemeten moet worden. In hun model geven zij aan welke factoren van invloed zijn op het gedrag van medewerkers om het informatiebeveiligingsbeleid na te leven of niet. Belangrijk is dat medewerkers de kennis moeten hebben over welke risico's er zijn, wat de gevolgen hiervan zijn als het risico zich voordoet, welke middelen er zijn om de risico's te minimaliseren en hoeveel tijd het kost om deze middelen toe te passen. Dit zijn aspecten die dus bij de kennisvragen moeten terug komen. Aytes en Conolly geven verder aan dat de perceptie van medewerkers van grote invloed is op de keuze die zij maken om specifieke beveiligingsprocedures wel of niet na te leven. Het gaat er hierbij om of medewerkers het beleid weten te vinden, vinden of dit bruikbaar is, de negatieve gevolgen kunnen inschatten van het niet naleven (incl. wat het kost om de eventuele schade te herstellen) en of zij denken dat collega's hen aanspreken als zij het beleid niet naleven. Dit zijn factoren die mede bepalen welk gedrag medewerkers vertonen. Het heeft betrekking op de gebruikersmotivatie c.q. houding van medewerkers, en houding is volgens Siponen (2000) een cruciale factor die het gedrag beïnvloedt. De andere cruciale factor is het hebben van kennis (Siponen, 2001).

Om de consequenties van het eigen handelen te kunnen overzien, dienen medewerkers te weten waarom informatiebeveiliging dient te worden toegepast, hoe dit moet worden gedaan en welke rol zij hierin hebben (Siponen & Karjalainen, 2011). Dit zijn vragen die

overlappend zijn aan de vragen die gesteld kunnen worden inzake de perceptie van medewerkers, zoals Aytes en Conolly (2003) in hun model hebben beschreven.

3.1.4. De vragenlijst en andere technieken

Er zijn verschillende technieken om het informatiebeveiligingsbewustzijn te meten. Een vragenlijst is een geaccepteerde techniek om gedrag, houding en percepties te meten van medewerkers (Berry & Houston in Da Veiga & Eloff, 2010). Hierbij worden dan drie- of vijfpuntsschalen gebruikt. De vragenlijst kan hierbij aangevuld worden met biografische vragen, zoals leeftijd (Da Veiga, Martins, & Eloff, 2007). Een vragenlijst kan schriftelijk of digitaal worden afgenomen. Furnell, Gennatou en Dowland (2002) hebben hiervoor een prototype software ontwikkeld voor kleine organisaties om te werken aan het informatiebeveiligingsbewustzijn en deze te evalueren. Hierbij krijgen medewerkers verschillende scenario's voorgelegd en kan de medewerker zelf maatregelen treffen. Hiermee raken medewerkers bekend met dreigingen, risico's, maatregelen en de gevolgen van het wel of niet treffen van specifieke maatregelen, dan wel het omzeilen van maatregelen.

Stanton, Stam, Mastrangelo en Jolton (2005) classificeren het gedrag van medewerkers naar zes categorieën. Dit is afhankelijk van het kennisniveau (beginner - expert) en de intentie (kwaadaardig – neutraal – welwillend) die een medewerker heeft met zijn gedrag. Om elk soort categorie te meten, adviseren zij om gebruik te maken van observaties, audits en self-ratings/self-reports. Neutrale en welwillende intenties zijn geschikt om te meten met vragenlijsten en audits, omdat medewerkers bereidwillig zijn om dit soort gedrag te laten meten. Om de betrouwbaarheid van de resultaten te verhogen, bevelen zij aan om meerdere meettechnieken te gebruiken. Kruger en Kearney (2006) geven aan dat dit kan met social engineering. Behalve social engineering kunnen ook pentesten worden uitgevoerd (Ceraolo, 1996) of onaangekondigde phishingmailtesten worden uitgezet (Dodge Jr. et al., 2007). Dit is gewenst omdat medewerkers in de praktijk ander gedrag kunnen vertonen dan dat zij aangeven in een vragenlijst.

3.2. Inhoudelijke uitgangspunten voor de methodiek

In de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' is puntsgewijs beschreven welke verantwoordelijkheden gemeenten moeten nemen met betrekking tot informatiebeveiliging (Jorritsma-Lebbink, 2013). Deze is tot stand gekomen in samenwerking met diverse partijen, waaronder gemeenten zelf. Een belangrijk punt uit de resolutie is dat de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) als normenkader voor informatiebeveiliging wordt erkend voor gemeenten (VNG, 2013a). De BIG dient gehanteerd te worden volgens het 'pas toe of leg uit' principe (VNG, 2013b). Het gemeentelijk informatiebeveiligingsbeleid dient vervolgens hierop te zijn gebaseerd.

De BIG is afgeleid van de Baseline Informatiebeveiliging Rijksdienst (BIR), die weer is afgeleid van ISO 27001/27002, welke internationaal is geaccepteerd als beveiligingsstandaard (IBD, 2013). De BIG bestaat uit een strategisch en tactisch deel. In de strategische BIG staat bij de randvoorwaarden dat verantwoord en bewust gedrag van mensen essentieel is voor een goede informatiebeveiliging. Hoe dit georganiseerd dient te worden staat in de tactische BIG.

De tactische BIG is een verdere uitwerking van de strategische BIG en bevat het normenkader. De BIG bevat 303 maatregelen die voorgesteld worden om toe te passen.

Deze maatregelen garanderen hiermee het vertrouwelijkheidsniveau ‘vertrouwelijk’, waardoor rekening is gehouden met onopzettelijke menselijke dreigingen, opzettelijke menselijke dreigingen, social engineering en niet-menselijke dreigingen. Door medewerkers op te leiden, kunnen zij beschikken over de juiste kennis en het bijbehorende gedrag naleven om de kans en de impact van een dreiging te minimaliseren.

Om het informatiebeveiligingsbewustzijn bij medewerkers te stimuleren en te ondersteunen was van 2013 tot begin 2015 de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID) actief. De Taskforce BID heeft samen met het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) de campagne iBewustzijn Overheid opgezet. Hiermee wordt ingezet op de aspecten kennis, houding en vaardigheden, zodat medewerkers van onbewust onbekwaam doorgroeien naar onbewust bekwaam omgaan met informatie (Taskforce_BID & Ministerie_BZK, 2014). Deze campagne geeft hiermee invulling aan het doorgroeimodel van Thomson & Solms (2006) dat ervoor zorgt dat er gewerkt wordt aan het creëren van een cultuur waarbij informatiebeveiliging een tweede natuur is van medewerkers.

Een van de belangrijke producten die bij deze iBewustzijn-campagne is ontwikkeld, zijn de 10 gouden regels. Deze gouden regels geven aan hoe medewerkers zich dienen te gedragen om niet alleen risico’s te voorkomen, maar ook om te leren hoe met incidenten moet worden omgegaan (Taskforce_BID, 2014b). De 10 gouden regels zijn gecategoriseerd naar vier thema’s: iBewust binnen, iBewust buiten, iBewust achter je scherm en iBewust in de cloud. Deze thema’s houden het volgende in (Taskforce_BID, 2014a):

- iBewust Binnen: Alles over bewust en veilig werken binnen de kantoormuren;
- iBewust Buiten: Alles over verantwoord thuis en onderweg werken;
- iBewust Achter je scherm: Alles over het herkennen en vermijden van digitale bedreigingen, zoals hacks, virussen, phishing e-mails;
- iBewust in de Cloud: Verantwoord omgaan met Cloud-omgeving, sociale media en andere (open source) online tools.

De thema’s geven aan vanuit welk perspectief naar risico’s is gekeken om gouden regels op te stellen. Deze thema’s kennen een zekere overlap met elkaar. De thema’s ‘Binnen’ en ‘Buiten’ typeren de fysieke werkomgeving, waar zowel het thema ‘Achter je scherm’ als ‘In de Cloud’ op van toepassing is.

De vier thema’s en de daar bijbehorende gouden regels geven aan op welke wijze het gedrag van medewerkers kan bijdragen aan compliancy op het gebied van informatiebeveiliging conform de BIG. De gouden regels geven hiermee de uitgangspunten weer voor het meten van het informatiebeveiligingsbewustzijn van medewerkers bij Nederlandse gemeenten.

3.3. Uitgevoerde onderzoeken bij Nederlandse gemeenten op het gebied van het informatiebeveiligingsbewustzijn en naleving van het informatiebeveiligingsbeleid

Er zijn geen onderzoeksresultaten beschikbaar inzake gehouden onderzoeken bij Nederlandse gemeenten op het gebied van informatiebeveiligingsbewustzijn en naleving van het informatiebeveiligingsbeleid. Het enige onderzoek dat indirect verband hield met deze onderzoeksvraag is het onderzoek van Van der Goes (2012). Van der Goes deed onderzoek naar in hoeverre Limburgse gemeenten ‘gewapend’ waren tegen social

engineering. Dit onderzoek toont de urgentie aan van het werken aan het informatiebeveiligingsbewustzijn van medewerkers van Nederlandse gemeenten – expliciet met betrekking tot social engineering. Van der Goes (2012) beschrijft dat de Code van Informatiebeveiliging informatiebeveiligingsmaatregelen bevat op het gebied van informatiebeveiligingsbewustzijn. Deze maatregelen zijn voor gemeenten tegenwoordig belegd in de BIG. Het onderzoek geeft verder geen nieuwe uitgangspunten of inzichten die meegenomen kunnen worden in de te ontwikkelen methodiek waarmee het informatiebeveiligingsbewustzijn bij medewerkers van Nederlandse gemeenten gemeten kan worden.

Via het Platform van Informatiebeveiliging is verder nog het onderzoek van Neys (2003) gevonden. Zij heeft het onderzocht in hoeverre het gedrag van IT'ers bij de Rabobank ICT bijdragen aan het niveau van de informatiebeveiliging. Dit is gedaan met behulp van het model van Clarke, genaamd het model van 'normale overtredingen'. Dit model meet niet het informatiebeveiligingsbewustzijn, maar analyseert waarom bepaald gedrag wordt vertoond dat tegenstrijdig is met het beleid. Dit model kan waardevol zijn in onderzoek naar het verklaren waarom bepaald gedrag afwijkt van hetgeen dat in het informatiebeveiligingsbeleid is vastgelegd. Dit model kan echter niet worden gebruikt voor het meten van het actuele informatiebeveiligingsbewustzijnniveau.

3.4. Resultaat literatuurstudie: Methodiek om het informatiebeveiligingsbewustzijn te meten bij medewerkers van Nederlandse gemeenten

Er zijn veel publicaties beschikbaar omtrent het opzetten en het belang van information security awareness programs en over information security awareness culture. Een beperkt aantal publicaties gaat specifiek over het meten van het informatiebeveiligingsbewustzijn. In totaal zijn drie methoden gevonden voor het meten van het informatiebeveiligingsbewustzijn:

1. Information Security Program Maturity Grid Model (Stacey, 1996);
2. Model van Kruger en Kearney (2006);
3. Framework voor ICT-awareness (Kruger et al., 2006).

Er is een methode gevonden die het niveau van informatiebeveiliging meet en niet expliciet het niveau van informatiebeveiligingsbewustzijn:

4. Het model van Silva et al. (2012).

Daarnaast zijn er twee methoden gevonden voor het meten van de informatiebeveiligingscultuur:

5. Information Security Competence Maturity Model (Thomson & Solms, 2006);
6. Information Security Culture Framework (Da Veiga & Eloff, 2010).

Het Information Security Program Maturity Grid Model (Stacey, 1996) is onduidelijk in de wijze hoe het is opgebouwd. Het Framework voor ICT-awareness (Kruger et al., 2006) leidt weliswaar tot betrouwbare resultaten, maar stuit op ethische kwesties en het vergaren van systeemdata is tijdrovend en kostbaar. Het Information Security Competence Maturity Model (Thomson & Solms, 2006) geeft slechts aan wat de uitkomst is van een cultuurmeting aan de hand van vier cultuurtyperingen en beschrijft niet hoe dit gemeten kan worden. Het Information Security Culture Framework (Thomson & Solms, 2006) gaat veel verder en dieper dan het vraagstuk hoe het informatie-beveiligingsbewustzijn kan worden gemeten.

Gezien de onderzoeksvraag, waarbij er specifiek wordt gezocht naar een methodiek voor het domein Nederlandse gemeenten, die valide, betrouwbaar en effectief gebruikt kan worden, wordt het model van Kruger en Kearney (2006) als basis gebruikt. Het model is flexibel en aanpasbaar naar de specifieke eigenschappen die horen bij een Nederlandse gemeentelijke organisatie. In deze methodiek wordt rekening gehouden met aspecten als herbruikbaarheid, gebruiksgemak en is het model wetenschappelijk onderbouwd. Omdat dit model als basis is gebruikt, wordt het model in bijlage 12 uitgebreider beschreven.

Hiermee is op verantwoorde wijze een methodiek als basis beschikbaar. Door deze inhoudelijk te 'vullen' met (gedrags)risico's die specifiek voor Nederlandse gemeenten gelden, wordt de methodiek specifiek gemaakt voor dit domein. Hiervoor worden de 10 gouden gedragsregels uit de campagne iBewustzijn Overheid gebruikt. Op basis hiervan is het niet alleen mogelijk om per gedragsrisico en per dimensie (kennis, houding of gedrag) de resultaten te kwantificeren, maar is het ook mogelijk om de resultaten te abstraheren naar de vier thema's uit de desbetreffende campagne. De methodiek dient verder ook randvoorwaardelijk te voldoen aan een aantal belangrijke elementen die in de literatuur staan beschreven – welke als cruciaal worden beschouwd voor het meten van het informatiebeveiligingsbewustzijn.

Het daadwerkelijk meten van het informatiebeveiligingsbewustzijn kan op diverse manieren, maar gekozen is voor een survey omdat dit een geaccepteerde methodiek is om gedrag, houding en kennis te meten. Deze techniek kan aangevuld worden met technieken die meer tijd en geld kosten, zoals social engineering, gecontroleerde phishingmails, observaties, audits, pentesten en het onderzoeken van systeemdata. Dit komt de betrouwbaarheid van de gegeven antwoorden ten goede. In verband met beperkte onderzoekstijd en –middelen heeft dat niet plaatsgevonden.

Om te komen tot een survey is per gouden regel bepaald op welke wijze de gouden regel gemeten kan worden. Vervolgens zijn deze factoren weer doorvertaald naar specifieke surveyvragen, die gericht zijn op de dimensies kennis, houding en gedrag. Hierbij zijn per factor de kennis-, houdings- en gedragsvragen op elkaar afgestemd, zodat ze steeds hetzelfde aspect meten. De kennisvragen zijn afgestemd op belangrijke elementen die in de literatuur worden genoemd. De kennisvragen moeten meten:

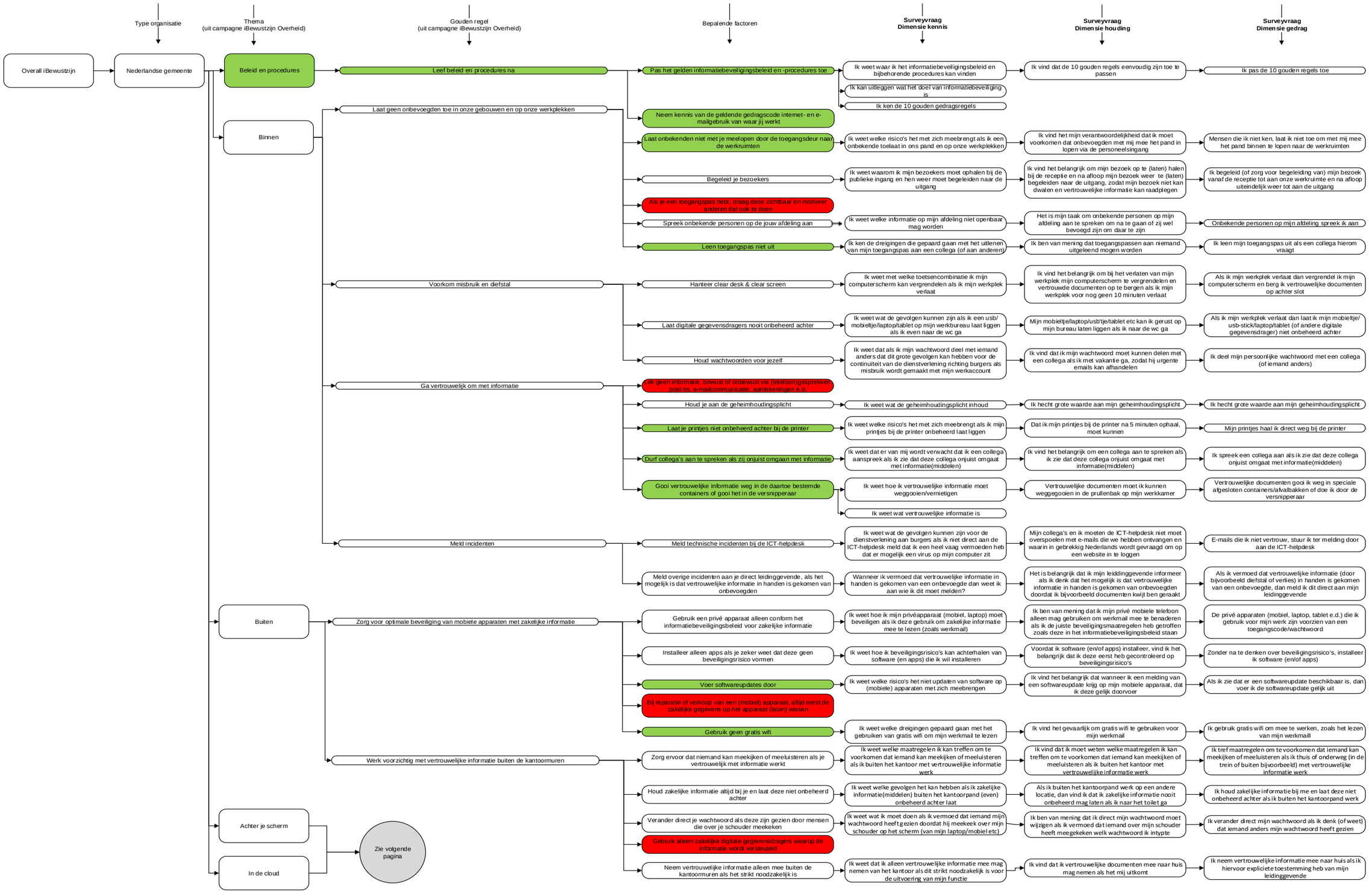
- wat bedrijfsgevoelige activa zijn;
- welke risico's en dreigingen hiervoor gelden en wat de gevolgen hiervan zijn;
- welke middelen er zijn om deze activa te beschermen, waar deze middelen gevonden kunnen worden om toe te passen (zoals procedures) en of deze ook bruikbaar gevonden worden.

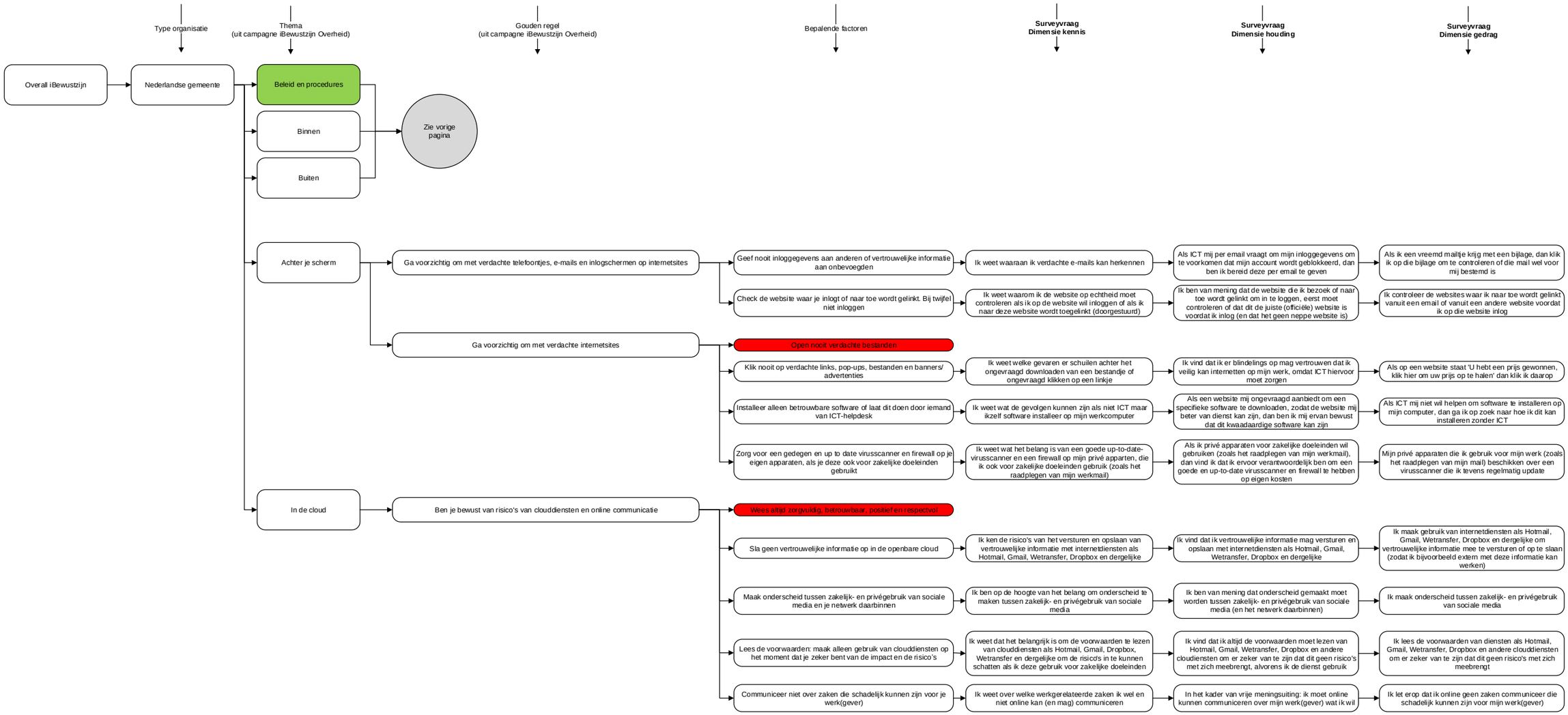
In figuur 2 is het resultaat uit de literatuurstudie visueel weergegeven. Dit model dient van links naar rechts gelezen te worden gelezen. De kolommen geven stapsgewijs aan:

- wat er wordt gemeten (het iBewustzijn);
- waar het wordt gemeten (bij een gemeente);
- welk thema wordt gemeten en welke gedragsrisico's hier vervolgens binnen vallen (in het model zijn dit de gouden regels);
- hoe deze gedragsrisico's worden gemeten. De bepalende factoren kunnen hierbij als zogenaamde key prestatie indicatoren (kpi's) worden gezien van de gedragsrisico's (gouden regels);

- De survey meet tot slot deze bepalende factoren. De survey bestaat uit vragen die inzicht geven in het iBewustzijnniveau per dimensie (kennis, houding en gedrag).

De kennisvragen zijn hierbij steeds afgestemd op één van de drie belangrijke elementen die in de literatuur worden genoemd. Hierbij is één gouden regel naar eigen inzicht toegevoegd, namelijk het naleven van beleid en procedures, welke bij de surveyvragen meet of het beleid vindbaar en toepasbaar is (één van de belangrijke elementen om te meten). De gouden regel uit de campagne iBewustzijn Overheid 'Neem vertrouwelijke informatie alleen mee buiten kantoormuren als het strikt noodzakelijk is', is tekstueel in figuur 2 aangescherpt. Dit zorgt ervoor dat helder is dat het werken buiten de kantoormuren risico's met zich meebrengt. De oorspronkelijk gouden regel is vervolgens opgenomen als bepalende factor bij de aangescherpte gouden regel, aangezien deze op een lager abstractieniveau ligt. Tot slot is ook een aantal factoren op eigen inzicht en ervaring toegevoegd (groen gearceerd) en wordt in de empirische onderzoeksfase 1 voorgesteld om een aantal bepalende factoren te verwijderen (rood gearceerd). De antwoordcategorieën van de kennisvragen gaan uit van een tweepuntsschaal en die van de houdings- en gedragsvragen van een vijfpuntsschaal.


Type organisatie
Thema
(uit campagne iBewustzijn Overheid)
Gouden regel
(uit campagne iBewustzijn Overheid)
Bepalende factoren
Surveyvraag
Dimensie kennis
Surveyvraag
Dimensie houding
Surveyvraag
Dimensie gedrag
Overall iBewustzijn
Nederlandse gemeente
Beleid en procedures
Leef beleid en procedures na
Pas het gelden informatiebeveiligingsbeleid en -procedures toe
Ik weet waar ik het informatiebeveiligingsbeleid en bijbehorende procedures kan vinden
Ik vind dat de 10 gouden regels eenvoudig zijn toe te passen
Ik pas de 10 gouden regels toe
Ik kan uitleggen wat het doel van informatiebeveiliging is
Ik ken de 10 gouden gedragsregels
Binnen
Laat geen onbevoegden toe in onze gebouwen en op onze werkplekken
Neem kennis van de geldende gedragscode internet- en e-mailgebruik van waar jij werkt
Laat onbekenden niet met je meelopen door de toegangsdeur naar de werkruimten
Ik weet welke risico's het met zich meebrengt als ik een onbekende toelaat in ons pand en op onze werkplekken
Ik vind het mijn verantwoordelijkheid dat ik moet voorkomen dat onbevoegden met mij mee het pand in lopen via de personeelsingang
Mensen die ik niet ken, laat ik niet toe om met mij mee het pand binnen te lopen naar de werkruimten
Begeleid je bezoekers
Ik weet waarom ik mijn bezoekers moet ophalen bij de publieke ingang en hen weer moet begeleiden naar de uitgang
Ik vind het belangrijk om mijn bezoek op te (laten) halen bij de receptie en na afloop mijn bezoek weer te (laten) begeleiden naar de uitgang, zodat mijn bezoek niet kan dwalen en vertrouwelijke informatie kan raadplegen
Ik begeleid (of zorg voor begeleiding van) mijn bezoek vanaf de receptie tot aan onze werkruimte en na afloop uiteindelijk weer tot aan de uitgang
Als je een toegangspas hebt, draag deze zichtbaar en motiveer anderen dat ook te doen
Spreek onbekende personen op de jouw afdeling aan
Ik weet welke informatie op mijn afdeling niet openbaar mag worden
Het is mijn taak om onbekende personen op mijn afdeling aan te spreken om na te gaan of zij wel bevoegd zijn om daar te zijn
Onbekende personen op mijn afdeling spreek ik aan
Leen toegangspas niet uit
Ik ken de dreigingen die gepaard gaan met het uitlenen van mijn toegangspas aan een collega (of aan anderen)
Ik ben van mening dat toegangspassen aan niemand uitgeleend mogen worden
Ik leen mijn toegangspas uit als een collega hierom vraagt
Voorkom misbruik en diefstal
Hanteer clear desk & clear screen
Ik weet met welke toetsencombinatie ik mijn computerscherm kan vergrendelen als ik mijn werkplek verlaat
Ik vind het belangrijk om bij het verlaten van mijn werkplek mijn computerscherm te vergrendelen en vertrouwde documenten op te bergen als ik mijn werkplek voor nog geen 10 minuten verlaat
Als ik mijn werkplek verlaat dan vergrendel ik mijn computerscherm en berg ik vertrouwelijke documenten op achter slot
Laat digitale gegevensdragers nooit onbeheerd achter
Ik weet wat de gevolgen kunnen zijn als ik een usb/ mobieltje/laptop/tablet op mijn werkbureau laat liggen als ik even naar de wc ga
Mijn mobieltje/laptop/usb'tje/tablet etc kan ik gerust op mijn bureau laten liggen als ik naar de wc ga
Als ik mijn werkplek verlaat dan laat ik mijn mobieltje/ usb-stick/laptop/tablet (of andere digitale gegevensdrager) niet onbeheerd achter
Houd wachtwoorden voor jezelf
Ik weet dat als ik mijn wachtwoord deel met iemand anders dat dit grote gevolgen kan hebben voor de continuiteit van de dienstverlening richting burgers als misbruik wordt gemaakt met mijn werkaccount
Ik vind dat ik mijn wachtwoord moet kunnen delen met een collega als ik met vakantie ga, zodat hij urgente emails kan afhandelen
Ik deel mijn persoonlijke wachtwoord met een collega (of iemand anders)
Ga vertrouwelijk om met informatie
Lek geen informatie, bewust of onbewust via (telefoon)gesprekken, post-its, e-mailcommunicatie, aantekeningen e.d.
Houd je aan de geheimhoudingsplicht
Ik weet wat de geheimhoudingsplicht inhoud
Ik hecht grote waarde aan mijn geheimhoudingsplicht
Ik hecht grote waarde aan mijn geheimhoudingsplicht
Laat je printjes niet onbeheerd achter bij de printer
Ik weet welke risico's het met zich meebrengt als ik mijn printjes bij de printer onbeheerd laat liggen
Dat ik mijn printjes bij de printer na 5 minuten ophaal, moet kunnen
Mijn printjes haal ik direct weg bij de printer
Durf collega's aan te spreken als zij onjuist omgaan met informatie
Ik weet dat er van mij wordt verwacht dat ik een collega aanspreek als ik zie dat deze collega onjuist omgaat met informatie(middelen)
Ik vind het belangrijk om een collega aan te spreken als ik zie dat deze collega onjuist omgaat met informatie(middelen)
Ik spreek een collega aan als ik zie dat deze collega onjuist omgaat met informatie(middelen)
Gooi vertrouwelijke informatie weg in de daartoe bestemde containers of gooi het in de versnipperaar
Ik weet hoe ik vertrouwelijke informatie moet weggooien/vernietigen
Vertrouwelijke documenten moet ik kunnen weggegooien in de prullenbak op mijn werkkamer
Vertrouwelijke documenten gooi ik weg in speciale afgesloten containers/afvalbakken of doe ik door de versnipperaar
Ik weet wat vertrouwelijke informatie is
Meld incidenten
Meld technische incidenten bij de ICT-helpdesk
Ik weet wat de gevolgen kunnen zijn voor de dienstverlening aan burgers als ik niet direct aan de ICT-helpdesk meld dat ik een heel vaag vermoeden heb dat er mogelijk een virus op mijn computer zit
Mijn collega's en ik moeten de ICT-helpdesk niet moet overspoelen met e-mails die we hebben ontvangen en waarin in gebrekkig Nederlands wordt gevraagd om op een website in te loggen
E-mails die ik niet vertrouw, stuur ik ter melding door aan de ICT-helpdesk
Meld overige incidenten aan je direct leidinggevende, als het mogelijk is dat vertrouwelijke informatie in handen is gekomen van onbevoegden
Wanneer ik vermoed dat vertrouwelijke informatie in handen is gekomen van een onbevoegde dan weet ik aan wie ik dit moet melden?
Het is belangrijk dat ik mijn leiddinggevende informeer als ik denk dat het mogelijk is dat vertrouwelijke informatie in handen is gekomen van onbevoegden doordat ik bijvoorbeeld documenten kwijt ben geraakt
Als ik vermoed dat vertrouwelijke informatie (door bijvoorbeeld diefstal of verlies) in handen is gekomen van een onbevoegde, dan meld ik dit direct aan mijn leidinggevende
Buiten
Zorg voor optimale beveiliging van mobiele apparaten met zakelijke informatie
Gebruik een privé apparaat alleen conform het informatiebeveiligingsbeleid voor zakelijke informatie
Ik weet hoe ik mijn privéapparaat (mobiel, laptop) moet beveiligen als ik deze gebruik om zakelijke informatie mee te lezen (zoals werkmail)
Ik ben van mening dat ik mijn privé mobiele telefoon alleen mag gebruiken om werkmail mee te benaderen als ik de juiste beveiligingsmaatregelen heb getroffen zoals deze in het informatiebeveiligingsbeleid staan
De privé apparaten (mobiel, laptop, tablet e.d.) die ik gebruik voor mijn werk zijn voorzien van een toegangscode/wachtwoord
Installeer alleen apps als je zeker weet dat deze geen beveiligingsrisico vormen
Ik weet hoe ik beveiligingsrisico's kan achterhalen van software (en apps) die ik wil installeren
Voordat ik software (en/of apps) installeer, vind ik het belangrijk dat ik deze eerst heb gecontroleerd op beveiligingsrisico's
Zonder na te denken over beveiligingsrisico's, installeer ik software (en/of apps)
Voer softwareupdates door
Ik weet welke risico's het niet updaten van software op (mobiele) apparaten met zich meebrengen
Ik vind het belangrijk dat wanneer ik een melding van een softwareupdate krijg op mijn mobiele apparaat, dat ik deze gelijk doorvoer
Als ik zie dat er een softwareupdate beschikbaar is, dan voer ik de softwareupdate gelijk uit
Bij reparatie of verkoop van een (mobiel) apparaat, altijd eerst de zakelijke gegevens op het apparaat (laten) wissen
Gebruik geen gratis wifi
Ik weet welke dreigingen gepaard gaan met het gebruiken van gratis wifi om mijn werkmail te lezen
Ik vind het gevaarlijk om gratis wifi te gebruiken voor mijn werkmail
Ik gebruik gratis wifi om mee te werken, zoals het lezen van mijn werkmail
Werk voorzichtig met vertrouwelijke informatie buiten de kantoormuren
Zorg ervoor dat niemand kan meekijken of meeluisteren als je vertrouwelijk met informatie werkt
Ik weet welke maatregelen ik kan treffen om te voorkomen dat iemand kan meekijken of meeluisteren als ik buiten het kantoor met vertrouwelijke informatie werk
Ik vind dat ik moet weten welke maatregelen ik kan treffen om te voorkomen dat iemand kan meekijken of meeluisteren als ik buiten het kantoor met vertrouwelijke informatie werk
Ik tref maatregelen om te voorkomen dat iemand kan meekijken of meeluisteren als ik thuis of onderweg (in de trein of buiten bijvoorbeeld) met vertrouwelijke informatie werk
Houd zakelijke informatie altijd bij je en laat deze niet onbeheerd achter
Ik weet welke gevolgen het kan hebben als ik zakelijke informatie(middelen) buiten het kantoorpand (even) onbeheerd achter laat
Als ik buiten het kantoorpand werk op een andere locatie, dan vind ik dat ik zakelijke informatie nooit onbeheerd mag laten als ik naar het toilet ga
Ik houd zakelijke informatie bij me en laat deze niet onbeheerd achter als ik buiten het kantoorpand werk
Verander direct je wachtwoord als deze zijn gezien door mensen die over je schouder meekeken
Ik weet wat ik moet doen als ik vermoed dat iemand mijn wachtwoord heeft gezien doordat hij meekeek over mijn schouder op het scherm (van mijn laptop/mobiel etc)
Ik ben van mening dat ik direct mijn wachtwoord moet wijzigen als ik vermoed dat iemand over mijn schouder heeft meegekeken welk wachtwoord ik intypte
Ik verander direct mijn wachtwoord als ik denk (of weet) dat iemand anders mijn wachtwoord heeft gezien
Gebruik alleen zakelijke digitale gegevensdragers waarop de informatie wordt versleuteld
Neem vertrouwelijke informatie alleen mee buiten de kantoormuren als het strikt noodzakelijk is
Ik weet dat ik alleen vertrouwelijke informatie mee mag nemen van het kantoor als dit strikt noodzakelijk is voor de uitvoering van mijn functie
Ik vind dat ik vertrouwelijke documenten mee naar huis mag nemen als het mij uitkomt
Ik neem vertrouwelijke informatie mee naar huis als ik hiervoor expliciete toestemming heb van mijn leidinggevende
Achter je scherm
In de cloud
Zie volgende pagina



Figuur 2 Resultaat literatuurstudie: Methodiek ter validatie voor empirische onderzoeksfase 1

4. Resultaten empirisch onderzoek

Zoals beschreven in paragraaf 2.3. bestaat het empirisch onderzoek uit twee fasen. In de eerste fase is gekeken in hoeverre de methodiek die ontworpen is naar aanleiding van de literatuurstudie correct en volledig is. In de tweede fase is gekeken naar de effectiviteit van deze methodiek. De resultaten zijn in dit hoofdstuk per fase beschreven. Hierbij dient opgemerkt te worden dat de resultaten uit fase 1 hebben geleid tot conclusies die pas behandeld worden in hoofdstuk 5, maar op basis van deze conclusies is de methodiek aangepast ten behoeve van de empirische onderzoeksfase 2.
Let op: in dit hoofdstuk zijn dus enkel de resultaten beschreven. De conclusies die uit deze resultaten zijn getrokken staan in hoofdstuk 5 'Conclusies en aanbevelingen'.

4.1. Resultaten uit fase 1

In deze paragraaf staan de onderzoeksresultaten beschreven naar aanleiding van de interviews die zijn gehouden met de CISO van de gemeente Edam-Volendam, de voorzitter van de domeingroep Awareness van het CIP, een afvaardiging van de IBD en betrokkenen bij de oprichting en implementatie van de campagne iBewustzijn Overheid. De interviews spitsten zich toe op drie onderzoeksvragen:

1. In hoeverre is het model volledig, waarbij het de 10 belangrijkste gedragsrisico's meet?
2. In hoeverre is het model correct opgezet?
3. In hoeverre is de ontwikkelde methodiek effectief, waarbij rekening wordt gehouden met de aspecten haalbaarheid, begrijpelijkheid en bruikbaarheid? In deze empirische onderzoeksfase lag de focus op het aspect bruikbaarheid.

Per onderzoeksvraag is de analyse op de resultaten uitgewerkt. De paragrafen 4.1.1. tot en met 4.1.3. bevatten de uitgewerkte analyses. Hierbij is aangegeven welke overeenkomsten en verschillen zijn waargenomen uit de vier gehouden interviews. Het model dat ten grondslag lag aan deze interviews staat in figuur 2. De interviewverslagen zijn opgenomen in bijlagen 4 tot en met 7.

4.1.1. Onderzoeksresultaten ten behoeve van onderzoeksvraag 1

In hoeverre is het model volledig, waarbij het de 10 belangrijkste gedragsrisico's meet?

Om te bepalen wat de belangrijkste gedragsrisico's zijn die de methodiek dient te meten, is tijdens het interview gevraagd welke ontwikkelingen en trends er zijn op het gebied van informatiebeveiliging die risico's met zich meebrengen. Van hieruit zijn de 10 belangrijkste gedragsrisico's afgeleid.

Vanuit de interviews is een gezamenlijk beeld gecreëerd op de ontwikkelingen en bijbehorende organisatierisico's die van invloed zijn op de informatiebeveiliging van gemeenten. De volgende ontwikkelingen zijn geconstateerd:

- Toename van cybercriminaliteit (via besmette e-mails, zoals phishingmails, en besmette internetpagina's; dit leidt tot incidenten met ransomeware[4], cryptoware[5], en identiteitsfraude);
- Gemeenten gaan meer de samenwerking op zoeken met andere gemeenten en partners (ketensamenwerking); waardoor gemeenten meer (persoons)gegevens verwerken en ontsluiten in het kader van eenmalige opslag, meervoudig gebruik;

[4] Een chantagemethode waarbij malware de *computer* van het slachtoffer ontoegankelijk maakt (vergrendelt)
[5] Bij cryptoware is het doel van de gijzeling niet de computer zelf, maar de *bestanden* op de computer

- Er vindt een verschuiving plaats in de manier van werken: er wordt (meer) gestreefd naar tijd- en plaatsonafhankelijk werken;
- Meer digitalisering van informatie en gebruik van mobiele devices;
- Veel data is online beschikbaar (en wordt online gedeeld);
- Er lijkt een verschil in benadering van informatiebeveiliging tussen verschillende generaties. De jongere generatie (na de jaren 90) is meer digitaal minded en groeit op in een digitaal tijdperk met allerlei mobiele devices, waarin zij gewend is dat data open is en dat gegevens gedeeld worden. De oudere generatie is opgegroeid in een tijdperk waarin informatie vooral op papier was vastgelegd en data niet 'open' was. Vanuit een ander perspectief kijken zij naar het gebruik van informatie en mobiele devices;
- Medewerkers worden onvoldoende begeleid bij veranderingen. Zij kunnen de informatie niet op waarde schatten; zijn onvoldoende bewust van hun rol en kunnen de gevolgen van hun eigen handelingen niet overzien;
- De organisatiecultuur sluit niet aan op de geconstateerde ontwikkelingen waarbij informatiebeveiliging tevens niet binnen de processen is geborgd;
- Medewerkers melden niet of niet tijdig incidenten.

Verder zijn ontwikkelingen benoemd die geen deel uitmaken van het gezamenlijke beeld. Dat zijn de volgende ontwikkelingen:

- De ontwikkeling van wet- en regelgeving loopt achter op de praktijk. Die zijn hoofdzakelijk gericht op het 'papieren tijdperk'. Daarbij is de Wet Openbaarheid Bestuur (WOB) gericht op het openbaar maken van bestuurlijke informatie, maar vanuit beveiligingsperspectief is dit niet wenselijk in verband met de risicogevoeligheid. Wetgeving houdt hier nog onvoldoende rekening mee;
- Bestuurders zijn gericht op bestuurlijke zaken, maar deze zaken zijn niet gericht op de digitale ontwikkelingen en mogelijkheden;
- Big data maakt het mogelijk om steeds meer (overheids)gegevens met elkaar te koppelen om te analyseren.

Vanuit deze ontwikkelingen is een gezamenlijk beeld gecreëerd op de belangrijkste gedragsrisico's. Tijdens het interview is geen expliciete een-op-een (of een-op-meer) relatie gelegd tussen de ontwikkelingen en de gedragsrisico's. De deskundigen hebben eerst de belangrijkste risico's benoemd om vervolgens daaruit de belangrijkste gedragsrisico's te abstraheren. Tezamen kwamen zij tot meer dan 10 belangrijke gedragsrisico's. In hoofdstuk 5.1.1. zijn deze vergeleken met de 10 gouden regels, om te kunnen concluderen in hoeverre het model volledig is. Het resultaat van de vier interviews met de deskundigen leidde tot de volgende 12 gedragsrisico's:

1. Lekken en misbruik data door phishingmails en het online delen van data (met eventueel identiteitsfraude tot gevolg);
2. Niet vertrouwelijk omgaan met informatie door (online of in de 'kroegen') te communiceren over werkgerelateerde zaken;
3. Het aspect privacy wordt onvoldoende gewaarborgd met het oog op actuele en aankomende nieuwe privacy wet- en regelgeving;
4. Verstoren continuïteit bedrijfsvoering door te klikken op advertenties of op linkjes in phishingsmails die cryptoware/ransomeware bevatten (niet zo specifiek benoemd in de interviews, maar volgt uit de huidige actualiteit in combinatie met cybercriminialiteit);
5. Medewerkers hebben onvoldoende kennis hoe om te gaan met alle ontwikkelingen vanuit beveiligingsperspectief (hoe voer ik verantwoord de

keukentafelgesprekken, hoe beveilig ik mijn mobiele devices, welke gegevens mag ik waar wel en waar niet in opslaan etc.). Medewerkers worden onvoldoende meegenomen in al deze ontwikkelingen en hierin onvoldoende begeleid. Medewerkers zorgen mede hierdoor dat informatiebeveiliging niet in de procesuitvoering is gewaarborgd. Concreet gemaakt leidt dit naar het gedragsrisico: niet (tijdig) consulteren van de CISO;

6. Niet de waarde van de informatie kunnen inschatten;
7. Niet bewust zijn van de risico's van eigen handelen op het gehele proces of op de organisatie;
8. Incidenten worden niet (tijdig) gemeld (wellicht vanuit belangenperspectief en/of omdat zij de impact onvoldoende kunnen inschatten en/of omdat zij incidenten niet herkennen als zodanig);
9. Niet of onvoldoende naleven van beleid en richtlijnen/procedures (wellicht door een onwerkbare situatie door te veel aan maatregelen/beleid/procedures);
10. Elkaar niet aanspreken op gedrag;
11. Documenten en devices onbeheerd op bureau laten liggen, en computerschermen niet 'locken' in verband met het vertrouwen dat men in collega's heeft (onvoldoende naleving van cleardesk en clearscreen principe);
12. Onvoldoende commitment (waaronder het niet/onvoldoende beschikbaar stellen van middelen) en aandacht voor informatiebeveiliging van 'hoger hand' (bestuur en MT).

Bij het analyseren van de interviewresultaten inzake de gedragsrisico's zijn tussen de vier interviews geen verschillen waargenomen. Dit was eerder wel het geval bij de analyse van de resultaten inzake ontwikkelingen in relatie tot de organisatierisico's. De vier interviews hebben op dit punt dus enkel geleid tot een gemeenschappelijk beeld op de belangrijkste gedragsrisico's.

4.1.2. Onderzoeksresultaten ten behoeve van onderzoeksvraag 2

In hoeverre is het model correct opgezet?

Voor deze onderzoeksvraag zijn gegevens opgevraagd die inzicht geven of het model correct is opgebouwd en rekening houdt met de belangrijkste gedragsrisico's die voortvloeien uit de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Hierbij is gekeken naar de opbouw van het model. Hierbij gaat het dan specifiek over: de opbouw van de thema's, de belangrijkste gedragsrisico's, de subfactoren en de surveyvragen. Deze onderdelen moeten namelijk in lijn zijn met elkaar ten gunste van de correctheid van het model.

De inhoud (belangrijkste gedragsrisico's) van de methodiek is gebaseerd op de gouden regels uit de campagne iBewustzijn Overheid. Deze zijn afgeleid uit de 10 gouden regels die eerder waren geformuleerd vanuit de campagne iBewustzijn Rijk. Deze 10 gouden regels zijn opgesteld vanuit richtlijnen van verschillende departementen en Zelfstandige BestuursOrganen (ZBO's) ("met een hoge mate van 'boerenverstand'"). Dit is gedaan door een multidisciplinaire werkgroep vanuit het programma iBewustzijn Rijk. Die 10 gouden regels zijn voor gemeenten geschikt gemaakt door het materiaal van iBewustzijn Rijk om te schrijven voor overheid breed gebruik (waaronder dus ook gemeenten). Hierbij heeft een reviewronde plaatsgevonden door een aantal gemeenten, waaronder de gemeente Groningen.

De kern bij de bepaling van de gouden regels vormde de drie vragen:

1. Wat doe je nu?
2. Welk risico loop je daarmee?
3. Wat zou een veiliger gedrag zijn?

Bij het bepalen in hoeverre het model correct is opgebouwd, is het volgende bij de interviews aangegeven:

- Drie van de vier interviews geven weer dat de gouden regels (belangrijkste gedragsrisico's) de thema's meten. De IBD deelde die mening niet en merkte op dat het model een zekere mate van hiërarchie kent, waarbij de thema's van gelijke orde behoren te zijn. De vijf genoemde thema's zijn van verschillend niveau en tegelijk onlosmakelijk met elkaar verbonden, wat het lastig maakt om een arbitraire scheiding aan te brengen (dat wat in het voorgelegde model wel is gedaan). De gedragsrisico's die hieruit voortvloeien zijn volgens de IBD niet altijd aan één thema toe te kennen, maar hebben raakvlakken met meerdere thema's. Het model houdt daar geen rekening mee.
- De geïnterviewden deelden de mening dat de surveyvragen in lijn zijn met elkaar en dat er voldoende surveyvragen zijn gesteld om de subfactoren te meten. Meer surveyvragen hoeven niet gesteld te worden volgens de geïnterviewden.
- Verder zijn opmerkingen gemaakt over het toevoegen, splitsten en aanscherpen van specifieke onderdelen. Voor de leesbaarheid van dit product zijn deze niet in dit hoofdstuk in detail beschreven. In bijlage 13 zijn de specifieke opmerkingen weergegeven, waarbij tevens onderbouwd is aangegeven welke opmerkingen wel en niet uiteindelijk zijn verwerkt ten behoeve van fase 2 van het empirisch onderzoek.

4.1.3. Onderzoeksresultaten ten behoeve van onderzoeksvraag 3

In hoeverre is het model bruikbaar voor de onderzoeker?

In het interview is gevraagd in hoeverre de deskundigen verwachten dat het model eenvoudig is toe te passen en de resultaten eenduidig en direct gekwantificeerd kunnen worden. Dit is nodig zodat de resultaten gelijk kunnen worden geanalyseerd om het informatiebeveiligingsniveau te bepalen.

De geïnterviewden zijn het er over eens dat zij verwachten dat het model vanuit het oogpunt van de onderzoeker gebruiksvriendelijk en eenvoudig is toe te passen. Zij doen verder de aanname dat het model binnen elke gemeente kan worden gebruikt, maar geven aan dat het model flexibel moet zijn. Deze flexibiliteit is noodzakelijk omdat het model rekening moet houden met risico's die gelden voor de desbetreffende organisatie. In het model moeten risico's kunnen worden geschrapt, vervangen en worden toegevoegd. Een organisatie die thuiswerken toestaat, kent namelijk andere risico's dan een organisatie die dat niet toestaat. Het model moet hier rekening mee houden en mag dus niet star zijn. De geïnterviewden geven daarnaast aan dat zij verwachten dat door de opzet van de surveyvragen, waarbij gebruik is gemaakt van gesloten vragen, de resultaten uit de survey eenduidig en direct gekwantificeerd en geanalyseerd kunnen worden.

De voorzitter van de domeingroep Awareness van het CIP geeft hierbij aan dat een beperkte respons kan leiden tot vertekend beeld. Dit kan bijvoorbeeld veroorzaakt worden doordat alleen medewerkers die een informatiebeveiligingsfunctie hebben de

survey invullen. Daarom is het wenselijk om de data vanuit verschillende perspectieven te analyseren. Dit kan door bij het afnemen van de survey extra gegevens vast te leggen omtrent sexe, leeftijd, functie en dergelijke.

Daarnaast plaatst de voorzitter van de domeingroep Awareness van het CIP als enige een kanttekening bij de inzet van het model. Hij opteert voor een versnellingskamersessie, waardoor de survey niet bij elke medewerker hoeft te worden uitgezet. Een versnellingskamersessie houdt in dat een groep van bijvoorbeeld 15 personen bijeenkomen waarbij elke persoon plaatsneemt achter een laptop. Eén persoon (de moderator) leidt de sessie vanaf zijn laptop waar vanuit hij alles direct kan analyseren. Iedereen krijgt op de laptop dezelfde (survey)vragen waardoor in een kort tijdsbestek (dagdeel) alle gegevens en analyses voorhanden zijn. Een versnellinsgkamersessie wordt met ongeveer drie verschillende groepen gehouden. Dan is er volgens voorzitter van de domeingroep Awareness van het CIP een representatief beeld, mits de medewerkers uit die groepen een dwarsdoorsnede vormen van de organisatie. Vaak vinden medewerkers het ook eervol om hieraan mee te doen en neemt de bereidwilligheid toe. Tevens is er dan ook de gelegenheid om vragen toe te lichten (vanuit de moderator of vanuit de medewerkers die de antwoorden geven).

4.2. Resultaten uit fase 2

Op basis van de resultaten uit fase 1 is de methodiek bijgesteld. Een visualisatie van de aangepaste methodiek, welke in fase twee is toegepast om de effectiviteit te bepalen, is in bijlage 14 opgenomen. Met effectiviteit wordt bedoeld dat de methodiek begrijpelijk, haalbaar en bruikbaar is. Om de effectiviteit te bepalen is de aangepaste methodiek in de tweede empirische onderzoeksfase toegepast bij een negental medewerkers. In de paragrafen 4.2.1. tot en met 4.2.3. zijn de resultaten per aspect uiteengezet. Tot slot zijn in paragraaf 4.2.4. de resultaten beschreven van de controlevragen die zijn gesteld om inzicht te geven in de betrouwbaarheid van de antwoorden die de negen medewerkers hebben gegeven op de surveyvragen.

4.2.1. Begrijpelijkheid

Op de vraag wat de eerste algemene indruk was van de begrijpelijkheid van de totale vragenlijst, antwoordden alle negen dat de vragenlijst in de regel begrijpelijk en helder was. De vragen waren hierbij goed leesbaar. Drie personen gaven aan dat zij moeite hadden met een aantal gedragsvragen uit de survey. Dit kwam doordat sommige voorbeeldsituaties die bij de vragen werden weergegeven, nooit of zelden waren voorgekomen. Zij wisten niet hoe zij dan de vraag moesten beantwoorden, omdat wordt gevraagd wordt hoe vaak men specifiek gedrag had vertoond in die voorbeeldsituatie.

Ten aanzien van de vraag over de eenduidigheid van de surveyvragen, heeft voornamelijk de gemeentesecretaris aangegeven dat specifieke surveyvragen aangescherpt moesten worden. Deze opmerkingen zijn verwerkt ten behoeve van de andere acht interviews. Bij de andere acht interviews zijn voornamelijk opmerkingen gemaakt over een aantal spellingsfouten, een aantal te lange zinnen in de vraagstelling, het toepassen van dubbele ontkenningen in de vraagstelling en werd aangegeven dat het prettiger is als de stijl van de vragen eenduidig is (alle vragen positief of negatief formuleren). Tot slot werd aangegeven dat een aantal vragen te abstract/te ruim was geformuleerd en dat vragen specifieker gesteld moesten worden voor de eenduidigheid van de vragen.

Alle negen personen gaven verder aan dat de survey zelfstandig kon worden ingevuld. Daarbij gaven zij aan dat zij geen toelichting nodig hadden over hoe de vragen en antwoordcategorieën gelezen c.q. gebruikt moesten worden – behoudens de opmerkingen die zij eerder hierover hadden gemaakt bij de vraag omtrent de eenduidigheid. Aansluitend gaven allen personen aan dat de vragen grotendeels op hun werksituatie van toepassing waren. Daar waar dit niet het geval was, kwam dit omdat men niet beschikte over zakelijke verstrekte mobiele devices, niet buiten kantoor werkte, privé devices niet voor zakelijke doeleinden gebruikte of omdat men niet met anderen dan collega's vertrouwelijke werkgerelateerde gesprekken voerde.

Acht personen gaven aan dat de afkorting CISO voor hen onbekend was. Aanvullend wilden twee personen weten wat het woordje 'kennen' inhoudt bij de kennisvraag in hoeverre men de gouden regels kent. Daarbij wilde één persoon weten wat het woordje 'toepassen' inhoudt bij de vraag in hoeverre men de gouden regels toepast. Vervolgens gaven alle negen aan dat de vragen in de regel helder waren geformuleerd. Twee personen gaven aan dat zij de structuur van de vragenlijst prettig vonden, waarbij de vragen en antwoorden waren gecategoriseerd.

Tot slot gaven allen personen aan dat de surveyvragen eenvoudig te beantwoorden waren op basis van de gegeven antwoordopties. Eén persoon miste de antwoordoptie 'niet van toepassing' omdat niet alle vragen voor deze persoon van toepassing waren op de werksituatie. Twee personen gaven aan dat sommige vragen op elkaar leken en dat het lijkt alsof er herhaling optreedt, terwijl deze vragen andere facetten meten. Vier personen gaven tijdens het interview ter aanvulling aan dat zij het fijn vonden om specifieke antwoorden te kunnen nuanceren in het opmerkingenveld. Alle negen hebben bij het afnemen van de surveyvragen hiervan gebruik gemaakt. Dit gebeurde bij de kennisvragen, waarbij men uitsluitend 'ja' of 'nee' kon beantwoorden. Daarnaast gebeurde dit bij de gedragsvragen waarbij de voorbeeldsituaties niet vaak waren voorgekomen. Zij gaven aan dat bij de kennisvragen hier behoefte aan was omdat deze vragen vroegen naar het hebben van inzicht in het eigen handelen of waarom bepaalde maatregelen gelden. Deze vragen zijn ruim gesteld en zij wisten dan niet of hetgeen waarvan zij dachten dat het antwoord was, dan ook volledig de lading van het antwoord dekte van de vraag als zij 'ja' invulden. Of zij weten wel wat een gevolg van een specifieke handeling kan zijn, maar zijn niet in staat om meerdere (of alle) gevolgen te benoemen. Op dat moment had men dan ook behoefte om het antwoord te nuanceren.

4.2.2. Haalbaarheid

Gemiddeld deed men 20 minuten over de survey met 103 vragen, waarbij de tijd varieerde tussen de 16 minuten en 30 minuten. Hierbij dient opgemerkt te worden dat zij tijdens de survey ook tijd kwijt waren aan het plaatsen van opmerkingen voor het interview indien vragen onduidelijk waren. Zeven vonden het te lang duren en twee personen gaven aan dat het precies genoeg was. Zij vulden alle negen aan dat 10 tot 15 minuten voor hen het maximum is. Twee gaven aan dat wanneer het onderwerp van de vragenlijst hun interesse heeft, zij meer tijd voor zichzelf acceptabel vinden.

Als reactie op het aantal vragen gaven drie personen aan dat zij het gevoel hadden dat het minder dan 103 vragen waren. De rest vond het acceptabel, waarbij drie personen aangaven dat het niet om het aantal vragen gaat, maar om de tijdsduur van de survey.

Zeven van de negen gaven aan dat zij alle vragen met evenveel zorg hebben gelezen en vragen niet hebben 'afgeraffeld'. Vier hiervan gaven hierbij aan dat dit te maken had

omdat zij mij als onderzoeker kennen en mij willen helpen in het afstuderen, dan wel ik hen heb gevraagd de survey zorgvuldig in te vullen. Twee van deze zeven gaven aan dat zij het onderwerp interessant vonden en daarom alles aandachtig hebben gelezen en beantwoord. De andere twee hebben op het einde versneld omdat zij het te lang vonden duren.

Ten aanzien van de vraag wat zij vonden van de verhouding tussen het aantal vragen en de tijdsduur, kwamen dezelfde opmerkingen terug als bij de voorgaande vragen. Aanvullend gaven drie personen aan dat zij een sessie qua werkvorm prefereren boven een survey. Dit omdat een survey tussen de werkzaamheden door moet worden gedaan terwijl een sessie in de agenda wordt ingepland. Dit leidt ertoe dat zij in hun agenda voor een sessie tijd reserveren wat zij bij een survey niet doen. Daarbij gaf een andere persoon aan juist een vragenlijst te prefereren boven een sessie, omdat een vragenlijst minder tijd kost en eenvoudiger zelf is in te plannen.

4.2.3. Bruikbaarheid

De methodiek is in de empirische onderzoeksfase 1, na een viertal interviews met deskundigen, op maat gemaakt voor gemeenten. Het model heeft flexibiliteit als eigenschap. Op basis van deze interviews was de methodiek in twee dagen aangepast, inclusief de bijbehorende surveyvragen. In onderzoeksfase 2 is deze survey in de praktijk toegepast. Dit gebeurde na een korte inleiding over de wijze waarop de survey moest worden ingevuld, zonder inhoudelijke toelichting op de specifieke surveyvragen. Alle negen personen waren in staat de survey zelfstandig in te vullen. Op basis hiervan zijn de resultaten gekwantificeerd en gereed gemaakt voor analyse. Doordat de survey op papier is afgenomen, moesten de resultaten handmatig per vraag verwerkt worden om het informatiebeveiligingsbewustzijn per dimensie en per gedragsrisico te kwantificeren op basis van de formule van de waardefunctie (zie bijlage 12 voor deze formule). Deze kwantificatie kan voor de analysefase inzichtelijk worden gemaakt zoals in figuur 3. De cijfers in figuur 3, welke het bewustzijn kwantificeren, zijn echter in deze figuur fictief. Hiervoor is gekozen omdat aan de negen medewerkers is toegezegd dat de resultaten op het bewustzijnsniveau niet gepubliceerd zouden worden.[6]

	Totaal iBewustzijn per gedragsrisico			
	Kennis	Houding	Gedrag	Totaal
	81	74	73	76
Informatiebeveiliging en gewenste cultuur niet geborgd	85	76	70	77
Onbevoegden toegang verschaffen tot pand en werkruimten	93	76	81	83
Niet (tijdig) melden incident	90	89	76	85
Binnen niet voorzichtig met vertrouwelijke informatie	89	81	75	82
Buiten niet voorzichtig met vertrouwelijke informatie	74	47	70	63
(Privé) mobiele apparaten onvoldoende beveiligd	75	71	65	76
Vatbaar voor phishing	65	72	70	69
Onveilig internetten	75	65	70	74
Vertrouwelijke data online delen	78	73	76	76

Figuur 3 Informatiebeveiligingsbewustzijn per gedragsrisico en per dimensie

[6] Die cijfers geven inzicht in het risicoprofiel wat misbruikt kan worden door kwaadwillenden

Op basis van deze figuur is het mogelijk om de scores te analyseren. Het cijfer varieert tussen de 10 en de 100. Hoe hoger de waarde hoe hoger het bewustzijn is. De organisatie (het management) bepaalt zelf welke maatstaven worden gebruikt. In figuur 3 staat een score tussen de 90 en 100 voor goed (kleur groen), een score tussen de 70 en 89 voor gemiddeld (kleur oranje) en een score van minder dan 70 voor slecht (kleur rood). Het figuur is een gemiddelde van alle resultaten. Een vergelijkbaar figuur kan ook gemaakt worden specifiek voor een gemeente, organisatieafdeling, leeftijdsgroep, functie, sexe, loonklasse etc., zodat de resultaten verder inhoudelijk en meer in diepte geanalyseerd kunnen worden. In figuur 3 zijn de resultaten per dimensie en gedragsrisico inzichtelijk gemaakt en waardes hieraan toegekend, waardoor vervolgens direct gestart kan worden met de analyse.

4.2.4. Controlevragen ten aanzien van de betrouwbaarheid van de antwoorden

De surveyvragen omtrent de dimensies kennis, houding en gedrag besloegen in totaal respectievelijk 36, 33 en 34 vragen. Per dimensie waren 10 controlevragen gesteld nadat de survey was afgenomen (zie bijlage 9, vierde vragenlijst voor de controlevragen). Per dimensie is het resultaat beschreven, waarbij er is gekeken in hoeverre de antwoorden van de controlevragen overeenstemden met de antwoorden op de bijbehorende surveyvragen.

Kennis

Tabel 1 geeft de verhouding weer tussen het aantal antwoorden uit de controlevragen dat overeenkwam met de antwoorden uit de bijbehorende surveyvragen op de dimensie kennis.

Tabel 1 Percentage antwoorden uit controlevraag dat gelijk is aan surveyvraag

Omschrijving	Percentage
% antwoord controlevraag gelijk aan antwoord surveyvraag	74%
% antwoord controlevraag niet gelijk aan antwoord surveyvraag	26%

Van de 26% dat niet overeenkwam, bleek dat hiervan 22 procentpunten niet overeen kwamen doordat men bij de surveyvraag aangaf niet over de kennis te beschikken, terwijl bij de controlevraag bleek dat zij wél over de kennis beschikte. Als voorbeeld gaf men bij de surveyvraag aan niet te weten hoe een verdachte mail kan worden herkend, maar bij de controlevraag wist men 2 tot 3 criteria te benoemen waaraan bijvoorbeeld een phishingmail kan worden herkend.

Houding

Tabel 2 geeft de verhouding weer tussen het aantal antwoorden van de controlevragen dat overeenkwam met de antwoorden uit de bijbehorende surveyvragen op de dimensie houding.

Tabel 2 Percentage antwoorden uit controlevraag dat gelijk is aan surveyvraag

Omschrijving	Percentage
% antwoord controlevraag gelijk aan antwoord surveyvraag	48%
% antwoord controlevraag niet gelijk aan antwoord surveyvraag	52%

Van de 52% dat niet overeenkwam, bleek dat hiervan 34 procentpunten niet overeenkwam doordat het antwoord op de controlevraag één categorie (op de

vijfpuntschaal) afweek van het antwoord uit de surveyvraag. Dit betekent dat (48+34) 82% van antwoorden op de controlevragen overeenkwam met de antwoorden op de surveyvragen, met als kanttekening dat hierbij een afwijking van één schaal wordt toegestaan.
Men selecteerde bijvoorbeeld bij een surveyvraag het antwoord 'helemaal eens' en bij de controlevraag 'eens'. Doordat tussen dergelijke antwoordcategorieën geen arbitraire grens is aangehouden, is een afwijking van één antwoordcategorie te verklaren.
De antwoorden van de gemeentesecretaris zijn overigens hierin niet meegenomen, omdat de vragenlijst na dit interview is aangepast ten behoeve van de resterende acht.

Gedrag
Bij het vergelijken van de antwoorden uit controlevragen met de antwoorden uit de bijbehorende surveyvragen bleek dat deze niet één op één te vergelijken waren. Dit kwam doordat de controlevragen open vragen bevatten en surveyvragen gesloten vragen. De controlevragen hadden als antwoordcategorie een vergelijkbare vijfpuntsschaal moeten hebben (gesloten vragen structuur) om deze te kunnen vergelijken met de antwoorden op de surveyvragen. Daarom is gekeken op welke wijze de resultaten toch bruikbare informatie genereren voor dit onderzoek. Dit is gedaan door te onderzoeken in hoeverre de antwoorden uit de controlevragen het gewenste gedrag laten zien als reactie op de specifieke voorgelegde praktijkcasus. Het gaat er hierbij dus om of de respondenten over de kennis beschikken om verantwoord te reageren op een specifieke praktijksituatie. Hiervoor is gekozen omdat de kennisvragen uit de survey dit niet meten. Die vragen zijn namelijk gericht op één van de drie elementen (zie paragraaf 3.4.).

Tabel 3 geeft het percentage weer van het aantal verantwoorde reacties dat is gegeven op de voorgelegde specifieke praktijksituaties.

Tabel 3 Percentage antwoorden uit controlevraag dat gewenst gedrag vertoont

Omschrijving	Percentage
% antwoord controlevraag dat gewenst gedrag vertoont	72%
% antwoord controlevraag niet het gewenste gedrag vertoont	28%

Uit tabel drie blijkt dat in 72% van de voorgelegde praktijkcases men het gewenste gedrag vertoonde. In 28% van de gevallen vertoonden zij niet het gewenste gedrag.

5. Conclusies en aanbevelingen

In dit hoofdstuk staan de conclusies en aanbevelingen. In de eerste paragraaf staat in het kort de conclusie op de probleemstelling uit de literatuurstudie. Vervolgens staan in de paragrafen 5.2. t/m 5.4. de conclusies per deelvraag uit het empirisch onderzoek. Die deelvragen richtte zich op de validatie van het ontwikkelde referentiemodel naar aanleiding van het literatuuronderzoek. Paragraaf 5.5. geeft antwoord op de centrale onderzoeksvraag uit het empirisch onderzoek en paragraaf 5.6. gaat in op de betrouwbaarheid en validiteit van dat antwoord. Tot slot geeft paragraaf 5.7. aanbevelingen voor vervolgonderzoek.

5.1. Conclusie literatuuronderzoek

Het literatuuronderzoek heeft geresulteerd in een referentiemodel waarmee het informatiebeveiligingsbewustzijn bij medewerkers van Nederlandse gemeenten kan worden gemeten. Dit referentiemodel is opgebouwd uit bestaande modellen, waarbij het basismodel is ontleend van het model van Kruger & Kearney (2006). Dit model is verrijkt met elementen uit andere modellen. Het informatiebeveiligingsbewustzijn wordt gemeten aan de hand van de belangrijkste geldende gedragsrisico's, welke afkomstig zijn uit de 10 gouden regels van de campagne iBewustzijn Overheid (2014b). De meting vindt plaats door middel van een survey, omdat een survey een geaccepteerde methodiek is om het bewustzijn mee te meten (Berry & Houston in Da Veiga & Eloff, 2010). Het model is visueel weergegeven in figuur 2 (paragraaf 3.4.). Paragraaf 3.4. beschrijft de conclusie uit het literatuuronderzoek uitgebreider in detail. Dit model is vervolgens gevalideerd in de empirische onderzoeksfase.

5.2. Conclusie onderzoeksvraag 1 van het empirisch onderzoek

Onderzoeksvraag 1 was: In hoeverre is het model volledig, waarbij het de 10 belangrijkste gedragsrisico's meet?

Het model was inhoudelijk gevuld met de vier thema's en bijbehorende 10 gouden regels uit de campagne iBewustzijn Overheid. Om te onderzoeken of deze 10 gouden regels de 10 belangrijkste gedragsrisico's vormen, is allereerst onderzocht welke ontwikkelingen er momenteel zijn waar vanuit de belangrijkste risico's en vervolgens gedragsrisico's zijn bepaald.

Bij het analyseren van de onderzoeksresultaten inzake de waargenomen ontwikkelingen zijn drie abstractieniveaus geconstateerd. Het eerste abstractieniveau geeft een beeld van de omgeving waarin Nederlandse gemeenten momenteel opereren. Het geeft aan met welke trends c.q. verschuivingen zij te maken hebben. Vanuit deze verschuivingen (focus) hebben de geïnterviewden risico's benoemd die de gemeentelijke organisaties lopen (het tweede abstractieniveau). Van daaruit zijn uiteindelijk de belangrijkste gedragsrisico's gedestilleerd (het derde abstractieniveau) die gemeten dienen te worden. De focus is voor hen dus bepalend geweest bij het benoemen van de belangrijkste gedragsrisico's.

Het eerste abstractieniveau – welke de focus heeft bepaald voor de waargenomen ontwikkelingen op het tweede abstractieniveau zijn:

1. Er is een verschuiving in de fysieke werkomgeving van medewerkers. De verschuiving is van binnen (het kantoor) naar buiten (tijds- en plaatsonafhankelijk werken);

2. Er is een verschuiving van zelfstandig functioneren naar samenwerken met andere organisaties;
3. Er is een verschuiving in de informatiedrager: van analoog naar digitaal (digitalisering);
4. Er is een verschuiving van gesloten naar open databehandeling (online opslag, social media, cloudtoepassingen e.d.);
5. Er lijkt een verschil in benadering tussen generaties inzake informatiebeveiliging.

Vanuit het eerste abstractieniveau zijn de belangrijkste informatiebeveiligingsrisico's voor de gemeentelijke organisatie bepaald:

- Medewerkers worden onvoldoende begeleid bij veranderingen: zij kunnen de informatie niet op waarde schatten; zijn onvoldoende bewust van hun rol en kunnen de gevolgen van hun eigen handelingen niet overzien;
- De organisatiecultuur sluit niet aan op de geconstateerde ontwikkelingen;
- Incidenten en verdachte zaken worden niet (tijdig) gemeld;
- Informatiebeveiliging wordt niet binnen processen geborgd;
- Verstoring van de continuïteit;
- Verlies, lekken en misbruik van data;
- Toename cybercriminaliteit: in de vorm van valse e-mailberichten (zoals phishingmails) en besmette internetpagina's. Veel voorkomende incidenten op dit vlak hebben te maken met cryptoware, ransomeware en identiteitsfraude.

Vanuit deze informatiebeveiligingsrisico's is een gezamenlijk beeld gecreëerd door de deskundigen op de belangrijkste gedragsrisico's (het derde abstractieniveau). Om te bepalen of de 10 gouden gedragsregels ook de belangrijkste gedragsrisico's zijn, is per aangedragen gedragsrisico uit de interviews gekeken in hoeverre deze aansluit op de gouden gedragsregels. Door deze vergelijking is het mogelijk om te bepalen in hoeverre het model volledig is. Onderstaand de vergelijking per aangedragen gedragsrisico:

1. Lekken en misbruik data door phishingmails en het online delen van data: *phishing is opgenomen in gouden regel 8, het online delen van data kan worden opgenomen in gouden regel 10. Dit betekent dat gouden regel 10 aangepast moet worden in het model en zich moet richten op het online delen van informatie en online communicatie;*
2. Niet vertrouwelijk omgaan met informatie door (online of in de 'kroegen') te communiceren over werk gerelateerde zaken: *dit betreft het niet vertrouwelijk omgaan met informatie buiten de kantoormuren. Dit past niet binnen gouden regel 4. Dit moet opgenomen worden in gouden regel 10 omtrent het online communiceren en kan verwerkt worden in gouden regel 7 omtrent het 'fysiek' communiceren over vertrouwelijke zaken buiten de kantoormuren;*
3. Het aspect privacy wordt onvoldoende gewaarborgd met het oog op actuele en aankomende nieuwe privacy wet- en regelgeving: *zit niet in de 10 gouden regels en past hier ook niet in. Dit omdat privacy vanuit een ander perspectief kijkt naar informatie, namelijk vanuit het waarborgen van de privacyrechten van individuen. Informatiebeveiliging focust zich op het waarborgen van de betrouwbaarheid van de informatievoorziening;*
4. Verstoren continuïteit bedrijfsvoering door te klikken op advertenties of op linkjes in phishingsmails die cryptoware/ransomeware bevatten: a*dvertenties zijn opgenomen in gouden regel 9 en phishingmails zitten impliciet in gouden regel 8. Gezien de benoemde risico's mag phishing expliciet worden opgenomen in*

gouden regel 8 aangezien het niet herkennen van dergelijke mails als een groot gedragsrisico wordt gezien;

5. Het niet (tijdig) consulteren van de CISO: *wordt niet gedekt binnen de 10 gouden regels en kan toegevoegd worden aan gouden regel 1 ;*
6. Niet de waarde van de informatie kunnen inschatten: *wordt gedekt in de surveyvragen die zich richten op kennis*;
7. Niet bewust zijn van de risico's van hun eigen handelen op het gehele proces of op de organisatie: *wordt gedekt in de surveyvragen die zich richten op kennis*;
8. Incidenten worden niet (tijdig) gemeld: *is opgenomen in gouden regel 5*;
9. Niet of onvoldoende naleven van beleid en richtlijnen/procedures: *wordt gedekt in gouden regel 1;*
10. Elkaar niet aanspreken op gedrag: *wordt gedekt in gouden regel 4, maar past beter als subfactor bij gouden regel 1;*
11. Onvoldoende naleving van cleardesk en clearscreen principe: *wordt gedekt in gouden regel 3;*
12. Onvoldoende commitment en aandacht voor informatiebeveiliging van 'hoger hand' (bestuur en MT): *dit kan niet expliciet in dit model worden opgenomen, omdat dit enkel gemeten kan worden op bijvoorbeeld MT-niveau (een specifieke doelgroep). Het ontwikkelde model richt zich op alle medewerkers.*

Op basis van bovenstaande vergelijking kan geconcludeerd worden dat het model in de empirische onderzoeksfase in de basis volledig was. Dit betekent dat bovenstaande genoemde gedragsrisico's een overlap kennen met acht van de tien gouden regels uit het model van de empirische onderzoeksfase. Twee gouden regels gaan verder dan bovenstaande gevonden gedragsrisico's. De eerste betrof dat men geen onbevoegde mag toelaten in de gebouwen en op de werkplekken. Dit is vooral van toepassing op kleine tot middelgrote gemeenten, aangezien het toegangsbeleid daar fysiek (minder streng) is beveiligd dan bij grote gemeenten. De andere gouden regel heeft betrekking op het optimaal beveiligen van mobiele apparaten die zakelijke informatie bevatten. De gouden regels uit de iBewustzijn campagne Overheid ogen hiermee verder te gaan dan de gevonden gedragsrisico's uit de interviews.

Het model uit de empirische onderzoeksfase dient dus aangescherpt te worden met de gevonden gedragsrisico's die niet expliciet gedekt worden door de 10 gouden regels. Uit het onderzoek blijkt dan dat het model de volgende belangrijkste gedragsrisico's moet meten:

1. Informatiebeveiliging en bijbehorende gewenste cultuur is niet geborgd;
2. Onbevoegden toegang verschaffen tot de gebouwen en werkplekken;
3. Het niet (tijdig) melden van incidenten en verdachte zaken;
4. Binnen kantoormuren niet voorzichtig omgaan met vertrouwelijke informatie;
5. Buiten kantoormuren niet voorzichtig omgaan met vertrouwelijke informatie;
6. (Privé) mobiele apparaten met zakelijke informatie onvoldoende beveiligen;
7. Vatbaar voor phishing;
8. Onveilig internetten;
9. Vertrouwelijke data online delen (opslaan, versturen en communiceren).

Deze negen gedragsrisico's zijn herleid uit de eerste vier waargenomen verschuivingen. Als het bewustzijn van de gedragsrisico's wordt gemeten door een survey, is het aan te bevelen om ook vragen op te nemen over leeftijd. Hierdoor kan verschuiving vijf worden gemeten. Door dit ook te doen omtrent sexe, loonklasse, functie en dergelijke, is het

mogelijk om vanuit meerdere perspectieven het informatiebeveiligingsbewustzijn te meten en te analyseren.

Tot slot waren ontwikkelingen en trends benoemd die geen deel uitmaken van het gezamenlijke beeld van de deskundigen (zie hoofdstuk 4.1.1.). Deze ontwikkelingen zijn niet verwerkt in het model, omdat deze zich niet laten vertalen tot gedragsrisico's (die voor alle medewerkers gelden).

5.3. Conclusie onderzoeksvraag 2 van het empirisch onderzoek

Onderzoeksvraag 2 luidde: in hoeverre is de ontwikkelde methodiek correct opgezet?

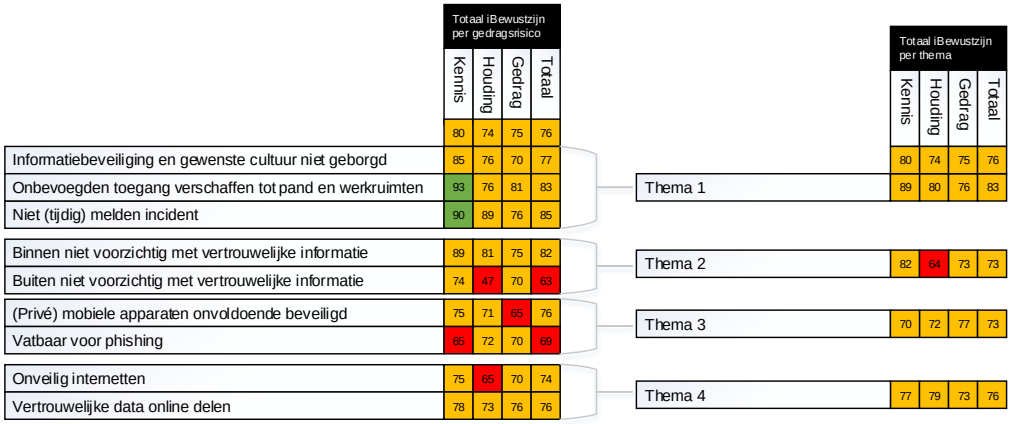
Het begrip 'correct' houdt in dat het model gedragsrisico's meet die voortvloeien uit de BIG. De surveyvragen moeten uiteindelijk deze gedragsrisico's meten, zodat het model meet wat het moet meten voor de gemeentelijke organisatie. Hierbij dienen de surveyvragen te meten dat medewerkers weten:

- wat bedrijfsgevoelige activa zijn;
- welke risico's en dreigingen hiervoor gelden en wat de gevolgen hiervan zijn;
- welke middelen er zijn om deze activa te beschermen, waar zij deze middelen kunnen vinden om toe te passen (zoals procedures) en deze ook bruikbaar vinden.

De gouden regels uit de campagne iBewustzijn Overheid zijn door een multidisciplinaire werkgroep afgeleid vanuit de Baseline Informatiebeveiliging Rijksdienst (BIR) en gereviewd door een aantal gemeenten. De BIG is afgeleid vanuit de BIR. Hieruit kan geconcludeerd worden dat de 10 gouden gedragsregels die in het model zijn opgenomen, op gemeenten van toepassing zijn. Op basis van de conclusie op onderzoeksvraag 1 dienen deze 10 gouden regels aangescherpt te worden voor gemeenten.

De kolom 'thema's' uit het model bevat thema's die van ongelijk niveau zijn. Daarnaast zijn de daaraan gekoppelde gedragsrisico's niet altijd aan één thema toe te kennen, maar hebben deze raakvlakken met meerdere thema's. Hierdoor is de opbouw van het model niet zuiver inzake de thema's. De kolom met thema's, waar vanuit de gedragsrisico's worden geformuleerd, dient vervangen te worden door twee andere kolommen. Dit op basis van de bevindingen bij onderzoeksvraag 1. De kolom thema's wordt vervangen door de kolom 'focus', welke bepaalt vanuit welk perspectief de hoofdrisico's voor een organisatie worden bepaald. Dit kan vanuit ontwikkelingen en waargenomen verschuivingen, zoals beschreven bij de conclusie op onderzoeksvraag 1. Maar dit kan ook vanuit de focus van een specifiek project, de hoofdstukindeling van de BIG of vanuit specifieke organisatiedoelen. Door een kolom 'focus' toe te voegen wordt inzichtelijk vanuit welk perspectief de gedragsrisico's worden bepaald. Dit model biedt die flexibiliteit om de kolom 'focus' anders in te vullen dan in dit onderzoek is gedaan. Na deze kolom dient de kolom 'hoofdrisico's' te worden opgenomen. Hiermee wordt inzichtelijk welke risico's er zijn voor de organisatie - geredeneerd vanuit de kolom 'focus'. Van daaruit kan vervolgens bepaald worden op welk gedrag (en welke gedragsrisico's) men wil sturen. Vanuit het empirische onderzoek is geen één-op-één relatie te leggen tussen de kolommen focus en hoofdrisico's, en hoofdrisico's en gedragsrisico's, waardoor de resultaten ten hoogste op het niveau van de gedragsrisico's kan worden geanalyseerd. Dit is wel gewenst. Indien de kolommen door een onderzoeker anders wordt ingezet, is het mogelijk om de resultaten van de

gedragsrisico's te bundelen tot een hoger niveau. Hierdoor kan op een andere wijze de resultaten geanalyseerd worden. Indien de thema's uit de campagne iBewustzijn Overheid van gelijke orde zouden zijn geweest, waardoor er een één-op-één relatie zou zijn tussen een thema en een gedragsrisico's, dan zou ook op themaniveau geanalyseerd kunnen worden. Figuur 4 is een uitbreiding van figuur 3, waarbij ook op themaniveau het bewustzijn inzichtelijk wordt gemaakt.



Figuur 4 Bewustzijn per gedragsrisico middelen naar bewustzijn per thema

De deskundigen hebben aangegeven dat de kolom met 'bepalende factoren' in grote lijn de belangrijkste gedragsrisico's meet. Deze hoeft dan ook niet aangepast te worden, behoudens de punten uit bijlage 13. De belangrijkste conclusie uit deze bijlage is dat de kolom 'bepalende factoren' met aansluitend de survey, rekening moet houden met de specifieke organisatie-eigenschappen. De deskundigen waren verder van mening dat de surveyvragen qua dimensies met elkaar in lijn waren en dat de kennisvragen telkens rekening houden met één van de drie elementen. In dat opzicht is het model dus correct opgebouwd.

5.4. Conclusie onderzoeksvraag 3 van het empirisch onderzoek

Onderzoeksvraag 3 was: In hoeverre is de ontwikkelde methodiek effectief, waarbij rekening wordt gehouden met de aspecten begrijpelijkheid, haalbaarheid en bruikbaarheid? Per aspect is de conclusie uitgewerkt en in subparagraaf 5.4.5. staat het antwoord op deze onderzoeksvraag.

5.4.1. Begrijpelijkheid

De survey was begrijpelijk en grotendeels op de werksituatie van de medewerkers van toepassing. Om te voorkomen dat vragen niet op de werksituatie van toepassing zijn, moet bij het opstellen van de survey rekening gehouden worden met de specifieke eigenschappen van de organisatie. Eventueel kan de antwoordcategorie 'niet van toepassing' worden toegevoegd, wat ertoe leidt dat het antwoord niet meetelt bij de kwantificering van het informatiebeveiligingsbewustzijn.

De introductie(tekst) bij de survey heeft een belangrijke rol bij de begrijpelijkheid van de surveyvragen. Hierin dient aangegeven te worden hoe (gedrags)vragen beantwoord moeten worden indien de voorgelegde casus zich niet of zelden of heeft voorgedaan. Ondanks dat de survey zelfstandig kon worden ingevuld, bevordert een dergelijke uitleg de zelfstandigheid. Dit wordt tevens bevorderd door surveyvragen te stellen die altijd relevant en van toepassing zijn op de werksituatie van de medewerker. Verder waren de surveyvragen in grote lijn eenduidig gesteld. Taalfouten, waaronder te lange zinnen of

dubbele ontkenningen, moeten voor de begrijpelijkheid niet in de survey voorkomen. Daarnaast dienen vragen niet abstract (c.q. ruim) gesteld te worden, maar heel concreet ten behoeve van de eenduidigheid. Dat geldt ook voor definities en begrippen. In de survey moet duidelijk zijn wie of wat de CISO is en moeten begrippen als ‘kennen’ en ‘toepassen’ worden gedefinieerd.

Het concreet maken van vragen en begrippen is verder van belang om te voorkomen dat men bij de beantwoording van de surveyvragen de antwoorden wil nuanceren, waardoor het gegeven antwoord wellicht niet overeenkomt met de feitelijke situatie. Een opmerkingenveld werd wel gewaardeerd door de medewerkers. Niet alleen ter nuancering, maar ook om aantekeningen te geven of tips terug te geven over de vraagstelling aan de onderzoeker. Het is daarom goed om bij een survey een dergelijk veld toe te voegen, omdat daar behoefte aan is. Dit veld geeft daarnaast ook inzicht in de mate van de betrouwbaarheid van de gegeven antwoorden. Indien antwoorden veel zijn genuanceerd, dan is de meting mogelijk niet volledig betrouwbaar. Nuancering was vooral van toepassing op de kennisvragen en gedragsvragen. Behalve concretisering van de kennisvragen, is een grotere spreiding in de antwoordcategorie noodzakelijk. Behalve de antwoordcategorieën ‘ja en nee’, is een derde antwoordcategorie noodzakelijk, zoals ‘deels wel/deels niet’. Door het toepassen van een driepuntsschaal is het mogelijk om nuances op te vangen. Dit zal hoogstwaarschijnlijk leiden tot meer betrouwbare antwoorden.

Het toepassen van structuur op de survey bevordert de leesbaarheid, waarbij vragen en antwoorden worden gecategoriseerd (op dimensie en bepalende factoor), en waarbij alle vragen in dezelfde stijl (of vorm, zoals positief of negatief) staan. Dit maakt de survey gebruiksvriendelijk voor de medewerker en voorkomt dat de medewerker extra ‘energie’ kwijt is in het ‘schakelen bij, dan wel het ‘vertalen’ van de vraag. Dit kan overigens betekenen dat de medewerker weet wat er wordt gemeten, wat het geven van sociaal wenselijke antwoorden aanlokkelijk kan maken. Voor de bereidwilligheid van het geven van betrouwbare antwoorden, is het van belang om bij de introductie van de survey aan te geven voor wie, waarvoor en waarom de meting wordt gehouden. Daarbij dient te worden aangegeven wat er met de resultaten wordt gedaan en wat de medewerker eraan heeft. Hierbij dient tevens aangegeven te worden dat sommige vragen op elkaar lijken, maar toch een ander facet van informatiebeveiliging meten en er dus geen herhaling van vragen in zit.

5.4.2. Haalbaarheid

De survey werd als te lang ervaren qua tijdsduur. Ongeveer 10 tot 15 minuten wordt als acceptabel gezien, waarin men dan bereidwillig is om een vragenlijst in te vullen. Het aantal vragen is voor de bereidwilligheid ondergeschikt aan de tijdsduur. Indien het langer duurt dan 15 minuten, dan bestaat de kans dat men gaat ‘versnellen’ bij de beantwoording. Versnelling leidt tot minder overwogen en doordachte antwoorden, wat de betrouwbaarheid niet ten goede komt. Dit betekent dat het niet mogelijk is om op dezelfde wijze alle negen gedragsrisico’s te meten. Gekozen kan worden voor het opsplitsen van de risico’s, waarbij periodiek een deel van de gedragsrisico’s wordt gemeten. Daarnaast zijn medewerkers ook bereid om deel te nemen aan een sessie (versnellingskamersessie). Voor de analyse is het dan van belang dat de deelnemers representatief zijn voor de gehele organisatie. Hiermee wordt tevens voorkomen dat een survey organisatiebreed hoeft te worden uitgezet en is het mogelijk om alle gedragsrisico’s te meten (met meer diepgang). Mensen zijn bereidwillig om tijd te reserveren in hun agenda voor een dergelijke sessie. Een sessie kan leiden tot meer

betrouwbare antwoorden. Afhankelijk van de organisatie kan afgewogen worden welke techniek succesvol is: een survey, een sessie of een andere techniek.

De interesse die men heeft in dit onderwerp lijkt mede van invloed op de bereidwilligheid. Daarom is het goed om bij de vragenlijst ook vragen op te nemen over de functie, zodat bij de analyse kan worden vastgesteld dat de deelnemers representatief zijn voor de organisatie. Hiermee wordt voorkomen dat voornamelijk geïnteresseerden en medewerkers die zich in hun functie bezighouden met informatiebeveiliging, de survey invullen, waardoor de onderzoeksresultaten niet gegeneraliseerd kunnen worden naar de gehele organisatie.

5.4.3. Controlevragen ten aanzien van de betrouwbaarheid van de antwoorden

Belangrijk is om te weten in hoeverre betrouwbare antwoorden worden gegeven op de surveyvragen. De controlevragen gaven hier inzicht in ten aanzien van de kennis- en houdingsvragen. Doordat dit op kleine schaal is onderzocht, kan hier geen harde uitspraak over worden gedaan. Daarvoor is vervolgonderzoek nodig. Bij de dimensie ‘gedrag’ kan hier geen uitspraak over worden gedaan, doordat bij de analyse bleek dat de controlevragen onvoldoende aansloten op de bijbehorende surveyvragen.

De antwoorden op de kennisvragen uit de survey ogen betrouwbaar. Hierbij lijkt het tegenovergestelde van sociale wenselijkheid het geval te zijn. Uit de controlevragen blijkt dat zij over meer kennis beschikken dan dat zij bij de survey aangaven. Reden kan zijn dat de vragen uit de survey te ruim zijn gesteld. Bij deze vragen had men vooral behoefte om het antwoord te nuanceren, waardoor zij eerder aangaven dat zij niet over de kennis beschikten dan wel.
Ook de antwoorden op de houdingsvragen komen grotendeels overeen. Met als kanttekening dat op een vijfpuntsschaal één antwoordcategorie afgeweken mag worden van het antwoord op de controlevraag ten opzichte van het antwoord op de surveyvraag. Doordat bij de controlevragen een specifieke casus is voorgelegd, en de surveyvragen algemener zijn gesteld, kan dit mogelijk de verklaring zijn waarom een aantal antwoorden op de controlevragen niet overeenkomt met de antwoorden op de surveyvragen.

De controlevragen inzake de dimensie ‘gedrag’ laten zien in hoeverre medewerkers aangeven over specifieke kennis te beschikken. Of zij weten wat zij moeten als reactie op een specifiek beveiligingsincident. Deze specifieke kennis wordt momenteel niet uitgebreid in de survey gemeten. De kennisvragen richten zich op waarom medewerkers specifiek gedrag moeten vertonen (en dus welke consequenties zijn handelen heeft in termen van risico’s, bedreigingen en gevolgen). Het meten van beide aspecten betekent dat bij elke bepalende factor twee kennisvragen gesteld moeten worden, wat de haalbaarheid (qua tijdsduur en aantal vragen) nadelig beïnvloed. Voor de validiteit van de kennisvragen is het wel wenselijk om beide aspecten te meten.

5.4.4. Bruikbaarheid

In de paragrafen 4.1.3. en 4.2.3. staan de onderzoeksresultaten ten aanzien van dit aspect. Wat de deskundigen verwachtten, is bevestigd in de tweede fase van het empirische onderzoek. Vanuit het oogpunt van de onderzoeker is de methodiek eenvoudig toe te passen en gebruiksvriendelijk. Hierbij kunnen de resultaten eenduidig en direct gekwantificeerd worden, waardoor de resultaten gelijk geanalyseerd kunnen worden om het informatiebeveiligingsbewustzijnniveau te bepalen. De hoofdrisico’s en gedragsrisico’s zijn voor meerdere gemeenten herkenbaar. Door het stellen van gesloten

vragen, is het mogelijk om meer vragen uit te zetten dan wanneer open vragen gesteld worden. Tevens is het mogelijk om gesloten vragen direct te kwantificeren. Het toevoegen van extra gegevens als sexe, leeftijd, functie en dergelijke maken het mogelijk om de analyse vanuit verschillende perspectieven te doen.
In de tweede fase van het empirisch onderzoek is tevens bevestigd dat de survey niet haalbaar is binnen de gestelde tijd van 10 tot 15 minuten, maar dat medewerkers bereid zijn om deel te nemen aan een sessie dat meer tijd in beslag neemt, waardoor het mogelijk is om alle facetten uitgebreid(er) te meten.

Bij het kwantificeren van de resultaten uit de survey is gebleken dat dit handmatig voor een complete organisatie enorm veel tijd vergt van de onderzoeker. Door de survey digitaal af te nemen is het mogelijk om bijvoorbeeld via Excel of SPSS de resultaten eenvoudig te kwantificeren en te analyseren.

Bij de analyse op de dimensie kennis is gebleken dat de kennisvragen steeds één van de drie elementen uit de literatuur meet. Door steeds een ander element te meten, wordt hierdoor niet telkens hetzelfde gemeten (zie ook paragraaf 5.3.3.). Op basis van deze ervaring kunnen kaders gesteld worden wat bij de dimensie ‘kennis’ per bepalende factor moet worden gemeten. De meting dient te meten:

- of medewerkers beschikken over de kennis hoe gehandeld dient te worden (welke procedures gelden);
- of de medewerkers weten waarom zij zo dienen te handelen (weten wat bedrijfsgevoelige activa zijn en wat de mogelijke consequenties zijn in termen van risico’s, bedreigingen en gevolgen).

Uit de literatuurstudie blijkt dat medewerkers ook de procedures bruikbaar en toepasselijk moeten vinden. Daarnaast moeten medewerkers weten waar zij de procedures kunnen raadplegen. Dit hoeft niet in de survey te worden gemeten, maar is een stap die volgt ná de analyse van de resultaten uit de survey als blijkt dat op bepaalde onderdelen laag wordt gescoord. Een lage score zou namelijk verklaard kunnen worden doordat medewerkers de procedures niet kennen, dan wel deze niet bruikbaar vinden. Deze elementen kunnen de discrepantie verklaren tussen de resultaten uit de dimensies kennis en gedrag.

5.4.5. Conclusie op onderzoeksvraag 3

Uit het empirisch onderzoek blijkt dat de survey niet effectief genoeg is. De survey bevat te veel vragen in relatie tot de gestelde tijdslimiet. Daarnaast dienen vragen concreter gemaakt te worden voor de begrijpelijkheid. De begrijpelijkheid wordt mede bepaald door een gebruiksvriendelijke structuur in de survey aan te houden voor de medewerkers, waarbij de vragen concreet (en niet abstract) zijn gesteld. In de introductietekst van de survey kan aangegeven worden wat het belang is van deze survey en de deelname van medewerkers. Hierbij kan tevens aangegeven worden hoe specifieke vragen ingevuld dienen te worden. Dit bevordert de begrijpelijkheid. De huidige survey is niet haalbaar in de tijdsduur van 10 tot 15 minuten die men acceptabel vindt voor deelname hieraan. De vragenlijst kan worden opgeknipt en periodiek worden uitgezet. Ook kan ervoor worden gekozen om alle facetten te meten via een sessie met deelnemers die representatief zijn voor de organisatie. Medewerkers zijn hiertoe bereid. De survey dient bij de kennisvragen te meten of medewerkers weten hoe én waarom zij zich dienen te gedragen in specifieke gevallen. Door aan de survey vragen toe te voegen omtrent sexe, leeftijd en functie is het mogelijk om het informatiebeveiligingsbewustzijn vanuit meerdere perspectieven te analyseren. Bij het verwerken van de resultaten uit de survey

vergt het veel tijd om dit handmatig te doen. Een eenvoudig instrument als Excel of SPSS kan hierbij ondersteuning bieden.

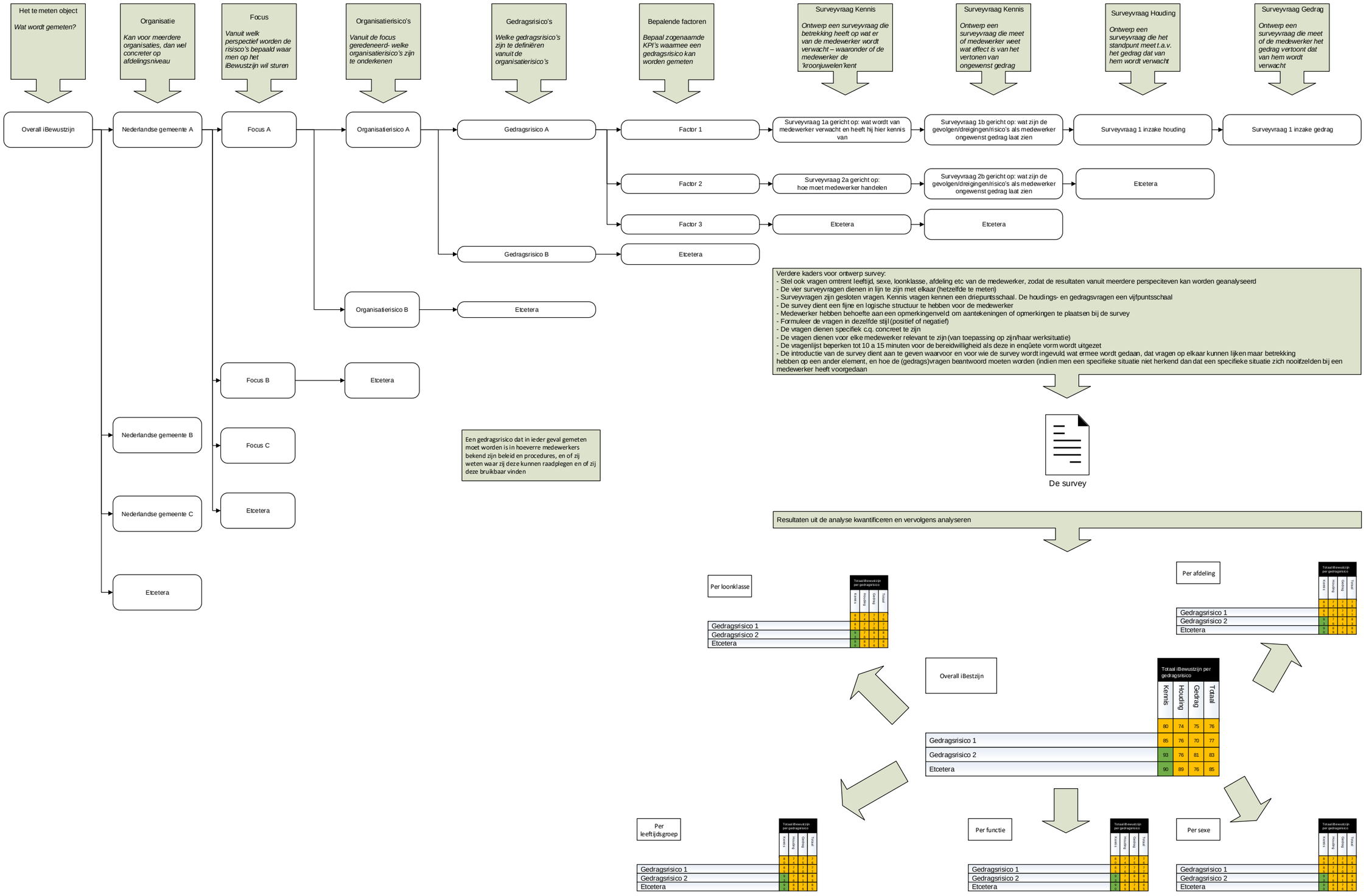
5.5. Antwoord op onderzoeksvraag

Het antwoord op de onderzoeksvraag is uitgebreid en gefragmenteerd beschreven in de paragrafen 5.2. tot en met 5.4. Het onderzoek heeft antwoord gegeven op de centrale onderzoeksvraag. Dit betekent dat een methodiek is ontwikkeld en gevalideerd waarmee het informatiebeveiligingsbewustzijn van medewerkers kan worden gemeten op de belangrijkste gedragsrisico's. Deze gedragsrisico's zijn bepaald op basis van generieke interne en externe (IT-)ontwikkelingen die van toepassing zijn op Nederlandse gemeenten.

Bijlage 14 bevat de methodiek, die 'gevuld' is met gemeentelijke uitgangspunten en die correct en volledig is op basis van de eerste fase uit het empirisch onderzoek.
Dit model is flexibel, duurzaam in gebruik en bruikbaar. Dit is noodzakelijk omdat specifieke organisatie- en gedragsrisico's over de tijd heen veranderen op basis van interne en externe (IT-)ontwikkelingen. Dit is van invloed op de vraag in hoeverre dit model volledig is. Anno 2015 vanuit de focus van vijf waargenomen verschuivingen, is dit model volledig. Vanuit een andere focus en naar verloop van tijd geldt een ander antwoord.

<u>Bijzondere 'bijvangst' – een multifunctioneel model</u>
Bij de analyse van de onderzoeksresultaten en het formuleren van de conclusies ten gunste van de onderzoeksvraag, is gebleken dat uit de gevonden methodiek een structuur kan worden gefilterd dat multifunctioneel kan worden ingezet (zie figuur 5). Dit is een belangrijke vondst voor de flexibiliteit van het model. Door deze vondst oogt het model generiek, waardoor dit model hoogstwaarschijnlijk kan worden toegepast door allerlei organisaties (en niet alleen gemeenten).

Dit blijkt uit de tweede fase van het empirisch onderzoek, waarbij geconcludeerd is dat de survey aangescherpt moet worden ten gunste van het aspect begrijpelijkheid. Deze empirische onderzoeksfase heeft kaders inzichtelijk gemaakt die gelden bij het opstellen van de survey. Wanneer de inhoudelijke uitgangspunten uit het eerder ontwikkelde model (bijlage 14) worden gehaald, dan blijft enkel de structuur van de methodiek met kaders over, die vanuit verschillende focussen kan worden ingezet. Deze structuur is visueel weergegeven in figuur 5. Hierbij is aangegeven hoe de methodiek toegepast dient te worden. Bijlage 15 geeft op hoofdlijnen een stappenplan weer van de toepassing van deze methodiek.



Figuur 5 Resultaat empirische onderzoeksfase: Methodiek om het informatiebeveiligingsbewustzijn te meten

5.6. Betrouwbaarheid en validiteit

De methodiek is gebaseerd op een wetenschappelijk onderbouwd model van Kruger en Kearney. Hierbij is de methodiek voorgelegd voor een peer en collegiale review aan deskundigen die zich bezighouden met het informatiebeveiligingsbewustzijn bij overheden en gemeenten. De collegiale review was nodig omdat ik vanuit mijn eigen CISO-rol bij drie gemeenten het model heb aangescherpt naar eigen inzicht en op basis van mijn ervaringen – wat de interne validiteit van het model ten gunste komt.

De ontworpen methodiek meet gedrag dat volgens Stanton et al. (2005) getypeerd kan worden als ‘naïve mistakes’ en ‘basic hygiene’. Medewerkers zijn bij deze gedragstypen bereidwillig om hun gedrag via een survey te laten meten. Hierbij hoeven medewerkers geen tot nauwelijks IT-kennis te hebben en hebben zij met hun gedrag geen kwaadwillende bedoelingen (bewust procedures omzeilen om schade toe te brengen). De doelgroep van de vragenlijst zijn de eindgebruikers (alle medewerkers die werken met informatie(middelen)). De methodiek is vervolgens op beperkte schaal toegepast bij een drietal kleine tot middelgrote gemeenten en bij een negental medewerkers die representatief zijn voor een gemeentelijke organisatie. Hierbij is gekeken in hoeverre het model effectief is en hoe het model effectiever kan worden gemaakt. Via controlevragen op de kennis- en houdingsvragen is gemeten in hoeverre via de survey betrouwbare antwoorden worden gegeven. Hieruit valt op te maken dat dit in grote lijn het geval is. Uit onderzoek blijkt daarbij wel dat het model effectiever kan worden gemaakt door de survey strakker in te richten. Door deze survey vervolgens op grote schaal uit te zetten bij meerdere gemeenten en medewerkers kan een sterkere uitspraak worden gedaan over de betrouwbaarheid en validiteit van het model. Dit kan tevens worden versterkt door naast de survey aanvullende onderzoekstechnieken toe te passen om de onderzoeksresultaten met elkaar te spiegelen.

Door voort te bouwen op een wetenschappelijk model, deze voor te leggen en deskundigen en het model op beperkte schaal toe te passen, kan gesteld worden dat de basis van het ontwikkelde model betrouwbaar en valide is. De aanname is dat de externe validiteit van het model breder is dan alleen voor kleine tot middelgrote gemeentelijke organisaties. Het model is specifiek gemaakt door het te ‘vullen’ met gemeentelijke uitgangspunten, maar het model biedt de flexibiliteit om dit tevens eenvoudig te wijzigen voor andere (overheids)organisaties.

5.7. Aanbevelingen

Op basis van de conclusies en paragraaf 5.5. over de betrouwbaarheid en de validiteit, doe ik twee aanbevelingen voor vervolgonderzoek:

1. In hoeverre is de ontwikkelde methodiek te generaliseren naar andere (overheids)organisaties?;
   Het model van Kruger en Kearney (2006) is uitgebreid en verrijkt op basis van een onderzoek(svraag) dat is gericht op het domein van Nederlandse gemeenten. De vraag is in hoeverre dit te generaliseren is naar andere (overheids)organisaties.
2. Op welke wijze leidt de survey uit de ontwikkelde methodiek tot de meest betrouwbare antwoorden?
   De methodiek is op beperkte schaal in de tweede fase van het empirisch onderzoek ingezet, waaruit blijkt dat de effectiviteit van deze methodiek grotendeels wordt bepaald door de survey. Dit is een onderzoek op zichzelf om de betrouwbaarheid van de methodiek te versterken.

Uit de literatuurstudie is gebleken dat het model van Clarke (Neys, 2003) mogelijk gebruikt kan worden om de discrepantie te onderzoeken tussen kennis en gedrag van medewerkers op het vlak van informatiebeveiliging. Op het moment dat dit onderzocht gaat worden, is mijn aanbeveling dit model hierin mee te nemen.

6. Reflectie

Dit hoofdstuk bestaat uit een productreflectie en een procesreflectie. De productreflectie beschrijft de betekenis van de conclusies en aanbevelingen. De procesreflectie reflecteert het onderzoeksproces.

6.1 Productreflectie

De conclusies van dit onderzoek hebben als theoretische relevantie dat het model van Kruger en Kearney (2006):

- is uitgebreid met de kolommen 'focus' en 'hoofdrisico's', waarbij de kolom 'focus' flexibel kan worden ingezet en bepalend is vanuit welke focus het informatiebeveiligingsbewustzijn wordt gemeten;
- is verrijkt en verscherpt, waarbij kaders zijn meegegeven aan de surveyvragen voor het versterken van de betrouwbaarheid. Hierbij dienen de kennisvragen twee aspecten te meten (weet een medewerker hoe hij zich moet gedragen en waarom). Daarnaast moeten de vragen minimaal een driepuntsschaal hebben als antwoordcategorie (ja – deels wel/deels niet – nee);
- meer valide is geworden, doordat is gebleken dat dit model ook gebruikt kan worden om het informatiebeveiligingsbewustzijn bij medewerkers van Nederlandse gemeenten te meten.

Daarnaast is een eerste stap gezet richting de onderzoeksvraag die zich richt op het verklaren van de discrepantie tussen kennis en gedrag.

De praktische relevantie is dat er een methodiek beschikbaar is voor gemeenten om het informatiebeveiligingsbewustzijn te meten. Hiermee kan bepaald worden op welke vlakken een security awareness programma zich op moet focussen. Hierbij kan de effectiviteit van het programma worden gemeten door middel van een 0-meting en een 1-meting. Daardoor kan onderzocht worden hoe effectief het informatiebeveiligingsbeleid en –procedures binnen de organisatie zijn. De aanbevelingen geven aan dat het nodig is om de betrouwbaarheid van de survey te vergroten door te onderzoeken op welke wijze en door middel van welke vraagstelling de meest betrouwbare antwoorden kan worden verkregen op de surveyvragen. Dat is in dit onderzoek niet vastgesteld – wel zijn er kaders meegegeven die hier richting aan geven. Daarnaast is een aanbeveling gedaan om te onderzoeken of dit model verder gegeneraliseerd kan worden, waardoor deze methodiek breder kan worden ingezet. De laatste aanbeveling leidt niet tot een onderzoeksvraag, maar geeft een aanwijzing in de richting van het instrument dat gebruikt kan worden om de discrepantie tussen kennis en gedrag te onderzoeken.

6.2 Procesreflectie

Doordat de onderzoeksvraag in de praktijk actueel is, waren de deskundigen bereid om deel te nemen aan het onderzoek. Zij hebben waardevolle input geleverd. Ook de bereidheid onder gemeentelijke medewerkers voor het interview was groot. Hoewel dit vooral verklaard kan worden doordat ik de medewerkers persoonlijk ken. Het voordeel hiervan is dat de methodiek daardoor bij drie verschillende gemeenten en bij een negental medewerkers kon worden ingezet. Om te voorkomen dat de survey voor de medewerkers te veel tijd in beslag zou nemen waardoor het interview niet binnen de gestelde 1,5 uur kon worden afgerond, is eerst de survey getest door een willekeurige medewerker op tijdsduur. Hieruit bleek dat de complete survey kon worden getest. Vervolgens zijn de surveyvragen aangepast na het eerste interview, omdat hieruit bleek dat de survey qua structuur en scherpte aangepast diende te worden. Daarna is deze survey bij de overige acht medewerkers opnieuw getest wat waarschijnlijk heeft

geresulteerd in minder opmerkingen dan wanneer de survey niet op voorhand zou zijn aangescherpt.

Bij twee interviews met de deskundigen is de tijdsduur voor het interview van 2,5 uur overschreden, waar bij één interview een vervolgafspraak is gepland en bij een ander interview de resterende vragen zijn gemaild. Oorzaak hierbij is waarschijnlijk dat bij deze interviews twee tot drie personen tegelijk werden geïnterviewd waardoor de doorlooptijd toenam. Op voorhand was het berekend op één persoon. Nadat bleek dat men intern meerdere personen wilden laten deelnemen ten gunste van het onderzoek, had ik de interviewtijd moeten verruimen. De vraag is dan alleen of men bereid is om zich 3,5 uur te laten interviewen. Dat zou in overleg moeten gaan met de betrokkenen.

Dit afstudeeronderzoek heeft inzicht gegeven over hoe een wetenschappelijk onderzoek kan verlopen. Hieruit is voor mij inzichtelijk geworden dat onderzoeksvragen nauw (c.q. klein) moeten worden gesteld. Dat heb ik in het begin als frustrerend ervaren omdat mijn oorspronkelijke onderzoeksvraag ambitieuzer was en zich richtte op het verklaren van de discrepantie tussen kennis en gedrag. Anderzijds was een te ambitieuze onderzoeksvraag niet haalbaar geweest binnen de onderzoeksperiode van 12 maanden. Wetenschappelijk onderzoek verloopt, naar mijn inziens, via kleine (niet te ambitieuze) stappen, waarbij het onderzoek echt waardevol is als vervolgonderzoeken worden uitgevoerd. Door die kleine stappen, en dus meerdere onderzoeken, is het mogelijk om van een beschrijvende onderzoeksvraag, via een verklarende onderzoeksvraag tot een toetsende onderzoeksvraag te komen, waardoor er uiteindelijk een getoetste methodiek is waarmee het informatiebeveiligingsbewustzijn kan worden gemeten. Voordat ik mijn onderzoek uitvoerde, was ik in de veronderstelling dat grotere stappen konden worden genomen om ‘versneld’ antwoord te krijgen op de oorspronkelijke onderzoeksvraag waarbij de discrepantie tussen kennis en gedrag zou worden verklaard.

7. Referenties

Bij de literatuurstudie zijn meerdere (wetenschappelijke) referenties geraadpleegd, maar deze zijn niet allemaal benoemd in hoofdstuk 3 waarin de resultaten staan uit de literatuurstudie. Alleen de belangrijkste resultaten zijn opgenomen.

Wetenschappelijke referenties

Aytes, K., & Conolly, T. (2003). *A Research Model for Investigating Human Behavior Related to Computer Security.* Paper presented at the AMCIS 2003 Proceedings.

Ceraolo, J. P. (1996). Penetration testing through social engineering. *Information Systems Security, 4*(4).

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29*(2), 196-207.

Da Veiga, A., Martins, N., & Eloff, J. H. P. (2007). Information security culture – validation of an assessment instrument. *Southern African Business Review, 11*(1), 147-166.

Dodge Jr., R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security, 26(1)*, 73-80.

Furnell, S. M., Gennatou, M., & Dowland, P. S. (2002). A prototype tool for information security awareness and training. *Logistics Information Management, 15*(5/6), 352-357.

Goes, van der L. J. (2012). *Social engineering en de Limburgse gemeenten.* (Master in Business Process Management & IT), Open Universiteit Nederland. Retrieved from http://dspace.ou.nl/bitstream/1820/4578/1/INF_20121211_Goes.pdf

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security, 16*(4), 377-397.

Koroliov, V., Turesson, M., & Brolin, O. (2009). *What is your password?* (Bachelor Thesis in Informatica), Jönköping University.

Kruger, H. A., Drevin, L., & Steyn, T. (2006). *A framework for evaluating ICT security awareness*. Paper presented at the Proceedings of the ISSA 2006 from Insight to Foresight Conference, Balalaika Hotel, Sandton, South Africa.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security, 25*(4), 289-296.

Neys, C. (2003). *It'ers, regels en security awareness.* (Master in Security in Information Technology), Technische Universiteit, Eindhoven. Retrieved from http://www.pvib.nl/scripties

Silva, L., Menezes, S., & Costa, A. P. C. S. (2012). *A model for evaluating information security with a focus on the user*. Paper presented at the Mediterranean Conference on Information Systems (MCIS) 2012 Proceedings.

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

Siponen, M. T. (2001). Five dimensions of information security awareness. *Computers and Society 31*(2), 24-29.

Siponen, M. T., & Karjalainen, M. (2011). Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches. *Journal of the Assocation for Information Systems, 12*(8), 518-555.

Stacey, T. R. (1996). The information security program maturity grid. *Information System Security, 5*(2), 22-34.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviours. *Computers and Security, 24(2)*, 124 – 133.

Thomson, K. L., & Solms, R. v. (2006). Towards an information security competence maturity model. *Computer Fraud & Security, 2006*(5), 11-15.

Niet-wetenschappelijke referenties

Blankena, F. (2015). Digibeet kan geen geuzennaam meer zijn - Twee jaar Taskforce Bestuur en Informatieveiligheid Dienstverlening. Retrieved 29-04, 2015, from http://ibestuur.nl/partner-ictu/digibeet-kan-geen-geuzennaam-meer-zijn

IBD. (2013). Strategische Baseline Informatiebeveiliging Nederlandse Gemeenten. Den Haag: KING.

ISO/IEC. (2014). 27000:2014 *Information technology - Security techniques - Information security management systems - Overwiew and vocabulary*. Geneve: ISO.

Jorritsma-Lebbink, A. (2013). Aanbiedingsbrief: Resolutie Informatieveiligheid, randvoorwaarde voor de professionele gemeente. Retrieved 17-12, 2014, from http://www.vng.nl/files/vng/brieven/2013/20131031_ledenbrief_resolutie-informatieveiligheid-randvoorwaarde-voor-de-professionele-gemeente.pdf

Taskforce_BID. (2014a). Factsheet van de Campagne iBewustzijn Overheid. Retrieved 30-01, 2015, from http://www.taskforcebid.nl/inspiratie/campagne-ibewustzijn-overheid/

Taskforce_BID. (2014b). Gouden Regels. Retrieved 30-01, 2015, from https://www.ibewustzijnoverheid.nl/aanbod/gouden-regels/

Taskforce_BID, & Ministerie_BZK. (2014). Campagne iBewustzijn Overheid. Retrieved 30-01, 2015, from http://www.taskforcebid.nl/inspiratie/campagne-ibewustzijn-overheid/

Vennix, J. (2006). *Theorie en praktijk van empirisch onderzoek*. Harlow: Pearson Education Limited.

VNG. (2013a). Resolutie: Informatieveiligheid, randvoorwaarde voor de professionele gemeente. Retrieved 03-12, 2014, from http://www.vng.nl/files/vng/brieven/2013/attachments/20131031_resolutie-informatieveiligheid.pdf

VNG. (2013b). Toelichting op resolutie: Informatieveiligheid, randvoorwaarde voor de professionele gemeente. Retrieved 17-12, 2014, from http://www.vng.nl/files/vng/brieven/2014/attachments/20140729_toelichting_resolutie.pdf

Bijlage 1 Begrippen en definities

Begrijpelijk *(aspect van effectief)*
Het model is eenvoudig toe te passen. De vragen en antwoordcategorieën uit de survey, welke zijn afgeleid van het model, zijn eenvoudig en helder voor de personen die de vragen moeten beantwoorden. Dit uit zich doordat de vragenlijst zelfstandig kan worden ingevuld zonder dat de vragen en antwoordcategorieën uitgelegd moeten worden.

Bruikbaar *(aspect van effectief)*
Het model en de vragenlijst is gebruiksvriendelijk en eenvoudig toe te passen door de onderzoeker binnen een willekeurige Nederlandse gemeente. De gegeven antwoorden zijn voor de onderzoeker eenduidig en direct te kwantificeren, waardoor resultaten gelijk kunnen worden geanalyseerd per dimensie (kennis, houding en gedrag) en gedragsrisico, zodat inzicht is in het informatiebeveiligingsbewustzijnniveau.

CISO
De Chief Information Security Officer (CISO) is op concernniveau verantwoordelijk voor de informatiebeveiliging binnen een organisatie en stuurt de informatiebeveiligingsfuncties op het lagere niveau aan.

Correct *(te meten aspect uit probleemstelling)*
Het model meet gedragsrisico's die voortvloeien uit de BIG, en de surveyvragen zijn hieruit afgeleid. Tevens zijn surveyvragen afgeleid uit drie belangrijke elementen die uit de literatuurstudie voortkomen. Deze elementen houden in dat medewerkers weten:

- wat bedrijfsgevoelige activa zijn;
- welke risico's en dreigingen hiervoor gelden en wat de gevolgen hiervan zijn;
- welke middelen er zijn om deze activa te beschermen, waarbij zij deze middelen kunnen vinden om toe te passen (zoals procedures) en deze ook bruikbaar vinden.

Effectief *(te meten aspect uit probleemstelling)*
Het model is begrijpelijk, bruikbaar en haalbaar.

Eindgebruikers
Medewerkers binnen een organisatie die met informatie(middelen) werken.

Haalbaar *(aspect van effectief)*
De verhouding tijdsduur versus het aantal vragen is voor de onderzoeker en de personen die de surveyvragen beantwoorden acceptabel, waardoor de betrouwbaarheid van de antwoorden zoveel mogelijk wordt gewaarborgd.

Informatie
Informatie is een *asset* dat voor de bedrijfsvoering van een organisatie essentieel is. Informatie komt voor in de digitale en analoge vorm, maar ook in de vorm van kennis.

Informatiebeveiliging
Kruger & Kearney (2006) en ISO/IEC 27000 (2014) geven aan dat het bij informatiebeveiliging gaat om het waarborgen van de betrouwbaarheidsaspecten van de informatie, die bestaan uit:

- vertrouwelijkheid: informatie is niet toegankelijk voor ongeautoriseerde individuen, entiteiten of processen;
- integriteit: informatie is accuraat, juist en compleet;
- beschikbaarheid: de informatie is te benaderen en te gebruiken door geautoriseerden.

Informatie kan zich hierbij voordoen in de vormen analoog, digitaal en kennis (alleen opgeslagen en vastgelegd in de hoofden van een of meerdere personen). Deze definitie maakt duidelijk dat informatiebeveiliging dus niet alleen om techniek gaat, zoals hardware en systemen, maar ook om houding en gedrag. Met techniek is veel te regelen, maar vertrouwelijke informatie kan bijvoorbeeld altijd nog worden gelekt door medewerkers die vanuit hun functie geautoriseerd zijn tot deze informatie (bewust of onbewust door bijvoorbeeld social engineering).

Informatiebeveiligingsbeleid
Een document dat weergeeft op welke wijze informatiebeveiliging binnen een organisatie wordt vormgegeven, met welk doel, binnen welke kaders en hoe de verantwoordelijkheden zijn belegd.

Informatiebeveiligingsbewustzijn
Siponen (2000) omschrijft de term informatiebeveiligingsbewustzijn als een toestand waarin gebruikers in een organisatie op de hoogte zijn van de missie van informatiebeveiliging, en dit ook (willen) uitdragen.
Hierbij onderkent elke medewerker (Information Security Forum (ISF) in Kruger & Kearney, 2006):

- wat het belang is van informatiebeveiliging;
- in welke mate het van belang is voor de organisatie;
- wat hun taken en verantwoordelijkheden;
- en handelt hier ook naar.

Kruger & Kearney (2006) geven aan dat het erom gaat dat dit gedrag past in een omgeving van informatiebeveiliging. Het doel van het werken aan het informatiebeveiligingsbewustzijn is om gebruikers bewust te laten maken van de doelen van informatiebeveiliging en hen hieraan te laten committeren (Siponen, 2001).

Methode (c.q. methodiek)
De definitie van methode kan omschreven worden als een richtlijn voor het oplossen van een specifiek probleem, door het gebruik van modellen en andere instrumenten (Andersen in Koroliov et al., 2009). (Ongetwijfeld zijn er nog andere omschrijvingen voor deze definitie). Het antwoord op de hoofdvraag moet namelijk leiden tot een instrument waarmee het informatiebeveiligingsbewustzijn en bijbehorend gedrag kan worden gemeten bij medewerkers van Nederlandse gemeenten. De woorden methodiek en model liggen in elkaars verlengde, waarbij in dit verslag met model een visuele weergave van de methodiek wordt bedoeld.

Penetratietest (pentest)
Een pentest is een methode om de controls in de informatiebeveiliging van buitenaf te omzeilen en op zoek te gaan naar zwakke plekken in deze controls (Ceraolo, 1996).

Social engineering
Via social engineering probeert een kwaadwillende het vertrouwen te winnen van een medewerker om toegang te krijgen tot afgeschermde informatie(systemen) (Ceraolo, 1996).

Volledig *(te meten aspect uit probleemstelling)*
Het model meet de 10 belangrijkste gedragsrisico's van medewerkers bij Nederlandse gemeenten.

Bijlage 2 Vragenlijst t.b.v. interview met vier deskundigen

Introductie bestaande uit:

- Voorstelronde;
- Aangeven dat ik onderzoek doe naar de wijze waarop het informatiebeveiligingsbewustzijn kan worden gemeten bij medewerkers van Nederlandse gemeenten;
- Verloop van het interview bespreken;
- Anonimiteit en vertrouwelijkheid bespreken;
- Aangeven dat er een verslag wordt opgesteld, dat na afloop binnen een week aan hen wordt gestuurd om deze goed te keuren voordat de resultaten uit het interview worden verwerkt;
- Doel van onderzoek toelichten en aangeven dat er een model is ontwikkeld dat het informatiebeveiligingsniveau van medewerkers meet binnen een gemeentelijke organisatie;
- Toelichten dat het hierbij gaat om de componenten kennis, houding en gedrag, en uitleggen wat met deze componenten wordt bedoeld;
- Aangeven dat de bovengenoemde componenten gemeten worden met het model middels een vragenlijst en dat dit interview bedoeld is om te kijken of het model volledig en correct is;
- Toelichten dat het model wetenschappelijk is onderbouwd en dat de basis komt van het model van Kruger en Kearney (2006);
- Het model van Kruger en Kearney (2006) laten zien en toelichten;
- Vervolgens het model presenteren dat ontworpen is om het bewustzijn van medewerkers bij Nederlandse gemeenten te meten. Aangeven dat de inhoud is gebaseerd op de campagne iBewust Overheid, omdat deze aansluit op de BIG. Het model wordt in zijn geheel doorlopen;
- Toegelicht wordt wat met de resultaten uit de meting (survey) kan worden gedaan;
- Starten met het interview en vragen of het volledig is en of er zaken worden gemist.

Semigestructureerd interview
Onderstaande vragen stellen en hierop doorvragen indien relevant

<u>Volledig</u>
Vragenlijst om te beoordelen of de methodiek ‘volledig’ is.

Volledig is in de definitielijst gedefinieerd als:
Het model meet de 10 belangrijkste gedragsrisico’s van medewerkers bij Nederlandse gemeenten.

Deze definitie benoemen en vervolgens onderstaande vragen stellen:

1. Welke ontwikkelingen neemt u waar die van invloed zijn op de gemeentelijke informatiebeveiliging?
    a. Internationaal:
    b. Landelijk:
    c. Lokaal:

2. Welke risico's brengt dit met zich mee op de gemeentelijke informatiebeveiliging waar het gedrag van medewerkers invloed op heeft?
3. Wat zijn volgens u de belangrijkste gedragsrisico's van medewerkers bij Nederlandse gemeenten? *(Vraag naar toelichting en de onderbouwing van het antwoord)*
4. Hoe zou uw top 10 eruit zien op belangrijkste gedragsrisico's eruit zien? *(Vraag naar onderbouwing van het antwoord)*
5. Wat is uw conclusie ten aanzien van de volledigheid van het voorgelegde model? *(Indien het model gewijzigd moet worden, welke wijzigingen moeten dan plaats vinden en wat is hiervoor de onderbouwing?)*

<u>Aspect 'Correct'</u>
Vragenlijst om te beoordelen of de methodiek correct is.

Correct is in de definitielijst gedefinieerd als:
Het model meet gedragsrisico's die voortvloeien uit de BIG, en de surveyvragen zijn hier van uit afgeleid. Tevens zijn surveyvragen afgeleid uit drie belangrijke elementen die uit de literatuurstudie voortkomen, waarbij medewerkers dienen te weten:

- *wat bedrijfsgevoelige activa zijn;*
- *welke risico's en dreigingen hiervoor gelden en wat de gevolgen hiervan zijn;*
- *welke middelen er zijn om deze activa te beschermen, waarbij zij deze middelen kunnen vinden om toe te passen (zoals procedures) en deze ook bruikbaar vinden.*

Deze definitie benoemen en vervolgens onderstaande vragen stellen:
Onderstaande vier vragen alleen stellen aan betrokkenen bij de campagne iBewust Overheid:

1. Op welke wijze is de campagne iBewust Overheid geschikt gemaakt voor gemeenten?
2. Wie/Welke partijen hebben de 10 gouden regels opgesteld?
3. Hoe zijn déze 10 gouden regels gekomen?
4. In hoeverre verhouden de 10 gouden regels zich tot de BIG?

Voor allen:
Het model van links naar rechts doorlopen waarbij de volgende vragen worden gesteld:

1. In hoeverre meten de gouden regels de thema's?
2. In hoeverre meten de subfactoren de gouden regels?
3. In hoeverre meet de vraag de gouden regel?
4. In hoeverre houden de kennisvragen rekening met de drie elementen uit de literatuur?
5. In hoeverre zijn de kennis-, houding- en gedragsvragen per subfactor in lijn met elkaar gebracht?
6. Moeten meer vragen (en zo ja welke) gesteld worden om een specifieke gouden regel te meten binnen een specifieke dimensie om een goede indicatie te krijgen van het bewustzijnniveau – rekeninghoudend met de effectiviteit van de vragenlijst (totaal aantal vragen / bereidwilligheid om zoveel vragen te beantwoorden)?
7. Wat is uw conclusie ten aanzien van de correctheid van de vragenlijst?

Aspect ‘Bruikbaarheid

Vragenlijst om te beoordelen of de methodiek bruikbaar is voor de onderzoeker. Bij het interview wordt hen gevraagd een uitspraak te doen over de verwachte bruikbaarheid van het model.

Bruikbaar (aspect van effectief) is in de definitielijst gedefinieerd als:
Het model en de vragenlijst is gebruiksvriendelijk en eenvoudig toe te passen door de onderzoeker binnen een willekeurige Nederlandse gemeente. De gegeven antwoorden zijn voor de onderzoeker eenduidig en direct te kwantificeren, waardoor resultaten gelijk kunnen worden geanalyseerd per dimensie (kennis, houding en gedrag) en gedragsrisico, zodat inzicht is in het informatiebeveiligingsbewustzijnniveau.

Deze definitie benoemen en vervolgens onderstaande vraag stellen:

1. Als u het model bekijkt vanuit het oogpunt van de onderzoeker, in hoeverre oogt dit model dan toepasbaar in termen van gebruikersvriendelijk en eenvoudig? Hiermee wordt bedoeld dat een onderzoeker weinig voorbereidingstijd nodig heeft om het model te begrijpen en toe te passen.
2. In hoeverre is het model toepasbaar op alle Nederlandse gemeenten? (Zijn alle elementen uit het model van toepassing op alle Nederlandse gemeenten?)
3. Toelichten hoe resultaten worden gekwantificeerd en vervolgens de vraag stellen: In welke mate denkt u dat de resultaten eenduidig en direct kunnen worden gekwantificeerd?
4. In hoeverre bent u van mening dat de gekwantificeerde resultaten gelijk kunnen worden geanalyseerd per dimensie, factor en thema? (Geven de gekwantificeerde resultaten direct inzicht in het informatiebeveiligingsniveau, zonder eerst deze resultaten te moeten verwerken voordat deze geanalyseerd kunnen worden?)
5. Wat is uw conclusie ten aanzien van de bruikbaarheid van dit model – gezien vanuit het oogpunt van de onderzoeker / de persoon die het model moet toepassen in de praktijk?

Bijlage 3 Uitnodigingsbrief voor vier deskundigen

Onderzoek naar methodiek om het informatiebeveiligingsbewustzijn van medewerkers bij gemeenten te kunnen meten

Verzoek om u als deskundige op het gebied van informatiebeveiliging te mogen interviewen om de kwaliteit van het ontwikkelde model te valideren

Dhr. Y. Lammerts van Bueren
XXX

m. XXX
t. XXX

Organisatienaam
Ter attentie van dhr./mevr.
Adres
Postcode + vestigingsplaats

6 mei 2015

Geachte heer/mevrouw,

In het kader van mijn masterthesis voor mijn opleiding Business Process Management & IT aan de Open Universiteit heb ik een model ontwikkeld waarmee het informatiebeveiligingsbewustzijn bij medewerkers van Nederlandse gemeenten kan worden gemeten. Een dergelijke methodiek is hiervoor nog niet voorhanden maar wel wenselijk gezien de aangenomen resolutie ‘Informatieveiligheid, randvoorwaarde voor een professionele gemeente’ op de buitengewone algemene ledenvergadering van de VNG op 29 november 2013. De resolutie bepaalt dat gemeenten aantoonbaar in control moeten zijn op het gebied van informatieveiligheid conform de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Een belangrijke factor hierin is de wijze waarop medewerkers het informatiebeveiligingsbeleid naleven (gedragscomponent).

Het ontwikkelde model meet het informatiebeveiligingsbewustzijn van medewerkers, dat bestaat uit de componenten kennis, houding en gedrag. Dit model is specifiek ontwikkeld voor medewerkers van Nederlandse gemeenten en dient gevalideerd te worden. Hierbij wordt gekeken of het model correct en volledig is.

Specifieke tekst voor deskundige CIP
Ik zou het waarderen als ik dit model aan u kan voorleggen als deskundige binnen het CIP op het gebied van informatiebeveiligingsbewustzijn, aangezien het CIP het expertisecentrum is voor informatiebeveiliging van, voor en door overheidsorganisaties. Uw CIP-collega Ad Reuijl heeft u hiervoor voorgedragen. Aan de hand van een maximaal 2,5 durend interview op uw werklocatie zal ik het model toelichten en voorleggen. Als het model gevalideerd en definitief is, dan zal het model en de kennis hiervan uiteraard worden gedeeld (openbaar worden gemaakt), zoals het CIP nastreeft als expertisecentrum.

Specifieke tekst voor CISO Edam-Volendam
Aangezien ik als onderzoeker tevens als CISO werkzaam ben bij een andere gemeente, is het waardevol als er een review op wordt gedaan door een collega CISO van een andere gemeente die invulling geeft aan de VNG-resolutie en tegelijk al werkt aan het informatiebeveiligingsbewustzijn van haar gemeente. De gemeente Edam-Volendam voldoet aan dit profiel en daarom zou ik graag aan de hand van een maximaal 2,5 durend interview op uw werklocatie dit model willen toelichten en aan u willen voorleggen ter validatie.

Specifieke tekst voor deskundige Informatiebeveiligingsdienst voor gemeenten (IBD)
De IBD is het landelijke orgaan dat gemeenten adviseert en ondersteunt op het gebied van informatiebeveiliging conform de BIG. Het is daarom waardevol als ik het model aan u kan voorleggen om te valideren. Aan de hand van een maximaal 2,5 durend interview op uw werklocatie zal ik het model toelichten en voorleggen. Als het model gevalideerd en definitief is, dan zal het model en de kennis hiervan uiteraard worden gedeeld (openbaar worden gemaakt) op de community van de IBD, zodat alle gemeenten het model kunnen gebruiken.

Specifieke tekst voor persoon die betrokken was bij het opzetten van de iBewustzijn campagne van de overheid.
Het ontwikkelde model is mede gebaseerd op de iBewustzijncampagne van de overheid waar u bij betrokken was. Daarom acht ik het waardevol om dit model aan u voor te leggen ter validatie. Aan de hand van een maximaal 2,5 durend interview op uw werklocatie zal ik het model toelichten en voorleggen.

Het vertrouwelijke karakter van dit interview wordt uiteraard gewaarborgd en met u voorafgaand aan het interview besproken. Tevens wordt van het interview een verslag uitgewerkt dat aan u wordt voorgelegd voordat de resultaten uit het interview worden meegenomen in het onderzoek.

Ik hoop dat u het leuk vindt om bij te dragen aan de ontwikkeling van dit model. Behalve dat het model wordt beoordeeld of het correct en volledig is, wordt het model ook beoordeeld op effectiviteit door het toe te passen bij een select aantal medewerkers van drie verschillende gemeenten.

Indien u geïnteresseerd bent in het uiteindelijke onderzoeksrapport, dan zal ik deze u ter zijne tijd toesturen (verwachting is september 2015).

Graag hoor ik van u of we een afspraak in mei/juni kunnen plannen voor het interview.
Indien u vragen of nadere informatie over dit onderzoek wil hebben, dan kunt u mij bereiken op telefoonnummer XXX of een email versturen naar XXX.

Met vriendelijke groet,

Youri Lammerts van Bueren

Bijlage 4 Interviewverslag IBD

Anita van Nieuwenborg
Teamleider Informatiebeveiligingsdienst voor gemeenten (IBD)

Sonja Kok
Economisch psycholoog, gewerkt voor IT en Telecom- bedrijven, was verantwoordelijk voor de positionering, communicatie en woordvoering bij de Taskforce Bestuur en Informatieveilheid Dienstverlening en is woordvoerder en communicatieadviseur bij de IBD.

Semigestructureerd interview
Onderstaande vragen stellen en hierop doorvragen indien relevant

<u>Volledig</u>
Vragenlijst om te beoordelen of de methodiek 'volledig' is.

1. Welke ontwikkelingen neemt u waar die van invloed zijn op de gemeentelijke informatiebeveiliging?
    a. Internationaal:
    b. Landelijk:
    c. Lokaal:

    Antwoord
    - Visiebrief minister Plasterk omtrent een digitale overheid in 2017;
    - Meer digitalisering/digitaal werken;
    - Meer ketengericht werken, zoals decentralisatie in het sociale domein;
    - De gemiddelde gemeentelijke medewerker is niet opgegroeid met digitale informatie. Er zijn weinig gedragsregels omtrent de wijze waarop zij met digitale informatie moeten omgaan. Daarentegen zorgt verjonging van medewerkers bij gemeenten voor een andere benadering. Zij groeien op in een digitaal tijdperk, waarin zij gewend zijn dat data open is en dat gegevens gedeeld worden. Tel hierbij de 'onbevangenheidt' van medewerkers op (uitgaan van het goede vertrouwen);
    - Wet- en regelgeving is hoofdzakelijk gebaseerd op het papieren tijdperk. Deze regelgeving houdt nog onvoldoende rekening met de digitale situatie (loopt acht op de praktijk);
    - De Wet Openbaarheid Bestuur (WOB) is gericht op het openbaar maken van bestuurlijke informatie, maar vanuit technisch/ICT perspectief wil je dit niet in verband met de risicogevoeligheid (wetgeving houdt hier nog onvoldoende rekening mee);
    - Big data: steeds meer (overheids)gegevens worden aan elkaar gekoppeld;
    - Informatiebeveiliging krijgt veel (landelijke) aandacht momenteel. Informatiebeveiliging gaat snel en medewerkers weten nog niet altijd wat er nu allemaal mogelijk is en welke beveiligingsrisico's specifiek gedrag met zich meebrengt;
    - Er komt steeds meer privacybescherming (strengere regelgeving op privacyvlak – zowel op landelijk als Europees niveau). Organisaties moeten hierdoor steeds meer maatregelen treffen, waardoor het onwerkbaar wordt (kan worden);

- Bestuurders zijn gericht op bestuurlijke zaken, maar deze zaken zijn vaak niet gericht op de digitale ontwikkelingen/mogelijkheden (zoals de impact die de gemeente Haren ondervond doordat een bewoner abusievelijk via social media iedereen uitnodigde voor haar 16-jarige verjaardag / lees project-X);
- Toename van cybercriminaliteit.

2. Welke risico's brengt dit met zich mee op de gemeentelijke informatiebeveiliging waar het gedrag van medewerkers invloed op heeft? (tegelijk beantwoord met de vragen 3 en 4)

   Antwoord
   - Identiteitsfraude;
   - Verlies / uitlekken data;
   - Misbruik en inkijken van gegevens; men hoeft niet meer een fysieke kast op te zoeken – de meeste data is digitaal. Men moet vertrouwelijk omgaan met data (ongeacht of dit thuis is of op het werk);
   - Risico big data: de gekoppelde data verschillend uitgelegd worden, vanuit verschillende doelen (vanuit pensioen, zorg, etc). Dit betekent dan ook dat men voorzichtig moet zijn met het delen van data.

   Dit komt mede door:
   - Volggedrag: ik doe het, want hij doet het ook. Men kan de risico's en de impact van eigen handelen onvoldoende inschatten – is niet altijd voldoende bewust van de gevaren;
   - Onwerkbare situatie: door de vele maatregelen kunnen zaken onwerkbaar worden, dan wel gaat men eromheen werken;
   - Aanspreken: mensen durven elkaar niet aan te spreken omdat zij geen betweter willen zijn;
   - Online communicatie: mensen communiceren steeds meer op social media over wat zij hebben gedaan op hun werk en waaraan zij werken.

3. Wat zijn volgens u de belangrijkste gedragsrisico's van medewerkers bij Nederlandse gemeenten?

   Antwoord
   Zie vraag 2.

4. Hoe zou uw top 10 eruit zien op belangrijkste gedragsrisico's eruit zien?

   Antwoord
   De onderwerpen die in ieder geval gemeten moeten worden zijn vermeld in het antwoord op vraag 2.

5. Wat is uw conclusie ten aanzien van de volledigheid van het voorgelegde model?

   Antwoord
   De 10 gouden regels, zoals deze in het model zijn opgenomen dekken de belangrijkste risico's. Identiteitsfraude mag explicieter in het model terugkomen. Daarbij, al vooruitkijkend op de relatie tussen de gouden regels en de vier thema's: de gouden gedragsregels (belangrijkste gedragsrisico's) zijn in

werkelijkheid niet altijd binnen één thema terug te voeren, zoals het model suggereert. In het huidige model worden de gouden regels gekoppeld aan één thema, waardoor een gedragsrisico niet altijd volledig de lading dekt. Zo is de gouden regel om vertrouwelijk om te gaan met informatie niet specifiek gebonden aan het thema 'Binnen'. Dit geldt ook voor als je onderweg werkt (in de trein), op terras, thuis of elders buiten de kantoormuren.
Kortom, de gouden regels dekken de grootste lading, maar worden qua volledigheid onterecht geremd doordat zij aan één thema zijn gekoppeld.

Opmerking: bewustzijn laat zich moeilijk meten en is moeilijk te meten. 95% van de mensen weten wat van hen wordt verwacht - los ervan of het anoniem is. De houding wordt beïnvloed door de mate waarin zij worden aangemoedigd/gestimuleerd om de gewenste houding te laten zien.

Aspect 'Correct'
Vragenlijst om te beoordelen of de methodiek correct is.

8. In hoeverre meten de gouden regels de thema's?

   Antwoord
   - Thema's: deze moeten van gelijke orde zijn. De thema's Binnen en Buiten zijn van gelijke orde. De thema's Beleid, Achter je scherm en in de Cloud zijn van een ander niveau en onlosmakelijk met elkaar verbonden, wat het lastig maakt de thema's op te delen. De toevoeging van het thema Beleid aan de bestaande vier thema's uit de iBewust Overheid campagne is terecht;
   - Er zit een zekere hiërarchie in het model. Het beleid en je rol daarbinnen kennen bepaalt verder hoe ik mij binnen de andere thema's ga gedragen. Het beleid vormt de input;
   - De gouden regels kunnen de thema's niet overlappen, omdat deze nu aan één thema zijn gekoppeld. Gouden regels zijn terug te voeren op meerdere thema's;
   - De gouden regels 3 en 4 overlappen elkaar.

   Kortom: De relatie tussen de thema's en de gouden regels is niet eenduidig, waardoor onduidelijk is of de gouden regels de thema's volledig meten.

9. In hoeverre meten de subfactoren de gouden regels

   Antwoord
   - Gouden regel 3 'Voorkom misbruik en diefstal' moet aangescherpt worden door:
     - Subfactor 'Hanteer clear desk en clear screen' op te splitsen om het verschil tussen deze twee aspecten duidelijker tot uiting te krijgen;
     - Aanvullend op subfactor 'Houd wachtwoorden voor jezelf' ook subfactor 'Verander wachtwoord met regelmaat' op te nemen;
   - Gouden regel 4 'Ga vertrouwelijk om met informatie aanscherpen door:
     - Subfactor 'Houd je aan de geheimhoudingsplicht' te laten vervallen. Is te algemeen/globaal;
     - Subfactor toevoegen 'Praat niet onnodig met anderen over je werk';
   - Gouden regel 5 'Meld incidenten' vereenvoudigen door:

    - Subfactor ‘Meld technische incidenten bij de ICT-helpdesk’ en de subfactor ‘Meld overige incidenten aan je direct leidinggevende als het mogelijk is dat vertrouwelijke informatie in handen is gekomen van onbevoegden’ samen te voegen. De vraag is of mensen het verschil tussen een technisch en overig incident scherp hebben – en of zij weten wat een incident is. Subfactor opnemen als ‘Meld verdachte zaken altijd aan je leidinggevende en de ICT-helpdesk’;
- Gouden regel 6 ’Zorg voor optimale beveiliging van mobiele apparaten met zakelijke informatie’ aanscherpen door:
    - Subfactor ‘Gebruik geen gratis wifi’ te verruimen. Gratis wifi kan gebruikt worden, maar men moet vanuit risicoperspectief weten (bewustzijn) wat wel en niet met gratis wifi kan worden gedaan;
- Gouden regel 7 ‘Werk voorzichtig met vertrouwelijke informatie buiten de kantoormuren’ aanscherpen door:
    - Subfactor ‘Neem vertrouwelijke informatie alleen mee buiten de kantoormuren als het strikt noodzakelijk’ niet alleen betrekking te laten hebben op papieren dossiers, maar ook informatie die op mobiele devices staat;
- Gouden regel 8 ‘Ga voorzichtig om met verdachte telefoontjes, e-mails en inlogschermen op internetsites’ kan samengevoegd worden met gouden regel 9 ‘Ga voorzichtig om met verdachte internetsites’. Deze zijn van gelijk niveau en meten in feite hetzelfde, namelijk het voorzichtig omgaan met verdachte digitale zaken. Daarbij de gouden regel aanvullen met ‘en bij twijfel niet verder gaan’;
- Gouden regel 9 ‘Ga voorzichtig om met verdachte internetsites:
    - Weten medewerkers wat verdachte internetsites zijn?;
    - Subfactor ‘Zorg voor een gedegen en up to date virusscanner en firewall op je eigen apparaten, als je deze voor zakelijke doeleinden gebruikt’ aanscherpen naar ‘Zorg altijd voor een gedegen en up to date virusscanner en firewall op je eigen apparaten, zeker als je deze ook voor zakelijke doeleinden gebruikt.

10. In hoeverre meet de vraag de gouden regel?

    Antwoord
    - Niet specifiek één voor één doorlopen. Doordat de gouden regels en subfactoren aangescherpt moeten worden, moeten ook de vragen aangepast worden.

11. In hoeverre houden de kennisvragen rekening met de drie elementen uit de literatuur?

    Antwoord
    - De kennisvragen houden rekening met een van de drie elementen. Vraag is wel hoe je sociale wenselijkheid (zo veel) mogelijk uitsluit op vragen als ‘Weet je wat het risico/impact/gevolg is van …..’.

12. In hoeverre zijn de kennis-, houding- en gedragsvragen per subfactor in lijn met elkaar gebracht?

    Antwoord
    - Zie vraag 3.

13. Moeten meer vragen (en zo ja welke) gesteld worden om een specifieke gouden regel te meten binnen een specifieke dimensie om een goede indicatie te krijgen van het bewustzijnniveau – rekeninghoudend met de effectiviteit van de vragenlijst (totaal aantal vragen / bereidwilligheid om zoveel vragen te beantwoorden)?

    Antwoord
    - Voor de bereidwilligheid moeten er niet te veel vragen gesteld worden. Daarnaast brengt een grote lijst aan vragen het risico met zich mee dat medewerkers de vragenlijst gaan afraffelen. Er hoeven dus zeker niet meer vragen gesteld te worden om een specifieke gouden regel te meten. Het aantal subfactoren per gouden regel is namelijk al voldoende.

14. Wat is uw conclusie ten aanzien van de correctheid van de vragenlijst?

    Antwoord
    - Het model dient op een aantal plekken aangescherpt te worden. In de basis is die correct, maar een aantal gouden regels en subfactoren moeten aangepast worden, en de relatie tussen de thema's en de gouden regels moeten opnieuw bekeken worden.

Aspect 'Bruikbaarheid'

Vragenlijst om te beoordelen of de methodiek bruikbaar is voor de onderzoeker. Bij het interview wordt hen gevraagd een uitspraak te doen over de verwachte bruikbaarheid van het model.

15. Als u het model bekijkt vanuit het oogpunt van de onderzoeker, in hoeverre oogt dit model dan toepasbaar in termen van gebruikersvriendelijk en eenvoudig? Hiermee wordt bedoeld dat een onderzoeker weinig voorbereidingstijd nodig heeft om het model te begrijpen en toe te passen.

    Antwoord
    - Het model 'an sich' oogt gebruiksvriendelijk en eenvoudig. Wel kunnen de gedragsregels vanuit verschillende perspectieven benaderd worden.

16. In hoeverre is het model toepasbaar op alle Nederlandse gemeenten? (Zijn alle elementen uit het model van toepassing op alle Nederlandse gemeenten?)

    Antwoord
    - De methodiek en de uiteindelijke inhoud kan van toepassing zijn op alle gemeenten, maar specifieke risico's, en in het verlengde specifieke subfactoren, hoeven niet op elke organisatie van toepassing te zijn. Dat is afhankelijk van de wijze waarop de organisatie werkt of hoe ver zij al zijn met digitalisering.

17. Toelichten hoe resultaten worden gekwantificeerd en vervolgens de vraag stellen: In welke mate denkt u dat de resultaten eenduidig en direct kunnen worden gekwantificeerd?

    Antwoord
    - Als heldere richtlijnen worden meegegeven over hoe de betekenis van de kolommen kennis, houding en gedrag geanalyseerd moet worden dan is dit mogelijk.

18. In hoeverre bent u van mening dat de gekwantificeerde resultaten gelijk kunnen worden geanalyseerd per dimensie, factor en thema? (Geven de gekwantificeerde resultaten direct inzicht in het informatiebeveiligingsniveau, zonder eerst deze resultaten te moeten verwerken voordat deze geanalyseerd kunnen worden?)

    Antwoord
    - De gekwantificeerde resultaten maken analyse mogelijk (onder voorwaarde van hetgeen dat als antwoord is gegeven bij vraag 3).

19. Wat is uw conclusie ten aanzien van de bruikbaarheid van dit model – gezien vanuit het oogpunt van de onderzoeker / de persoon die het model moet toepassen in de praktijk?

    Antwoord
    - Het model oogt bruikbaar en praktisch. Over de inhoud zijn wat opmerkingen – maar de inhoud is mede afhankelijk van de eigenschappen van de organisatie hoe je de inhoud vorm geeft en vanuit welk perspectief er naar de gouden regels wordt gekeken. Daarnaast staan er veel vragen. Het maximum aantal tijd dat ongeveer gevraagd kan worden van een medewerker die deelneemt aan de survey is 10 minuten.

Bijlage 5 Interviewverslag CIP

Jan Renshof

- Voorzitter (samen met Brenno de Winter) van de domeingroep Awareness van het CIP (Centrum Informatiebeveiliging en Privacybescherming)
- Hoofd van een samenwerkingsverband van de ministeries OCW, SZW en Financiën dat zich richt op integrale aanpak van veiligheid, integriteit en crisismanagement (VIC)

Semigestructureerd interview

Aspect 'Volledig'

Vragenlijst om te beoordelen of de methodiek 'volledig' is.

1. Welke ontwikkelingen neemt u waar die van invloed zijn op de gemeentelijke informatiebeveiliging?
   a. Internationaal:
   b. Landelijk:
   c. Lokaal:

   Antwoord
   - Tijd plaats en onafhankelijk werken;
   - Toenemende digitalisering;
   - Verschil in benadering tussen ouderen en jeugd;
   - Manier van werken verandert binnen organisaties. In de laatste 50 jaar is niet zo veel verandert in verhouding ten opzichte van de laatste 5 jaar;.
   - Rol vanuit de media is meer bepalend voor manier van werken – jongeren groeien hierin op (multitasken) en ouderen kost het meer energie om in deze beweging mee te gaan;
   - Er gaan meer taken en handelingen gepaard met het meer digitaal en tijds- en plaatsonafhankelijk werken;
   - De dreigingen veranderen. Vroeger kwamen deze meer vanuit intern, nu meer vanuit extern door de toenemende cybercriminaliteit (hacking, social engineering e.d.).

2. Welke risico's brengt dit mee op de gemeentelijke informatiebeveiliging waar het gedrag van medewerkers invloed op heeft?

   Antwoord
   - Mens is spil in organisatie en tegelijk zwakste schakel. Organisatie heeft vaak andere belangen en onvoldoende voor ogen dat er effectiever gewerkt kan worden via bewustzijn en opleiding;
   - Informatiebeveiliging wordt vaak met de mond beleden, maar niet in de praktijk afgedwongen, zoals verplichte modules volgen, die mede je functioneren bepalen. Dat wordt niet afgedwongen (onvoldoende commitment van hoger hand);
   - De organisatie staat onvoldoende stil om na te gaan of medewerkers voldoende mee kunnen gaan in al deze veranderingen;
   - Veel zaken zijn nieuw, systemen werken niet of onvoldoende en als iets uitvalt dan is het moeilijker te improviseren;

- Werkprocessen worden steeds ingewikkelder, waardoor de kans op fouten groter wordt en de kans op imagoschade toeneemt. Mensen worden hierin onvoldoende begeleid;
- Eenduidigheid raakt zoek. Veel complexer nieuwer veld waarin wordt gewerkt. Hierbij ontbreken richtlijnen ontbreken, en als deze er zijn dan weet men vaak niet hoe deze richtlijnen geïnterpreteerd moeten worden;
- Verschil in benadering ouderen en jongeren inzake privacy: jongeren hebben privacy minder helder op het netvlies. Zij delen al veel data online en benaderen dit vanuit een ander perspectief (gebruikersgemak). Ouderen zijn er gericht en gesteld op privacy, en delen of geven daarom niet snel persoonsgegevens;
- Informatiebeveiliging is nog onvoldoende ingebed in de processen, waardoor informatiebeveiliging (lees de CISO) vaak achter de feiten aanloopt en er minder efficiënt gewerkt wordt. Andere zaken hebben meer prioriteit dan informatiebeveiliging i.v.m. de werkdruk. Informatiebeveiliging moet meer ingebed worden in de processen.

3. Wat zijn volgens u de belangrijkste gedragsrisico's van medewerkers bij Nederlandse gemeenten?

   Antwoord
   - Het lekken van gegevens dat vervolgens misbruikt wordt (meer data online i.c.m. cybercriminaliteit ten behoeve van onder andere identiteitsfraude);
   - Het niet of te laat melden van incidenten, vanuit ander belangenperspectief;
   - Men kent vaak wel de belangrijkste gedragsvoorschriften maar gaat er op een andere manier mee om;
   - Medewerkers hebben veelal onvoldoende kennis om de gevolgen en risico's van hun eigen handelingen te kunnen inschatten voor het proces of de organisatie;
   - Documenten en andere zaken op het bureau onbeheerd achter laten, omdat zij hun collega's vertrouwen;
   - Elkaar niet aanspreken op gedrag als geconstateerd wordt dat een collega onjuist omgaat met informatie(middelen).

4. Hoe zou uw top 10 eruit zien op belangrijkste gedragsrisico's eruit zien?
   Antwoord
   De belangrijkste zijn bij vraag 3 genoemd.

5. Wat is uw conclusie ten aanzien van de volledigheid van het voorgelegde model?

   Antwoord
   De gouden regels zijn één voor één doorlopen. De belangrijkste gedragsrisico's staan erin. Ten aanzien van een aantal gouden regels worden de volgende opmerkingen gemaakt:
      - GR 2 'Laat geen onbevoegden toe in onze gebouwen en op onze werkplekken': Dit verschilt per organisatie. Vooral grote organisaties/gemeenten kennen de werkwijze dat men alleen het pand in komt als men zich kan legitimeren. Hierdoor geldt bijvoorbeeld bij het Rijk dat een toegangspas niet meer zichtbaar hoeft te worden gedragen. Bij het Rijk geldt een strenge toegangsbeveiliging. Daarnaast

is dit moeilijk af te dwingen of na te leven, waar onder het aanspreken van een onbekende doordat er steeds meer flexibel wordt gewerkt;
- Gouden regel 5 ‘Meld incidenten’: Vanuit verschillend handelingsperspectief en belangen worden bij lange na niet alle incidenten (tijdig) gemeld. Dit is afhankelijk van naar wie het incident uitstraalt. Daarnaast kunnen medewerkers vaak de impact van een incident niet inschatten. Diefstal van een mobiele device moet bijvoorbeeld altijd gemeld worden, zodat de gegevens op het device van afstand gewiped kunnen worden;
- Gouden regel 6 ‘Zorg voor optimale beveiliging van mobiele apparaten met zakelijke informatie’: Een van de subfactoren hierbij is dat bij reparatie of verkoop het (mobiele) apparaat altijd de gegevens op het apparaat gewist moeten worden. Bij het Rijk gebeurt dat altijd intern, waardoor een dergelijke subfactor niet altijd van toepassing hoeft te zijn op een specifieke organisatie;
- Gouden regel 7 ‘Werk voorzichtig met vertrouwelijke informatie buiten de kantoormuren’: Iedereen weet het wel, maar gaat er op een eigen manier mee om.
- Gouden regel 10 ‘Ben je bewust van de risico’s van clouddiensten en online communicatie’: Dat laatste gaat vooral over gedrag dat altijd geldt (niet alleen vanuit het perspectief van informatiebeveiliging). Er is twijfel of dat dan ook als gouden regel benoemt moet worden.

Overige opmerking: Het rijk kent ook 8 of 10 gouden regels: deze dekken de lading uit het model. Tevens gelden de gouden regels uit het model voor alle overheden.

Aspect ‘Correct’

Vragenlijst om te beoordelen of de methodiek correct is.

6. In hoeverre meten de gouden regels de thema’s?

   Antwoord
   - De vier thema’s worden gemeten door alle 10 de gouden regels

   Opmerking: Wat je vanuit organisatie krijgt aangereikt, daarvan moeten medewerkers ervan uitgaan dat het veilig is. Dat is de basis. Met informatiebeveiliging is het moeilijk iedereen te bereiken. Integrale beveiliging boeit niemand, totdat het misgaat.

7. In hoeverre meten de subfactoren de gouden regels

   Antwoord
   - Rekening houdend met de eerdere opmerkingen bij het aspect volledig, dekken de subfactoren de gouden regels. Zoals eerder opgemerkt, niet elke subfactor geldt voor elke organisatie. Het onbeheerd achter laten van printjes zou al niet kunnen als je alleen maar beveiligd kan printen (wat zeker bij een aantal organisaties geldt);
   - Je houden aan de geheimhoudingsplicht is breder dan alleen voor informatiebeveiliging. Het is de vraag of deze dan ook in dit model op deze wijze moet worden gemeten;

- Met betrekking tot het melden van incidenten: dit moet altijd gemeld worden aan de leidinggevende, ongeacht of het een technisch incident is of niet. De leidinggevende moet namelijk de impact en eventuele schade bepalen om de vervolgstappen te kunnen bepalen. De subfactoren kunnen beter gewijzigd worden in:
    - 1 Meld het incident;
    - 2 Inventariseer de eventuele impact en schade van het incident.

8. In hoeverre meet de vraag de gouden regel?

   Antwoord
   - De vragen zijn één voor één doorlopen en meten de gouden regels. Wel zijn er wat verbetervoorstellen en opmerkingen hierover:
       - Hoe meer je vraagt, hoe minder respons je waarschijnlijk krijgt;
       - Houdingsvragen mogen stelliger worden neergezet: ipv ik ben van mening dat toegangspassen aan niemand uitgeleend mogen worden → toegangspassen mogen niet uitgeleend worden;
       - De kennisvraag bij clear desk/clear screen: deze gaat alleen over clear screen, terwijl de houdingsvraag wel beide aspecten meet. Beter is het beide aspecten te meten gezien de subfactor;
       - De kennisvraag bij ‘houd wachtwoorden voor jezelf’: het delen van wachtwoorden hoeft niet alleen gevolgen te hebben voor burgers en dienstverlening, maar kan ook persoonlijke gevolgen hebben (bijvoorbeeld als iemand onder jou naar porno kijkt). Daarbij sluit de houdingsvraag hier niet op aan. Dit geldt overigens voor meerdere vragen waarin de gevolgen enkel zijn beperkt tot burgers en dienstverlening;
       - Houdingsvragen of allemaal positief of allemaal negatief formuleren. Deze staan nu door elkaar (zelfde vorm aanhouden);
       - Het gebruik van privé apparaten: dit is afhankelijk van het beleid van de organisatie of dit wordt toegestaan of niet;
       - De kennisvraag bij het doorvoeren van softwareupdates: er bij vermelden dat het gaat om de door de organisatie aangereikte softwareupdates. Dit heeft te maken dat de Baseline Informatiebeveiliging er vanuit gaat dat wat de organisatie aanreikt aan zijn medewerkers, dat dit veilig/verantwoord is. Dan moet een medewerker de updates krijgen aangereikt en deze moet hij dan ook doorvoeren;
       - Omtrent het gebruik van gratis wifi ten behoeve van webmail: dit kan ook algemener, waardoor het niet gaat om webmail maar bijvoorbeeld om internetbankieren;
       - Communiceer niet over zaken die schadelijk zijn voor je werkgever: dit kan ook over online zaken gaan, maar ook over het communiceren op andere plekken of bij andere gelegenheden (zoals in een samenzijn met journalisten in een kroeg om mee te borrelen, wat bij het Rijk vaker gebruikelijk is).

9. In hoeverre houden de kennisvragen rekening met de drie elementen uit de literatuur?

   Antwoord
   De kennisvragen houden rekening met de drie elementen.

10. In hoeverre zijn de kennis-, houding- en gedragsvragen per subfactor in lijn met elkaar gebracht?

    Antwoord
    De vraag is gelijk beantwoord bij vraag 3. Behoudens een paar kleine aanpassingen, zijn de vragen in lijn met elkaar.

11. Moeten meer vragen (en zo ja welke) gesteld worden om een specifieke gouden regel te meten binnen een specifieke dimensie om een goede indicatie te krijgen van het bewustzijnniveau – rekeninghoudend met de effectiviteit van de vragenlijst (totaal aantal vragen / bereidwilligheid om zoveel vragen te beantwoorden)?

    Antwoord
    Nee. Zoals eerder opgemerkt. Hoe meer je vraagt, hoe minder respons je waarschijnlijk krijgt.

12. Wat is uw conclusie ten aanzien van de correctheid van de vragenlijst?

    Antwoord
    Na wat kleine aanpassingen vanuit eerdere opmerkingen, is de lijst correct.

Aspect 'Bruikbaarheid

Vragenlijst om te beoordelen of de methodiek bruikbaar is voor de onderzoeker. Bij het interview wordt hen gevraagd een uitspraak te doen over de verwachte bruikbaarheid van het model.

13. Als u het model bekijkt vanuit het oogpunt van de onderzoeker, in hoeverre oogt dit model dan toepasbaar in termen van gebruikersvriendelijk en eenvoudig? Hiermee wordt bedoeld dat een onderzoeker weinig voorbereidingstijd nodig heeft om het model te begrijpen en toe te passen.

Antwoord
Jan is er positief over en geeft aan dat die zelfs ook bij andere overheden gebruikt kan worden. Je bent natuurlijk wel afhankelijk van het feit dat medewerkers hem invullen. Als tip geeft hij aan om het instrument niet uit te zetten bij alle medewerkers, maar in te zetten via een versnellingskamersessie, die ongeveer 3 maal wordt ingezet bij een groep van 15 personen achter een laptop. Eén persoon (de moderator) leidt de sessie vanaf zijn laptop en kan alles direct analyseren. Iedereen krijgt dezelfde vragen en in korte tijd (dagdeel) zijn alle gegevens en analyses dan ook voorhanden. Dan heb je representatief beeld, mits je mensen in de groepen hebt zitten die een dwarsdoorsnede vormen van de organisatie. Vaak vinden mensen het ook eervol om hieraan mee te doen en neemt de bereidwilligheid toe. Tevens is er ook de gelegenheid om vragen toe te lichten (vanuit de moderator of vanuit de medewerkers die de antwoorden geven).

14. In hoeverre is het model toepasbaar op alle Nederlandse gemeenten? (Zijn alle elementen uit het model van toepassing op alle Nederlandse gemeenten?)

    Antwoord
    - Kun je overal gebruiken, ook buiten gemeenten. ZBO's, Shell e.d.

15. Toelichten hoe resultaten worden gekwantificeerd en vervolgens de vraag stellen: In welke mate denkt u dat de resultaten eenduidig en direct kunnen worden gekwantificeerd?

    Antwoord
    Doordat de antwoorden gekwantificeerd zijn en te analyseren vanuit de verschillende dimensies, gouden regels en thema's, zijn de resultaten snel te analyseren.
    Opmerkingen:
        - Een survey kan een vertekend beeld geven, zeker als de respons minimaal is. Door vragen in te bouwen omtrent leeftijd, functie, en hoe lang je er al werkt, kunnen de gekwantificeerde resultaten beter geanalyseerd worden vanuit een andere context.

16. In hoeverre bent u van mening dat de gekwantificeerde resultaten gelijk kunnen worden geanalyseerd per dimensie, factor en thema? (Geven de gekwantificeerde resultaten direct inzicht in het informatiebeveiligingsniveau, zonder eerst deze resultaten te moeten verwerken voordat deze geanalyseerd kunnen worden?)

    Antwoord
    Zie vorige vraag. Positief antwoord.

17. Wat is uw conclusie ten aanzien van de bruikbaarheid van dit model – gezien vanuit het oogpunt van de onderzoeker / de persoon die het model moet toepassen in de praktijk?

    Antwoord
    Het model is bruikbaar, maar wees voorzichtig met de hoeveelheid vragen. Daarbij is het advies om het instrument via een versnellingskamer in te zetten. Het model kan tevens gebruikt worden bij meerdere overheidslagen, wat de bruikbaarheid vanuit dat oogpunt doet toenemen.

Bijlage 6
Interviewverslag betrokkenen campagne iBewustzijn Overheid

Giulietta Marani
Was binnen de Taskforce Bestuur en Informatieveiligheid Dienstverlening (BID), vanuit ICTU, portofoliomanager en daarmee verantwoordelijk voor het ontwikkelen van een kennis- en leerinfrastructuur en bijbehorend leer- en verankeraanbod ten behoeve van het informatiebeveiligingsbewustzijn bij bestuurders en de ambtelijke top. Daarnaast was zij kwartiermaker voor de iBewustzijncampagne Overheid, die zij samen met Kato Vierbergen vorm gaf.

In een online artikel over het programma iBewustzijn wordt Giulietta uitgebreid voorgesteld in haar rol bij de Taskforce BID (2015):
Giulietta Marani was binnen de Taskforce als portfoliomanager verantwoordelijk voor het ontwikkelen van een kennis- en leerinfrastructuur en bijbehorend leer- en verankeraanbod. Met handvatten die helpen het informatieveiligheidsbewustzijn en het risicobewust handelen van bestuurders en ambtelijke top te verbeteren. Marani: "Daarbij heb ik ingezet op hergebruik van de bestaande kennis en leerinfrastructuur en beproefd aanbod binnen de overheid. Waar nodig zijn afspraken gemaakt voor optimalisatie van die infrastructuur. Ook is samen met overheidslagen en markt nieuw aanbod ontwikkeld. Aanbod dat goed opdrachtgeverschap, betekenisgeving binnen een organisatie, het spreken van dezelfde taal en het inrichten van het informatieveiligheidsproces faciliteert. Het geheel is gebundeld in een campagnepakket iBewustzijn en te vinden op informatieveiligheid. pleio.nl. iBewustzijn biedt interactieve workshops, e-learningmodules en tal van ondersteunende middelen. Dit pakket draagt bij aan het inbedden van informatieveiligheid in de organisatie en in de keten. iBewustzijn ondersteunt organisaties daarbij in 2015."

Kato Vierbergen – Schuit
Sinds 2007 coördinerend beleidsmedewerker/programmacoördinator bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Zij ging in 2012 als gedelegeerd opdrachtgever Digivaardigheden aan de slag om leer- en ontwikkelvragen uit te werken voor het rijksbreed versterken van informatiebeveiligingsbewustzijn in het kader van de invoering van de BIR. Hierbij heeft zij input gehaald uit de verschillende departementen van het Rijk en de ZBO's. In 2013 is zij als gedelegeerd opdrachtgever gestart met de ontwikkeling van de e-learning, workshops en bewustzijnscampagne iBewustzijn Rijk die gericht waren op het Rijk en ZBO's. Zij heeft samenwerking gezocht met de Taskforce BID om het iBewustzijnprogramma vorm te geven. Daarbij is het uitgangspunt geweest dat de programma's van Rijk en Taskforce BID elkaar aan moesten vullen. De e-learningmodules en workshops gericht op medewerkers zijn onderling uitgewisseld met de modules en workshops gericht op bestuurders, zodat één aanbod ontstond voor alle medewerkers van alle bestuurslagen. Zij werkt momenteel samen met de ICTU om iBewustzijn te borgen en naar alle bestuurslagen één verhaal te brengen. Dit doet zij samen met Margot van der Linden.

Margot van der Linden
Vanuit de VNG Gemeente Traineeship heeft zij een opdracht gekregen van het ministerie van BZK en ICTU om de erfenis te borgen van de Taskforce BID op bewustzijnsvlak, welke 13 februari 2015 volgens planning is opgehouden te bestaan. Het gaat hierbij om het ontwikkelde leeraanbod. Zij organiseert en structureert hierbij de

bestaande kennis en informatie op het gebied van informatieveiligheid en informatiebewustzijn, het regelen van beheer en continuïteit van bestaande systemen en het opstellen en uitvoeren van een communicatieplan iBewustzijn Overheid. Het doel van deze opdracht is het zoveel mogelijk ondersteunen en stimuleren van informatiebewustzijn van alle ambtenaren. Hiervoor werkt zij samen met Kato Vierbergen.

Semigestructureerd interview

Volledig
Vragenlijst om te beoordelen of de methodiek 'volledig' is.

1. Welke ontwikkelingen neemt u waar die van invloed zijn op de gemeentelijke informatiebeveiliging?
    a. Internationaal:
    b. Landelijk:
    c. Lokaal:

    Antwoord
    Internationaal
    Toenemende cybersecurity en social engineering. Cybercriminelen worden steeds gewiekster, wat mede als gevolg heeft dat bijvoorbeeld phishingsmails steeds correcter worden ontworpen, zodat misbruik van gegevens kan worden gemaakt.

    Landelijk
    Landelijk zijn verschillende ontwikkelingen waar te nemen.
    De grootste ontwikkeling is dat steeds meer gegevens naar buiten toe worden gebracht. Gegevens worden landelijk tussen instanties gedeeld, of zoals bij de decentralisaties in het sociale domein overgeheveld aan een andere overheidslaag, en burgers posten steeds meer (persoonlijke) data online. Daarnaast ontvangen burgers van de overheid steeds vaker een 'kluisje' waarin zij hun gegevens kunnen raadplegen, én wordt data letterlijk steeds vaker mee naar buiten genomen via mobiele devices (door trends als Het Nieuwe Werken en BYOD). Burgers voelen zich daarbij vaak nog onvoldoende verantwoordelijk voor de kwaliteit van hun eigen gegevens in dat 'kluisje'.

    Daarnaast wordt opgemerkt dat het lijkt dat het bewustzijn per generatie verschilt, waarbij de nieuwere generaties steeds makkelijker worden in het online delen van hun eigen, wat identiteitsfraude meer in de hand gaat werken. Wellicht dat dit te maken heeft met dat de nieuwere generaties meer opgroeien in een digitale wereld en zaken meer vanuit gebruiksgemak bekijken dan vanuit informatiebeveiliging. De oudere generatie lijkt minder snel gegevens af te geven. Onbekend is of dit komt doordat zij meer doordrongen zijn van de risico's of dat dit wellicht te maken heeft dat zij nieuwe technieken niet willen/niet kunnen/of niet zo eenvoudig kunnen gebruiken. Behalve dat het iBewustzijn per generatie verschilt, kan het interessant zijn om te zien of dit verschilt per functie, opleidingsniveau etc.

    Lokaal
    Zoals ook bij landelijk gemeld, lokale overheden gaan over steeds meer gegevens beschikken doordat het Rijk taken overhevelt naar gemeenten, doordat

gemeenten gaan samenwerken met andere gemeenten of via ketensamenwerking.

2. Welke risico's brengt dit mee op de gemeentelijke informatiebeveiliging waar het gedrag van medewerkers invloed op heeft?

   Antwoord
   De risico's die deze ontwikkelingen met zich meenemen zijn:
   - Identiteitsfraude door cybercriminaliteit;
   - Onvoldoende kennis hoe veilig om te gaan met de gegevens die naar buiten worden gebracht. Voorbeeld: mag er bij de wijkteams in het sociale domein een printer staan? Mogen zij met tablets de keukentafelgesprekken voeren? Het wordt steeds moeilijker om de gegevens beveiligen, want de gegevens 'verhuizen' mee naar buiten;
   - Houding t.o.v. informatiebeveiliging verslechtert per generatie, wat de noodzaak voor het blijven werken aan het iBewustzijn vergroot. Scholen zouden hierin ook een rol moeten hebben (oppakken);
   - Men kiest vaak voor het gebruiksgemak t.o.v. informatiebeveiliging. Dit wordt mede veroorzaakt doordat een werkgever vaak nog niet beschikt over middelen om zaken veilig te faciliteren (voorbeeld, Dropbox. Gebruiksvriendelijk en handig. Is er een veilig alternatief?)

3. Wat zijn volgens u de belangrijkste gedragsrisico's van medewerkers bij Nederlandse gemeenten?

   Antwoord
   - Het onbewust onbekwaam handelen, wat per generatie verschilt. De nieuwe generatie[7] is steeds meer onbewust (glijdende schaal). De nieuwe generatie zien vooral de gebruiksvoordelen.
   - Het gaat vooral om het onbewust zijn van de waarde van de informatie, zeker van gecombineerde gegevens.

4. Hoe zou uw top 10 eruit zien op belangrijkste gedragsrisico's eruit zien?

   Antwoord
   In de top 10 moet in ieder geval tot uiting komen dat::
   - gegevens steeds gemakkelijker worden vrijgegeven met het risico dat ze worden misbruikt;
   - men risico's van hun eigen handelen moeten kunnen inschatten;
   - men bewust moet zijn van de waarde van de informatie waar zij mee werken, dan wel die zij bezitten.

5. Wat is uw conclusie ten aanzien van de volledigheid van het voorgelegde model?

   Antwoord
   Het model dekt de belangrijkste gedragsrisico's. Het model dient rekening te houden met dat houding per generatie kan verschillen en de gevolgen van cybercriminaliteit in de vorm van bijvoorbeeld identiteitsfraude kan nog in het

[7] Generatie vanaf 1990 –de periode waarin computer- en internetgebruik meer algemeen goed begon werd.

model worden opgenomen. Daarnaast is onderkend dat niet alle privacy risico's meegenomen zijn (zoals 'laat je niet kopiëren'). Daarnaast zijn ook niet alle aspecten rondom inkoop en aanbesteding meegenomen.

Aspect 'Correct'
Vragenlijst om te beoordelen of de methodiek correct is.

Onderdeel 1
Vragen over campagne iBewust Overheid

6. Op welke wijze is de campagne iBewust Overheid geschikt gemaakt voor gemeenten?

   Antwoord
   Het materiaal van iBewustzijn Rijk is omgeschreven naar gemeenten, met reviewronde door een aantal gemeenten. Dit is door de Taskforce BID gedaan. Daar waar nodig is de input vanuit de BIR aangepast aan de BIG.

7. Wie/Welke partijen hebben de 10 gouden regels opgesteld en welke partijen vertegenwoordigden hierbij de gemeenten?

   Antwoord
   De 10 gouden regels zijn opgesteld vanuit de richtlijnen die gebruikt zijn bij de verschillende departementen en ZBO's. Verder zie vraag 1. Daarbij zijn de gouden regels voorgelegd aan een aantal gemeenten via de accountmanager Gemeenten, waaronder in ieder geval de gemeente Groningen.

8. Hoe zijn déze 10 gouden regels gekomen (hoe zijn deze geselecteerd)?

   Antwoord
   Tijdens de ontwikkeling van de e-learning zijn op basis van de leerdoelen 4 modules benoemd. Per module zijn 'tips' verwerkt uit de in gebruik zijnde internet- en emailgedragscodes van de departementen. Die zijn samengevat in de 10 gouden regels. De 10 gouden regels zijn bepaald in een multidisciplinaire werkgroep vanuit iBewustzijn Rijk. Dat bevat een hoge mate van 'boerenverstand'. Van belang is dat er regels zijn en dat men er op aangesproken kan worden/elkaar erop aanspreekt. De gouden regels zijn de praktische vertaling van de gestelde leerdoelen. In het ontwerp is uitgegaan van:
   - Wat doe je nu?
   - Welk risico loop je daarmee?
   - Wat zou een veiliger gedrag zijn?

9. In hoeverre verhouden de 10 gouden regels zich tot de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)?

   Antwoord
   iBewustzijn is mede gebaseerd op de BIR en in de vertaling naar gemeenten zijn de aanvullende maatregelen uit de BIG meegenomen. De 10 gouden regels zijn opgesteld als geldend voor alle overheidslagen en dus algemeen gehouden.

Onderdeel 2

10. In hoeverre meten de gouden regels de thema's?

    Antwoord
    De gouden regels meten de vier thema's.

    Opmerking
    De kennissurveyvragen zijn ja/nee en het risico is dat een werknemer een vraag met 'ja' beantwoordt maar hier iets anders mee bedoelt dan de Gouden Regels (of de informatiebeveiligers). Dit zou je kunnen oplossen door bij enkele vragen om een toelichting te vragen.

11. In hoeverre meten de bepalende factoren de gouden regels

    Antwoord
    Deze meten de gouden regels.

12. In hoeverre meet de vraag de gouden regel?

    Antwoord
    De vragen meten de gouden regels. Alleen worden er bij de kennisvragen waarom-vragen gesteld waar normaliter een ik-weet-dat-vraag aan vooraf gaat. Voorbeeld: ik weet wat het risico is als ik een onbekende toelaat in ons pand (waarom-vraag). Hier gaat de vraag aan vooraf: ik weet dat ik geen onbekende mag toelaten. Deze laatste vraag komt niet expliciet in het model terug.

13. In hoeverre houden de kennisvragen rekening met de drie elementen uit de literatuur?

    Antwoord
    De vragen houden hier rekening mee, maar door enkel ja/nee te kunnen antwoorden is de betrouwbaarheid van het antwoord niet te controleren.

    Opmerking
    Het risico in de ja/nee kennisvragen is, dat medewerkers sociaal wenselijk antwoorden, maar toch ongewenst gedrag blijven vertonen. Het is bekend dat mensen heel creatief zijn in het bedenken van work-arounds als de voorzieningen niet aansluiten bij wat ze gewend zijn en/of ze niet overtuigd zijn (in houding/attitude) van het nut/risico of daarop niet aangesproken worden. Heel belangrijk is de cultuur in de organisatie, waarin het management een belangrijke rol heeft. Naast de 'gouden regels' is het ook belangrijk dat men elkaar aanspreekt op het naleven ervan.

14. In hoeverre zijn de kennis-, houding- en gedragsvragen lijn met elkaar gebracht

    Antwoord
    Deze zijn in lijn gebracht. Dit is erg goed gedaan. Door het op deze manier aan te pakken ondervang je deels het 'probleem' met de ja/nee vragen.

15. Moeten meer vragen (en zo ja welke) gesteld worden om een specifieke gouden regel te meten binnen een specifieke dimensie om een goede indicatie te krijgen van het bewustzijnniveau – rekeninghoudend met de effectiviteit van de vragenlijst (totaal aantal vragen / bereidwilligheid om zoveel vragen te beantwoorden)?

    Antwoord
    Per gouden regel zijn een of meerdere subfactoren bepaald om de gouden regel te meten. Elke subfactor wordt vervolgens gemeten met drie vragen. Dit is meer dan voldoende. Meer vragen zijn niet nodig. Per organisatie kan gekeken worden of op specifieke gouden regels (of subfactoren) aanvullende vragen nodig zijn omdat het aanverwante gedragsrisico meer leeft/erg actueel is. De basis van het model kan door elke gemeente, en zelfs elke overheidslaag gebruikt worden. Meer vragen voor het meten van de basis is niet nodig.

16. Wat is uw conclusie ten aanzien van de correctheid van de vragenlijst?

    Antwoord
    Het model houdt rekening met de belangrijkste gedragsrisico's, die afgeleid zijn uit de BIG. Op basis daarvan zijn vier thema's gekozen waaraan de gouden regels en vervolgens de subfactoren zijn gekoppeld. Dit is een logische lijn om tot slot te komen tot de surveyvragen. Het model is zeer waardevol en bruikbaar. Misschien hier en daar een open vraag om de kennis te controleren.

Aspect 'Bruikbaarheid

Vragenlijst om te beoordelen of de methodiek bruikbaar is voor de onderzoeker. Bij het interview wordt hen gevraagd een uitspraak te doen over de verwachte bruikbaarheid van het model.

17. Als u het model bekijkt vanuit het oogpunt van de onderzoeker, in hoeverre oogt dit model dan toepasbaar in termen van gebruikersvriendelijk en eenvoudig? Hiermee wordt bedoeld dat een onderzoeker weinig voorbereidingstijd nodig heeft om het model te begrijpen en toe te passen.

    Antwoord
    Minimale uitleg is nodig. Het is goed bruikbaar.

18. In hoeverre is het model toepasbaar op alle Nederlandse gemeenten? (Zijn alle elementen (blokken) uit het model van toepassing op alle Nederlandse gemeenten?)

    Antwoord
    De aanname is dat het model in veel gemeenten toe te passen is. Het kan lastiger worden bij gemeenten die ambtelijk gefuseerd zijn en met eigen collegeprogramma's en regels werken. Maar dat zou aan de specifieke gemeenten gevraagd moeten worden.

19. In welke mate denkt u dat de resultaten eenduidig en direct kunnen worden gekwantificeerd door de onderzoeker, naar aanleiding van de gestelde vragen en opbouw van de puntenscores?

    Antwoord
    Voldoende / geen opmerkingen

20. In hoeverre bent u van mening dat de gekwantificeerde resultaten gelijk kunnen worden geanalyseerd per dimensie, factor en thema?

    Antwoord
    Aan de resultaten kan een algemeen beeld gegeven worden, maar het zegt vooral iets over de mate van bewustzijn en het gedrag van mensen en minder over het beveiligingsniveau. Hiervoor zouden andere vragen en meetinstrumenten ingezet moeten worden (wordt er voldaan aan de BIG etc).

21. Wat is uw conclusie ten aanzien van de bruikbaarheid van dit model – gezien vanuit het oogpunt van de onderzoeker / de persoon die het model moet toepassen in de praktijk?

    Antwoord
    Mooi model. Het levert waarschijnlijk bruikbare en waardevolle inzichten op voor gemeenten die zich bezighouden met informatiebewustzijn en het verbeteren hiervan. Ook levert het inzichten –indien jaarlijks herhaalt- in hoeverre de campagnes en ingezette middelen effect gehad hebben.

Bijlage 7 Interviewverslag CISO gemeente Edam-Volendam

Remco Rekoert
CISO gemeente Edam-Volendam

Semigestructureerd interview
Onderstaande vragen stellen en hierop doorvragen indien relevant

Aspect 'Volledig'
Vragenlijst om te beoordelen of de methodiek 'volledig' is.

1. Welke ontwikkelingen neemt u waar die van invloed zijn op de gemeentelijke informatiebeveiliging?
    a. Internationaal
    b. Landelijk
    c. Lokaal

    Antwoord
    - De gemeentelijke digitale informatie wordt steeds meer bedreigd vanuit anderen landen. Denk hierbij aan phishingmails en hackers die bijvoorbeeld vanuit China proberen digitale gemeentelijke informatie te ontfutselen.
    - Daarbij maken medewerkers steeds meer gebruik van mobiele devices waar gevoelige informatie op zit. Dat zijn medewerkers niet gewend en daar houden zij ook geen rekening mee. Met als gevolg dat medewerkers onbeveiligde wifi gebruiken met alle risico's van dien. Bewustwording is de kracht van herhaling.
    - Er zijn ook ontwikkelingen op privacy gebied. Op Europees niveau werkt men aan een privacy verordening en op landelijk niveau is de meldplicht datalekken van kracht geworden.
    - Dit haakt aan op ontwikkelingen dat gemeenten over steeds meer persoonsgegevens beschikken vanuit onder andere de sociale transitie.
    - Op lokaal niveau gaan gemeenten meer fuseren en samenwerken. Dit 'mengt' culturen met elkaar en betekent dat er ook aan bewustwording moet blijven worden gewerkt, waarbij samenwerkende/gefuseerde gemeente elk van een ander bewustzijnsniveau komen.
    - Te veel bezig met 'on going' zaken waardoor informatiebeveiliging te laat bij processen betrokken wordt.

2. Welke risico's brengt dit mee op de gemeentelijke informatiebeveiliging waar het gedrag van medewerkers invloed op heeft?

    Antwoord
    - Door ontwikkelingen, waaronder fusies en samenwerkingen, zijn middelen en tijd een kwetsbaar punt. Organisatorisch gezien pakt het MT informatiebeveiliging onvoldoende op en wordt er te weinig op gestuurd. De prioriteit ligt elders. Tevens wordt de hoeveelheid qua Informatiebeveiliging onderschat door MT. Ook voor hen geldt continue herhalen.
    - Hierbij en hierdoor was lokaal de toegankelijkheid een kwetsbaar punt. Toegankelijkheid betekent hierbij de eenvoud om als onbevoegde het stadhuis te betreden. Bij kleinere gemeenten gelden minder strengere beveiligingseisen bij het betreden van het stadhuis dan bij grote gemeenten. Door de fusie is bij

de gemeente Edam-Volendam een voorgestelde aanpassing op dit vlak vooruitgeschoven.
- Daarnaast staan medewerkers in het sociaal domein onvoldoende stil bij hoe gevoelig de persoonsgegevens zijn en welke impact een beveiligingsincident kan hebben op de organisatie of een persoon.
- Er is verder bij gemeenten/MT nog weinig aandacht/realisatie voor informatiebeveiliging en privacy (behalve als er een wettelijke grondslag is). De focus ligt als eerste op het werkbaar maken en krijgen van processen (waaronder die uit de sociale transitie). Doordat er veel op gemeenten tegelijk afkomt (sociale transitie, samenwerkingen/fusies, bezuinigingen e.d.) komt informatiebeveiliging op een lagere plek te staan.
- Medewerkers onderschatten het belang van informatiebeveiliging, te meer omdat er onvoldoende op wordt gecontroleerd/gehandhaafd (door interne en externe personen/instanties).
- Een groot ander risico is dat de CISO niet tijdig wordt betrokken bij nieuwe ontwikkelingen, het ontwerpen van processen, het inkopen van informatiesystemen e.d. En dat terwijl medewerkers op informatiebeveiligingsvlak vaak onwetend zijn.

3. Wat zijn volgens u de belangrijkste gedragsrisico's van medewerkers bij Nederlandse gemeenten (in casu Edam Volendam)?

   Antwoord
   Op basis van de ontwikkelingen en opgesomde risico's bij de vragen 1 en 2 worden de volgende gedragsrisico's benoemd:
   - De houding van medewerkers – gemakzucht. Het gaat toch altijd goed ?!
   - Medewerkers hebben te weinig discipline om de afspraken op informatiebeveiligingsvlak na te leven. Het MT heeft hier ook een rol (draagvlak/commitment). De cultuur is hier nog niet naar.
   - Social engineering heeft hierdoor vrij baan.
   - Het opruimen van de bureau's en het afsluiten van beeldschermen bij het verlaten van de werkplek of het stadhuis gebeurt onvoldoende.
   - Medewerkers hebben onvoldoende overzicht over hun rol in het gehele proces. Zij zien alleen hun eigen schakel en kunnen niet inschatten wat de consequenties in het proces zijn als zij een beveiligingsincident veroorzaken (dan wel hadden kunnen voorkomen).

   Opmerking: Neem de tijd voor borging van informatiebeveiliging. Bij bewustwording gaat het om de kracht van de herhaling.

4. Hoe zou uw top 10 eruit zien op belangrijkste gedragsrisico's eruit zien?

   Antwoord
   In willekeurige volgorde benoemt de CISO van Edam-Volendam de volgende risico's:
   1. Meest belangrijke is het te laat betrekken van informatiebeveiliging in een proces, zoals onder andere het niet consulteren van de CISO.
   2. Beveiligingsincidenten en storingen niet melden bij de CISO of ICT.
   3. Geen vragen stellen over onduidelijkheden in het informatiebeveiligingsbeleid of andere gerelateerde documentatie, wat het naleven van het informatiebeveiligingsbeleid bemoeilijkt.

4. Internet, e-mail en sociale media onverantwoord gebruiken (medewerkers zijn zich onvoldoende bewust van hoeveel zij hiervan gebruik maken, evenals cloudtoepassingen. Die gebruiken zij vaker dan zij zelf weten).
5. Documenten niet vertrouwelijk behandelen. Documenten die vertrouwelijk zijn worden niet als zodanig geclassificeerd en worden tevens ook niet opgeborgen in afgesloten kasten.
6. Het verspreiden (delen, versturen etc.) van vertrouwelijke gegevens (waaronder persoonsgegevens). Door dit te plaatsen op internet of het versturen per email.
7. Wachtwoorden (inloggegevens) delen met anderen (bijvoorbeeld tijdens vakantieperiodes).
8. Systemen en werkplekken niet vergrendelen als de werkplek wordt verlaten.
9. Eigen meegebrachte devices op het werk t.b.v. het werk verantwoord gebruiken.
10. Apparatuur en informatie zonder toestemming verplaatsen of meenemen naar een andere locatie, op een onbeveiligde wijze.

5. Wat is uw conclusie ten aanzien van de volledigheid van het voorgelegde model?

Antwoord

Het model moet dynamisch zijn en moet structureel geëvalueerd worden op of het nog de belangrijkste gedragsrisico's meet. Het model moet tevens afgestemd worden op de werksituatie. Dit kan per gemeente verschillen. Dit wordt mede beïnvloed door trends en ontwikkelingen op internationaal/landelijk/lokaal niveau. Informatiebeveiliging moet afgestemd zijn op de organisatie. Het model zoals deze is gepresenteerd is volledig, behoudens een aantal aanpassingen. De genoemde risico's bij vraag 4 zijn afgezet tegen de 10 gouden regels uit het model. Alle risico's worden gedekt, behoudens de risico's 2, 3 en 9. Het model zal voor de volledigheid dan aangepast moeten worden op de volgende gebieden:

- Gouden regel uit het model 1 (leef beleid en procedures na) moet tevens de genoemde risico's 2 en 3 meten(vragen stellen en tijdig de CISO consulteren). Dit is volgens de CISO van Edam-Volendam een belangrijke om toe te voegen. Het gaat namelijk om discipline van medewerkers en het (h)erkennen van de eigen rol in het proces en hun houding ten opzichte van informatiebeveiliging. Deze twee risico's kunnen samengevat worden onder de noemer: consulteer tijdig de CISO. Dit bevordert het naleven en toepassen van beleid en procedures.
- Genoemde risico 9 (eigen gebrachte devices verantwoord gebruiken) wordt niet gedekt in het model onder het thema 'Binnen'. Deze moet gemeten worden in gouden regel 4 'Ga vertrouwelijk om met informatie'. Medewerkers nemen namelijk steeds vaker eigen devices mee (en usb-stickjes e.d.) naar het stadhuis.

Tot slot wordt het advies gegeven om ook het MT in het model te betrekken, wellicht in de vorm van een zelftest die door een CISO kan worden uitgevoerd.

Aspect 'Correct'
Vragenlijst om te beoordelen of de methodiek correct is.

6. In hoeverre meten de gouden regels de thema's?

   Antwoord
   Na het doorlopen van alle thema's en gouden regels uit het gepresenteerde model is de conclusie dat alle gouden regels de vier thema's meten. Deze hoeven op dat niveau niet aangepast te worden (behoudens aanpassingen die zijn genoemd bij de vragen omtrent het aspect 'volledigheid').

7. In hoeverre meten de subfactoren de gouden regels

   Antwoord
   Er worden een aantal opmerkingen hierover gemaakt:
   - Gouden regel 1 'Leef beleid en procedures na', voeg subfactor toe: Betrek/consulteer de CISO tijdig.
   - Gouden regel 2 'Laat geen onbevoegden toe in onze gebouwen en op onze werkplekken': hierbij is in het model de subfactor 'Als je een toegangspas hebt, draag deze zichtbaar en motiveer anderen dat te doen' voorgesteld te laten vervallen. Deze moet toch worden toegevoegd, omdat dit bepaald of mensen anderen aanspreken. Dit is een belangrijke factor voor deze gouden regel.
   - Gouden regel 4 'Ga vertrouwelijk om met informatie': Een belangrijke bepalende subfactor om hieraan toe te voegen is dat medewerkers afspraken moeten maken met derden om informatiebeveiligingsincidenten te voorkomen en de afspraken hierover vast te leggen (in contracten, SLA's, bewerkingsovereenkomsten e.d.). Medewerkers moeten zelf niet alleen vertrouwelijk met informatie omgaan, maar moeten dit ook derden (inhuur en anderen) opleggen die namens hen werkzaamheden verrichten. Werken in de cloud neemt toe (zie punt 10). Hierbij speelt dit een grote rol.
   - Gouden regel 5 'Meld incidenten': is uitgesplitst in het melden van technische incidenten aan de helpdesk ICT en overige incidenten aan de leidinggevende. Dit kan samengevoegd worden tot het altijd melden van incidenten aan de CISO.
   - Gouden regel 6 'Zorg voor optimale beveiliging van mobiele apparaten met zakelijke informatie': hierbij is in het model de subfactor 'Bij reparatie of verkoop van een (mobiel) apparaat, altijd eerst de zakelijke op het apparaat (laten[8]) wissen' voorgesteld te laten vervallen. Deze moet toch worden toegevoegd omdat als mobiele devices van de hand worden gedaan, wat met regelmaat gebeurt, dit belangrijk is om beveiligingsincidenten te voorkomen (lekken gegevens bijvoorbeeld).
   - Gouden regel 10 'Ben je bewust van risico's van clouddiensten en online communicatie: hierbij is een subfactor opgenomen waarbij is aangegeven dat medewerkers de voorwaarden moeten lezen als voordat zij gebruik gaan maken van clouddiensten. Dit heeft weinig waarde om te meten om een goede uitspraak te doen over gouden regel 10. Dit doen medewerkers toch niet, dan wel zelden. Weinigen lezen de (algemene) voorwaarden voordat zij hiermee

[8] Door I&A van eigen gemeente. Voor het gebruik van zakelijke gegevens op privé apparaten blijft de organisatie altijd zelf verantwoordelijk; dus ook zelf zeker weten dat de zakelijke gegevens worden verwijderd

aan de slag gaan. Deze subfactor kan dan ook vervallen, aangezien er dan nog 3 subfactoren zijn die deze gouden regel meten. NB ook leveranciers worden verplicht gesteld om de voorwaarden beter op te stellen.

8. In hoeverre meet de vraag de gouden regel?

   Antwoord
   - Gouden regel 2, subfactor ‘Spreek onbekende personen op jouw afdeling aan’: de kennisvraag ‘ik weet welke informatie op mijn afdeling niet openbaar mag worden’ dekt de lading niet.
   - Opmerking naar aanleiding van Gouden regel 2, subfactor ‘Leen toegangspas niet uit’. Bij de kennisvraag staat ‘ik ken de dreigingen die gepaard gaan met het uitlenen van mijn toegangspas aan een collega (of aan anderen). Dit kan de verwachting wekken bij medewerkers dat toegangspassen wel uitgeleend mogen worden op het moment dat zij de vragenlijst beantwoorden. Het is daarom goed om bij de inleiding van de survey te vermelden dat dat de gestelde vragen niet bepalen of aangeven welk gedrag wel of niet mag, maar dat de gestelde vragen een indruk geven over de stand van zaken.
   - Gouden regel 3, subfactor ‘Laat digitale gegevensdragers nooit onbeheerd achter’: bij de vraagstelling moet worden toegevoegd dat men dit niet onbeheerd achter laat *los van het feit of een of meerdere collega’s nog op de afdeling aanwezig zijn*. Medewerkers zullen de vraag anders interpreteren en dat onbeheerd betekent dat dit enkel geldt als zij hun werkplek verlaten en ook hun collega’s niet meer aanwezig zijn. De subfactor bedoeld echter met onbeheerd dat expliciet de medewerker de eigen digitale gegevensdragers niet meer beheerd.

9. In hoeverre houden de kennisvragen rekening met de drie elementen uit de literatuur?

   Antwoord
   Na het doorlopen van de kennisvragen – afgezet tegen de drie elementen, is de conclusie dat alle kennisvragen rekening houden met een van de drie elementen uit de literatuur.

10. In hoeverre zijn de kennis-, houding- en gedragsvragen per subfactor in lijn met elkaar gebracht?

    Antwoord
    De vragen zijn per subfactor bekeken. De vragen meten elke subfactor en de vragen zijn in lijn met elkaar gebracht.

11. Moeten meer vragen (en zo ja welke) gesteld worden om een specifieke gouden regel te meten binnen een specifieke dimensie om een goede indicatie te krijgen van het bewustzijnniveau – rekeninghoudend met de effectiviteit van de vragenlijst (totaal aantal vragen / bereidwilligheid om zoveel vragen te beantwoorden)?

    Antwoord
    Nee, er zijn voldoende vragen gesteld, waarbij elk subfactor wordt gemeten. Om een goede indicatie te krijgen is het aantal vragen meer dan genoeg.

12. Wat is uw conclusie ten aanzien van de correctheid van de vragenlijst?

    Antwoord
    De vragenlijst en het model zijn correct opgebouwd, behoudens een aantal aanpassingen die vermeld staan bij de voorgaande vragen. Voornamelijk op het vlak van de subfactoren kan een en ander aangescherpt worden ten behoeve van het meten van de gouden regels.

Aspect 'Bruikbaarheid

Vragenlijst om te beoordelen of de methodiek bruikbaar is voor de onderzoeker. Bij het interview wordt hen gevraagd een uitspraak te doen over de verwachte bruikbaarheid van het model.

13. Als u het model bekijkt vanuit het oogpunt van de onderzoeker, in hoeverre oogt dit model dan toepasbaar in termen van gebruikersvriendelijk en eenvoudig? Hiermee wordt bedoeld dat een onderzoeker weinig voorbereidingstijd nodig heeft om het model te begrijpen en toe te passen.

    Antwoord
    - Het model is eenvoudig toe te passen, omdat het flexibel is (gemakkelijk aan te passen) en logisch is opgebouwd.

14. In hoeverre is het model toepasbaar op alle Nederlandse gemeenten? (Zijn alle elementen uit het model van toepassing op alle Nederlandse gemeenten?)

    Antwoord
    - Niet alle vragen gelden voor elke gemeente. De vragenlijst en de belangrijkste gedragsrisico's moeten op de organisatie(cultuur) worden afgestemd. De methodiek leent zich hiervoor. Het vraagt wel van de onderzoeker enige consequentie in het bijhouden van de actuele gedragsrisico's en bijbehorende surveyvragen..

15. Toelichten hoe resultaten worden gekwantificeerd en vervolgens de vraag stellen: In welke mate denkt u dat de resultaten eenduidig en direct kunnen worden gekwantificeerd?

    Antwoord
    - Deze kunnen eenduidig en direct worden gekwantificeerd doordat er wordt gewerkt met een tweepunts- en een vijfpuntsschaal op de antwoorden.

16. In hoeverre bent u van mening dat de gekwantificeerde resultaten gelijk kunnen worden geanalyseerd per dimensie, factor en thema? (Geven de gekwantificeerde resultaten direct inzicht in het informatiebeveiligingsniveau, zonder eerst deze resultaten te moeten verwerken voordat deze geanalyseerd kunnen worden?)

    Antwoord
    - Doordat in een tabel de gekwantificeerde resultaten worden weergegeven, kunnen deze snel worden geanalyseerd. Zeker als je met kleuren gaat werken

en er een index erbij zet (rood, oranje, groen bijvoorbeeld). Dan kan het snel gelezen worden.

17. Wat is uw conclusie ten aanzien van de bruikbaarheid van dit model – gezien vanuit het oogpunt van de onderzoeker / de persoon die het model moet toepassen in de praktijk?

    Antwoord
    - Het model is flexibel en eenvoudig te gebruiken. Wel is de verwachting dat er te veel surveyvragen zijn. Het is goed om de survey dusdanig op te zetten dat het de lading dekt en maar maximaal 10 a 15 minuten invultijd kost van een medewerker (i.v.m. bereidwilligheid. Iedereen is namelijk druk).

    Tip van de CISO: De thema's kunnen ook anders worden benoemd, waarbij de thema's worden vervangen door de hoofdstukindeling uit de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Op deze wijze kan er op een andere manier de resultaten worden geanalyseerd (namelijk op welke aspecten uit de BIG moeten op bewustwordingsvlak nog stappen worden gezet).

Bijlage 8
Uitnodigingsbrief voor 9 ambtenaren van drie Nederlandse gemeenten

Onderzoek naar methodiek om het informatiebeveiligingsbewustzijn van medewerkers bij gemeenten te kunnen meten

Verzoek om je te mogen interviewen om de effectiviteit van het ontwikkelde model te beoordelen

Dhr. Y. Lammerts van Bueren
X

m. X
t. X

Gemeente..
Ter attentie van ..
Adres
Postcode + vestigingsplaats

6 mei 2015

Beste …,

In het kader van mijn masterthesis voor mijn opleiding Business Process Management & IT aan de Open Universiteit heb ik een model ontwikkeld waarmee het informatiebeveiligingsbewustzijn bij medewerkers van Nederlandse gemeenten kan worden gemeten. Een dergelijke methodiek is hiervoor nog niet voorhanden maar wel wenselijk gezien de aangenomen resolutie ‘Informatieveiligheid, randvoorwaarde voor een professionele gemeente’ op de buitengewone algemene ledenvergadering van de VNG op 29 november 2013. De resolutie bepaalt dat gemeenten aantoonbaar in control moeten zijn op het gebied van informatieveiligheid conform de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Een belangrijke factor hierin is de wijze waarop medewerkers het informatiebeveiligingsbeleid naleven (gedragscomponent).

Binnen onze gemeente zijn we vorig jaar gestart met invulling te geven aan de resolutie en zijn we begin dit jaar gestart met de voorbereidingen om te werken aan het informatiebeveiligingsbewustzijnniveau van onze medewerkers. Het ontwikkelde model meet het informatiebeveiligingsbewustzijn van medewerkers, dat bestaat uit de componenten kennis, houding en gedrag. Dit model is specifiek ontwikkeld voor medewerkers van Nederlandse gemeenten en kan gebruikt worden om concreet richting te geven aan de wijze waarop aan het informatiebeveiligingsbewustzijn dient te worden

gewerkt. Dit model dient echter nog wel beoordeeld te worden op effectiviteit (is het eenvoudig toe te passen en begrijpelijk voor medewerkers).

Om de effectiviteit van het model te beoordelen zou ik graag dit model bij een aantal medewerkers willen toepassen die werkzaam zijn binnen verschillende afdelingen, disciplines en gelederen. Daarom zou ik het erg waarderen als ik je maximaal 1,5 uur mag interviewen, waarbij ik het model toelicht, toepas en met je bespreek.

Het vertrouwelijke karakter van dit interview en je anonimiteit worden uiteraard gewaarborgd. Tevens wordt van het interview een verslag uitgewerkt die aan je wordt voorgelegd voordat de resultaten uit het interview worden meegenomen in het onderzoek.

Ik hoop dat je het leuk vindt om bij te dragen aan de ontwikkeling van dit model. Behalve dat het model wordt beoordeeld of effectiviteit bij een select aantal medewerkers, wordt het model ook beoordeeld of deze inhoudelijk correct en volledig is. Dit wordt gedaan met een aantal deskundigen binnen het vakgebied van informatiebeveiliging.

Indien je geïnteresseerd bent in het uiteindelijke onderzoeksrapport, dan zal ik je deze ter zijne tijd toesturen (verwachting is september 2015).

Graag hoor ik van je of we een afspraak in juni kunnen plannen voor het interview.
Indien je vragen of nadere informatie over dit onderzoek wil hebben, dan kun je mij bereiken op telefoonnummer XXX of een email versturen naar XXX.

Met vriendelijke groet,

Youri Lammerts van Bueren

Bijlage 9 Survey

Nr	Vraag	Antwoord		Eventuele opmerking
		Ja	Nee	
1	Ik ken de 10 gouden gedragsregels			
2	Ik weet waar ik de CISO voor kan raadplegen			
3	Ik weet waarom er van mij wordt verwacht dat ik een collega aanspreek als ik zie dat deze collega onjuist omgaat met informatie(middelen)			
4	Ik weet welke risico's het met zich meebrengt als ik een onbekende toelaat in ons pand en op onze werkplekken			
5	Ik weet waarom ik mijn externe bezoekers (burgers, leveranciers e.d.) moet ophalen bij de publieke ingang en hen na bezoek weer moet begeleiden naar de uitgang			
6	Ik weet waarom ik mijn toegangspas zichtbaar moet dragen			
7	Ik weet waarom ik onbekende personen op mijn afdeling moet aanspreken om na te gaan of zij wel bevoegd zijn om daar te zijn			
8	Ik ken de dreigingen die gepaard gaan met het uitlenen van mijn toegangspas			
9	Wanneer ik vertrouwelijke informatie ben verloren en vermoed dat het mogelijk is dat dit in handen is gekomen van onbevoegden dan weet ik aan wie ik dit (incident) moet melden			
10	Als ik iets of een situatie verdacht vind, dan weet ik aan wie ik dit moet melden			
11	Ik weet met welke toetsencombinatie ik mijn computerscherm kan vergrendelen als ik mijn werkplek verlaat			
12	Ik kan de mogelijke schade overzien voor de organisatie of de burger als ik vertrouwelijke documenten op mijn bureau laat liggen als ik mijn werkplek verlaat			
13	Ik weet wat de gevolgen kunnen zijn als ik een usb/mobieltje/laptop/tablet op mijn werkbureau laat liggen als ik even in overleg ga			
14	Ik weet welke risico's het delen van mijn wachtwoord met collega's kan hebben voor de continuïteit van de dienstverlening en voor burgers			

Nr	Vraag	Antwoord		Eventuele opmerking
		Ja	Nee	
15	Ik weet welke risico's het met zich meebrengt als ik mijn vertrouwelijke printjes bij de printer onbeheerd laat liggen			
16	Ik weet hoe ik vertrouwelijke informatie moet weggooien/vernietigen			
17	Ik weet wanneer informatie vertrouwelijk is			
18	Ik weet welke informatie(middelen) bedrijfskritisch zijn voor mijn organisatie (de zogenaamde 'kroonjuwelen' van de organisatie die bij verlies een enorme grote impact hebben op/voor de organisatie, de politiek en de burger)			
19	Ik weet welke maatregelen ik kan treffen om te voorkomen dat iemand kan meekijken of meeluisteren als ik buiten het kantoor met vertrouwelijke informatie werk			
20	Ik weet welke gevolgen het kan hebben als ik zakelijke informatie(middelen) buiten het kantoorpand (even) onbeheerd achter laat			
21	Ik weet wat ik moet doen als ik vermoed dat iemand mijn wachtwoord heeft gezien doordat hij meekeek over mijn schouder op het scherm (van mijn laptop/mobiel etc)			
22	Ik weet dat ik alleen vertrouwelijke informatie mee mag nemen van het kantoor als dit strikt noodzakelijk is voor de uitvoering van mijn functie			
23	Ik weet wat het risico is als ik vertrouwelijke werkgerelateerde gesprekken voer buiten het kantoor met mensen die niet bij mij op het kantoor werken (bijvoorbeeld in de trein, op terras of op een verjaardagsfeestje)			
24	Een van de basisbeveiligingsmaatregelen is het hebben van een wachtwoord/toegangscode op (privé) mobiele apparaten (mobiel, laptop, tablet), zeker als ik deze gebruik om zakelijke informatie mee te lezen (zoals werkmail)			
25	Ik weet hoe ik beveiligingsrisico's kan achterhalen van software (en apps) die ik wil installeren			
26	Ik weet welke risico's het niet updaten van software op (mobiele) apparaten met zich meebrengen			

Nr	Vraag	Antwoord		Eventuele opmerking
		Ja	Nee	
27	Ik weet waarom het belangrijk is dat bij reparatie of verkoop van een (mobiel) apparaat eerst de zakelijke gegevens van het apparaat moet worden zijn gewist			
28	Ik weet wat de gevolgen kunnen zijn als niet ICT maar ikzelf software installeert op mijn mobiele apparaten (laptop, mobiel, tablet e.d.)			
29	Ik weet wat het belang is van een goede up-to-date-virusscanner en een firewall op mijn privé apparten, die ik ook voor zakelijke doeleinden gebruik (zoals het raadplegen van mijn werkmail)			
30	Ik weet waarom ik niet mijn inloggegevens mag afstaan per email			
31	Ik weet waaraan ik verdachte e-mails kan herkennen			
32	Ik weet waarom ik de website op echtheid moet controleren als ik op de website wil inloggen als ik vanuit een email naar deze website wordt doorgestuurd (toegelinkt)			
33	Als ik internet dan weet ik wat de gevaren zijn van het klikken op: advertenties als 'KLIK HIER, U HEEFT EEN PRIJS GEWONNEN'; en meldingen die de website onverwachts op je scherm laat verschijnen met 'Download nu deze software om verder te kunnen'.			
34	Ik weet welke dreigingen gepaard gaan met het gebruiken van gratis wifi om mijn werkmail te lezen			
35	Ik ken de risico's van het versturen en opslaan van vertrouwelijke informatie met internetdiensten als Hotmail, Gmail, Wetransfer, Dropbox en dergelijke			
36	Ik weet over welke werkgerelateerde zaken ik wel en niet online kan (en mag) communiceren			

Nr	Vraag	Antwoord					Eventuele opmerking
		Helemaal oneens	Oneens	Eens/ Oneens	Eens	Helemaal eens	
1	De 10 gouden regels zijn eenvoudig toe te passen						
2	Vragen en onduidelijkheden over veilig en verantwoord werken met (vertrouwelijke) informatie(middelen) moeten aan de CISO gesteld worden						
3	Het is belangrijk dat collega's elkaar aanspreken als zij constateren dat er onjuist wordt omgegaan met informatie(middelen)						
4	Elke personeelslid dat via de personeelsingang het pand betreedt richting de werkruimten, is er voor verantwoordelijk dat hij moet voorkomen dat onbevoegden met hem mee het pand in lopen						
5	Het is belangrijk dat extern bezoek (burgers, leveranciers e.d.) altijd vanaf de receptie wordt begeleid en na bezoek weer wordt begeleid naar de uitgang, zodat bezoek niet kan dwalen en vertrouwelijke informatie kan raadplegen						
6	Het is belangrijk om de toegangspas zichtbaar te dragen						
7	Onbekende personen op de afdeling moeten daar door de aanwezige medewerkers worden aangesproken om na te gaan of zij wel bevoegd zijn om daar te zijn						
8	Toegangspassen mogen aan niemand uitgeleend mogen worden						
9	Het is belangrijk dat de medewerker zijn leidinggevende informeert als hij denkt dat het mogelijk is dat vertrouwelijke informatie in handen is gekomen van onbevoegden doordat hij bijvoorbeeld documenten kwijt is geraakt						
10	Verdachte zaken en situaties moeten altijd aan de leidinggevende worden gemeld						
11	Het is belangrijk om altijd bij het verlaten van de werkplek het computerscherm te vergrendelen						

Nr	Vraag	Antwoord					Eventuele opmerking
		Helemaal oneens	Oneens	Eens/ Oneens	Eens	Helemaal eens	
12	Bij het verlaten van de werkplek moeten vertrouwelijke documenten altijd worden opgeborgen (achter slot en grendel)						
13	Een mobieltje/laptop/usb'tje/tablet en andere digitale gegevensdragers mogen nooit onbeheerd op iemands werkplek liggen, ook al gaat hij even in overleg						
14	Wachtwoorden mogen niet gedeeld worden met een collega als de er iemand met vakantie gaat, zodat zijn collega zijn urgente emails kan afhandelen						
15	Vertrouwelijke printjes moeten altijd direct bij de printer worden weggehaald door de medewerker die de printopdracht heeft gegeven.						
16	Als er buiten het kantoor wordt gewerkt (bijvoorbeeld onderweg of thuis) dan moet die collega maatregelen treffen om te voorkomen dat iemand kan meekijken of meeluisteren als met vertrouwelijke informatie wordt gewerkt						
17	Als ik buiten het kantoorpand werk op een andere locatie, dan vind ik dat ik zakelijke informatie nooit onbeheerd mag laten als ik naar het toilet ga						
18	Wachtwoorden moeten gelijk gewijzigd worden als vermoed wordt dat iemand over de schouder heeft meegekeken welk wachtwoord er is ingetikt						
19	Vertrouwelijke informatie mag altijd mee naar huis worden genomen door een medewerker als het hem uit komt (bijvoorbeeld omdat hij thuis wil werken)						
20	Met mensen die niet op het kantoor werken, mogen geen vertrouwelijke werkgerelateerde gesprekken gevoerd worden (zoals thuis, met vrienden, op verjaardagsfeestjes etc.)						

Nr	Vraag	Antwoord					Eventuele opmerking
		Helemaal oneens	Oneens	Eens/ Oneens	Eens	Helemaal eens	
21	Mobiele apparaten die gebruikt worden voor zakelijke doeleinden dienen altijd voorzien te zijn van een toegangscode/wachtwoord						
22	Voordat een medewerker software (en/of apps) installeert, moet hij deze eerst gecontroleerd hebben op beveiligingsrisico's						
23	Het is belangrijk dat wanneer er een melding wordt gedaan op het mobiele apparaat van een softwareupdate, dat deze softwareupdate gelijk wordt doorgevoerd						
24	Voordat een medewerker zijn (mobiel) apparaat laat repareren of verkoopt, moet hij er altijd eerst voor zorgen dat de zakelijke gegevens ervan zijn gewist						
25	Medewerkers moeten op mobiele apparaten (laptops, tablets, mobieltjes e.d.) die zij gebruiken voor hun werk, kunnen installeren wat zij willen						
26	Medewerkers die privé apparaten ook voor zakelijke doeleinden gebruiken (zoals het raadplegen van werkmail), zijn ervoor verantwoordelijk dat zij een goede en up-to-date virusscanner en firewall hebben op eigen kosten						
27	Nooit en te nimmer mogen inloggegevens per email worden afgestaan						
28	Bij een mail die niet verwacht wordt of enigszins verdacht overkomt, moeten medewerkers de bijlagen op het werk kunnen openen om de echtheid van de mail te controleren						
29	Als een medewerker een mail ontvangt met een linkje daarin naar een website waarop men kan inloggen, dan moet een medewerker altijd voor het inloggen eerst de website op echtheid controleren (door te kijken of de url correct is weergegeven (url is http:www.'NAAM'.nl))						

Nr	Vraag	Antwoord					Eventuele opmerking
		Helemaal oneens	Oneens	Eens/ Oneens	Eens	Helemaal eens	
30	Medewerkers mogen er blindelings op vertrouwen dat men veilig kan internetten op het werk, omdat ICT hiervoor moet zorgen						
31	Gratis wifi is veilig om vertrouwelijke informatie mee te verwerken (lezen, versturen, bewerken)						
32	Vertrouwelijke informatie moet verstuurd en opgeslagen kunnen worden met internetdiensten als Hotmail, Gmail, Wetransfer, Dropbox en dergelijke						
33	Mede in het kader van vrije meningsuiting: Medewerkers moeten online kunnen communiceren over hun werk(gever) wat ze willen						

Nr	Vraag	Antwoord					Eventuele opmerking
		Nooit	Zelden	Zo nu en dan	Vaak	Altijd	
1	Ik pas de 10 gouden regels toe						
2	Als er onduidelijkheden zijn omtrent het veilig en verantwoord werken met (vertrouwelijke) informatie(middelen) dan raadpleeg ik de CISO (adviseur informatiebeveiliging)						
3	Ik spreek een collega aan als ik zie dat deze collega onjuist omgaat met informatie(middelen)						
4	Mensen die ik niet ken, laat ik niet toe om met mij mee het pand binnen te lopen naar de werkruimten						
5	Ik begeleid (of zorg voor begeleiding van) mijn extern bezoek (burgers, leveranciers e.d.) vanaf de receptie tot aan onze werkruimte en na afloop uiteindelijk weer tot aan de uitgang						
6	Mijn toegangspas draag ik zichtbaar						
7	Onbekende personen op mijn afdeling spreek ik aan						
8	Ik leen mijn toegangspas uit als een collega hierom vraagt						
9	Als ik vermoed dat vertrouwelijke informatie (door bijvoorbeeld diefstal of verlies) in handen is gekomen van een onbevoegde, dan meld ik dit (incident) direct aan mijn leidinggevende						
10	Als ik een verdachte zaak of situatie aantref, dan meld ik dit direct aan mijn leidinggevende						
11	Als ik mijn werkplek verlaat dan vergrendel ik mijn computerscherm						

Nr	Vraag	Antwoord					Eventuele opmerking
		Nooit	Zelden	Zo nu en dan	Vaak	Altijd	
12	Bij het verlaten van mijn werkplek, ook al is dat voor een overleg van 15 minuten, berg ik vertrouwelijke documenten op (achter slot en grendel)						
13	Als ik mijn werkplek verlaat, voor bijvoorbeeld een overleg, dan laat ik mijn mobieltje/usb-stick/laptop/tablet (of andere digitale gegevensdrager) nooit onbeheerd achter						
14	Ik deel (of heb eerder wel eens gedeeld) mijn persoonlijke wachtwoord met een collega						
15	Mijn vertrouwelijke printjes haal ik direct weg bij de printer						
16	Vertrouwelijke documenten gooi ik weg in speciale afgesloten containers/afvalbakken of doe ik door de versnipperaar						
17	Ik let heel goed op of niemand kan meekijken of meeluisteren als ik thuis of onderweg (in de trein of buiten bijvoorbeeld) met vertrouwelijke informatie werk						
18	Ik houd zakelijke informatie bij me en laat deze niet onbeheerd achter als ik buiten het kantoorpand werk						
19	Ik verander direct mijn wachtwoord als ik denk (of weet) dat iemand anders mijn wachtwoord heeft gezien						
20	Ik neem vertrouwelijke informatie mee naar huis als ik hiervoor expliciete toestemming heb van mijn leidinggevende						
21	Ik voer met mensen die niet mijn collega zijn vertrouwelijke gerelateerde gesprekken (thuis/met vrienden/etc)						

Nr	Vraag	Antwoord					Eventuele opmerking
		Nooit	Zelden	Zo nu en dan	Vaak	Altijd	
22	Als ik een privé apparaat (mobiel, laptop, tablet e.d.) gebruik voor mijn werk, dan zorg ik ervoor dat deze is voorzien van een toegangscode/wachtwoord						
23	Zonder na te denken over beveiligingsrisico's, installeer ik software (en/of apps)						
24	Als ik zie dat er een softwareupdate beschikbaar is, dan voer ik de softwareupdate gelijk uit						
25	Als ik mijn (mobiel) apparaat verkoop of laat repareren, dan zorg ik ervoor dat eerst de zakelijke gegevens er vanaf zijn gewist						
26	Als ICT mij niet wil helpen om software te installeren op mijn laptop dan ga ik op zoek naar hoe ik dit kan installeren zonder ICT						
27	Mijn privé apparaten die ik gebruik voor mijn werk (zoals het raadplegen van mijn mail) beschikken over een virusscanner die ik tevens regelmatig update						
28	Als ICT mij per email vraagt om mijn inloggegevens om te voorkomen dat mijn werkaccount wordt geblokkeerd, dan geef ik deze gegevens per email						
29	Als ik op mijn privémail een mail krijg dat ik een factuur van een bestelling van mijn werkgever binnen 7 dagen moet betalen, dan open ik de bijlage om te kijken of deze factuur wel voor mij is						
30	Ik controleer eerst de websites op waar ik naar toe wordt gelinkt vanuit een email op echtheid voordat ik op die website inlog						

Nr	Vraag	Antwoord					Eventuele opmerking
		Nooit	Zelden	Zo nu en dan	Vaak	Altijd	
31	Als op een website staat 'U hebt een prijs gewonnen, klik hier om uw prijs op te halen' dan klik ik daarop						
32	Ik gebruik gratis wifi om mee te werken, zoals het lezen van mijn werkmaill						
33	Ik maak gebruik van internetdiensten als Hotmail, Gmail, Wetransfer, Dropbox en dergelijke om vertrouwelijke informatie mee te versturen of op te slaan (zodat ik bijvoorbeeld extern met deze informatie kan werken)						
34	Ik let erop dat ik online geen zaken communiceer die schadelijk kunnen zijn voor mijn werk(gever)						

Controlevragen

Nr	Vraag	Antwoord
1	Stel je wilt thuiswerken en vraagt je af hoe je dit op een veilige en verantwoorde wijze kunt doen. Wie kan deze vraag vanuit zijn functie beantwoorden?	
2	Stel je bent een gevoelig collegevoorstel verloren toen je buiten het kantoor werkte. Aan wie moet je dit melden?	
3	Met welke toetsencombinatie kun je jouw computerscherm op het werk vergrendelen (locken)?	
4	Wanneer is informatie vertrouwelijk?	
5	Stel je zit in de trein en je vermoed dat de persoon naast je met je heeft meegekeken toen je inlogte op je laptop om je werkmail te kunnen raadplegen. Wat doe je?	
6	Wat is het risico als je werkt met software dat prima functioneert, maar waarvoor al een maand een nieuwe update voor beschikbaar is?	
7	Noem drie punten waaraan je een verdachte mail kunt herkennen (een mail waarvan je vermoed dat deze uit is op je inloggegevens)	
8	Stel je bent aan het internetten en de website geeft aan dat je de 100.000e bezoeker bent en dat je een prijs hebt gewonnen. De website geeft aan 'KLIK HIER OM JE PRIJS OP TE HALEN'. Waarom is het gevaarlijk is je daarop klikt?	
9	Waarom is het gevaarlijk om gratis wifi te gebruiken als je werkt met vertrouwelijke zakelijke informatie op je mobiele apparaat?	
10	Waarom is het onverstandig om documenten te versturen vanuit je werkmail naar je privémail om thuis te kunnen werken?	

Nr	Vraag	Antwoord (1-5)
1	Stel je bent op je werk en je ziet dat een collega onjuist (niet vertrouwelijk) omgaat met vertrouwelijke informatie. Op schaal van 1 tot 5: in hoeverre vind jij het noodzakelijk dat jij je je collega hierop aanspreekt? (1 is helemaal niet noodzakelijk, 5 is heel noodzakelijk)	
2	Je hebt op je werkplek overleg gehad met een externe. Het overleg is afgelopen en je moet snel naar het volgende overleg. Met de externe heb je al vaker overleg gehad en hij weet inmiddels zelf wel hoe hij bij de uitgang moet komen. In hoeverre vind je het noodzakelijk om hem eerst naar de uitgang te begeleiden voordat je naar je overleg gaat? Op een schaal van 1 tot 5 (1 is helemaal niet noodzakelijk, 5 is heel noodzakelijk)	
3	Je zit te werken op je werkplek. Een voor jou onbekend persoon komt de afdeling opgelopen en pakt een dossier het bureau van een collega die met vakantie is. Deze persoon vertelt dat hij dat dossier nodig heeft voor het overleg met een collegelid. In hoeverre vind jij het noodzakelijk om hem aan te spreken en te controleren wie hij is? (1 is helemaal niet noodzakelijk, 5 is heel noodzakelijk)	
4	Je bent op je werkplek druk aan het werk met een vertrouwelijk dossier. Je werkt een collegevoorstel op je computer uit. Tussentijds wil je even koffie halen. Op een schaal van 1 tot 5 (waarbij 1 heel onbelangrijk en 5 heel belangrijk vertegenwoordigt), hoe belangrijk vind je het om dan je computerscherm te vergrendelen?	
5	Je hebt het enorm druk op je werk. Daarom zit je ook op een werkplek waar geen collega's zitten. Op je bureau ligt een vertrouwelijk dossier, je werkmobieltje en een usb'tje. Je gaat in een overleg van ongeveer 10 minuten. In hoeverre vind jij het belangrijk om eerst al je spullen op te bergen, zodat deze niet onbeheerd blijven liggen? Op een schaal van 1 tot 5 (waarbij 1 heel onbelangrijk en 5 heel belangrijk vertegenwoordigt)	
6	Je gaat met vakantie en je verwacht in die periode een belangrijke mail te krijgen die het college moet lezen. Je achtervang (of een andere collega) werkt wel in jouw vakantieperiode en kan jouw mailbox in de gaten houden - en de mail doorsturen aan het college als je deze hebt ontvangen. Hiervoor moet je dan wel je inloggegevens aan hem geven gedurende de vakantieperiode. In hoeverre vind je dat het tijdelijk afstaan van inloggegevens moet kunnen, gezien deze situatie. Op een schaal van 1 tot 5 (waarbij 1 helemaal niet kunnen en 5 moet altijd kunnen vertegenwoordigt).	
7	Je wil thuiswerken op je eigen laptop. Je wil net beginnen en beseft ineens dat je nog geen virusscanner hebt. Deze kun je installeren voor €45. Dit moet je uit eigen zak betalen, want je werkgever gaat deze niet vergoeden. In hoeverre voel jij je verantwoordelijk om dit te installeren op je eigen kosten. Op een schaal van 1 tot 5 (waarbij 1 helemaal niet verantwoordelijk en 5 heel erg verantwoordelijk vertegenwoordigt)	
8	Je zit lekker op het terras in het zonnetje met je laptop. Dit terras beschikt over gratis wifi. Dat is wel zo handig. Je wil namelijk deze middag nog snel iets afhandelen voor je werk, zodat je dit niet morgen hoeft te doen. Hiervoor moet je inloggen op een systeem van je werk. Zonder gratis wifi kun je namelijk niet inloggen. In hoeverre vind je het veilig (c.q. verantwoord) om deze wifi te gebruiken? Op een schaal van 1 tot 5 (waarbij 1 heel onveilig en 5 heel veilig vertegenwoordigt)	
9	Je wil morgen thuis kunnen werken aan een vertrouwelijk dossier. Hiervoor moet je beschikken over digitale vertrouwelijke rapporten. Zonder deze rapporten heeft het geen zin om thuis te kunnen werken. Je kan vanuit huis namelijk niet bij je werkmail. In hoeverre vind je dat het moet kunnen dat je deze informatie naar je privémail stuurt? Op een schaal van 1 tot 5 (waarbij 1 heel onveilig en 5 heel veilig vertegenwoordigt)	
10	Op een website lees je een artikel van vorige week dat het college verwacht dat de lokale belastingen niet stijgen. Onder dit artikel staan allerlei reacties van blije burgers. Jij weet sinds gisteren dat het college werkt aan een raadsvoorstel om de OZB-belasting (belasting op koopwoningen) met 2% te laten stijgen. In hoeverre vind je dat je zo vriendelijk mag zijn om in een reactie op dat artikel te vermelden dat de strekking van het artikel is achterhaald en dat er waarschijnlijk toch een lichte belastingstijging komt? Het is namelijk wel zo eerlijk en transparant als men dit weet. Op een schaal van 1 tot 5 (waarbij 1 aangeeft dat dit nooit mag en 5 aangeeft dat dit altijd moet kunnen).	

Nr	Vraag	Antwoord
1	Een collega van je heeft een cliëntendossier op zijn bureau liggen. Hij loopt weg om met pauze te gaan en laat het dossier op zijn bureau liggen. Wat doe je?	
2	Je loopt het stadhuis binnen om naar je werkplek te gaan. Iemand die jij niet kent heeft zijn handen vol en vraagt of je zo vriendelijk wil zijn om de deur open te houden, zodat hij niet eventueel een toegangspas hoeft te pakken. Wat doe je?	
3	Je bent druk aan het werk op je afdeling. Er loopt iemand de afdeling op die je niet kent, zoals zo vaak - wellicht van een andere afdeling. Wat doe je?	
4	Je gaat met vakantie. Je collega, die nieuw is en over 3 dagen pas zijn toegangspas krijgt, vraagt of hij tot die tijd jouw toegangspas mag lenen. Hoe ga je hier mee om?	
5	Stel je hebt thuis gewerkt met papieren vertrouwelijke documenten. Je gaat met het openbaar vervoer naar je werk en je komt op je werk aan. Je constateert dat je een deel van de documenten kwijt bent. Eenmaal thuis ga je op zoek naar deze documenten, maar je hebt ze niet gevonden. Wat doe je, nu je weet dat het mogelijk is dat deze documenten in handen zijn gekomen van iemand anders die deze informatie niet tot zich mag nemen?	
6	Een tijdelijke collega die jou komt helpen is van bijna alle toegangsmiddelen voorzien. Hij is nog maar drie dagen aanwezig, maar heeft voor een specifiek systeem geen inloggegevens. In dat systeem moet hij wat belangrijke gegevens raadplegen - anders kan hij niet verder. Jij hebt wel toegang tot dat systeem. Hoe zorg je ervoor dat hij voor deze drie dagen in dat systeem kan?	
7	Je zit in de avondspits in de bus naar huis. Je wordt gebeld door een collega die bij de portefeuillehouder zit omtrent een vertrouwelijk dossier. De portefeuillehouder wil wat weten en dat is nogal urgent. Hoe ga je om met dit verzoek (zoals gezegd, het is druk in de bus)?	
8	Je wil morgen thuiswerken en je staat op het punt om nu naar huis te gaan van het werk. Om morgen te kunnen thuiswerken, moet je beschikken over een dossier met informatie die niet openbaar mag worden. Wat doe je?	
9	Je werkt thuis op je eigen laptop. Je krijgt een melding dat een software update klaar staat voor installatie. Wat doe je met deze melding?	
10	Je wilt op je werkcomputer een software installeren dat een aantal werkzaamheden voor je eenvoudiger maakt. ICT wil je hier niet bij helpen. Een collega, die handig is met computers, stelt jou voor om dit voor je te doen. Zou je gebruik maken van zijn aanbod?	

Bijlage 10 Vragenlijst t.b.v. interview met ambtenaar

Introductie bestaande uit:

- Toelichten dat er een VNG-resolutie is aangenomen die gemeenten voorschrijft dat en hoe informatiebeveiliging moet worden vormgegeven;
- Aanstippen dat de BIG de normenset voor informatiebeveiliging is en dat deze technische, organisatorische en gedragsmaatregelen voorschrijft;
- Aangeven dat het onderzoek zich verhoudt tot gedragsmaatregelen en dat het onderzoek zich focust op het meten van het informatiebeveiligingsbewustzijnniveau. Aangeven dat de mens (gedrag) een belangrijke factor is om de informatiebeveiliging te waarborgen, omdat vele technische en organisatorische maatregelen door medewerkers omzeild kunnen worden door procedures en beleid niet na te leven;
- Doel van onderzoek kenbaar maken en aangeven dat er een model is ontwikkeld dat het informatiebeveiligingsniveau van medewerkers meet binnen een gemeentelijke organisatie;
- Toelichten dat het hierbij gaat om de componenten kennis, houding en gedrag, en uitleggen wat met deze componenten wordt bedoeld;
- Aangeven dat de bovengenoemde componenten gemeten worden met het model middels een vragenlijst en dat dit interview bedoeld is om te kijken of deze vragenlijst voor medewerkers begrijpelijk en haalbaar is;
- Verloop van het interview bespreken (medewerker vult vragenlijst in en als dit is gedaan dan pas start het interview. Het gaat hierbij uitdrukkelijk niet om de gegeven antwoorden, maar om de begrijpelijkheid en haalbaarheid van de vragenlijst);
- Anonimiteit en vertrouwelijkheid bespreken;
- Aangeven dat er een verslag wordt opgesteld, die na afloop binnen een week aan hen wordt gestuurd om deze goed te keuren voordat de resultaten uit het interview worden verwerkt;
- Verifiëren of het duidelijk is en dan vragenlijst uitleggen. Aangeven dat het gesloten vragen zijn en dat als vragen of definities onduidelijk zijn dat ze hierbij een sterretje zetten zodat dit naderhand kan worden besproken;
- Starten met invullen vragenlijst door medewerker en de tijdsduur meten.

Semigestructureerd interview
Onderstaande vragen stellen en hierop doorvragen indien relevant

Aspect ‘Begrijpelijk’
Vragen om te beoordelen of de methodiek/vragenlijst begrijpelijk is.
Begrijpelijk is in de definitielijst gedefinieerd als:

Het model is eenvoudig toe te passen. De vragen en antwoordcategorieën uit de survey, welke zijn afgeleid van het model, zijn eenvoudig en helder voor de personen die de vragen moeten beantwoorden. Dit uit zich doordat de vragenlijst zelfstandig kan worden ingevuld zonder dat de vragen en antwoordcategorieën uitgelegd moeten worden.

Deze definitie benoemen en vervolgens onderstaande vragen stellen.

Algemeen
Voordat we de vragen één voor één doorlopen op begrijpelijkheid:

1. Wat is je algemene eerste indruk ten aanzien van de begrijpelijkheid van de totale vragenlijst?
2. Bij welke vragen en bij welke definities heb je een sterretje staan? *(deze sterretjes worden besproken als elke vraag uit de survey specifiek wordt bevraagd)*
3. In hoeverre is het mogelijk alle vragen te beantwoorden zonder dat je nog een toelichting of uitleg nodig hebt over wat er met een vraag of antwoordcategorie wordt bedoeld?

Per vraag uit de survey de volgende vragen stellen:

4. In hoeverre is de vraag op jouw werksituatie van toepassing?
5. Ten aanzien van de begrippen in de vraag: welke begrippen in deze vraag moeten uitgewerkt worden omdat de vraag anders niet eenduidig te beantwoorden is?
6. Wat vind je van de helderheid van de vraag?
7. In hoeverre kun je op basis van de gegeven antwoordopties de vraag eenvoudig[9] beantwoorden?

Aspect 'Haalbaar'
Vragenlijst om te beoordelen of de methodiek/vragenlijst haalbaar is.
Haalbaar is in de definitielijst gedefinieerd als:

De verhouding tijdsduur versus het aantal vragen is voor de onderzoeker en de personen die de surveyvragen beantwoorden acceptabel, waardoor de betrouwbaarheid van de antwoorden zoveel mogelijk wordt gewaarborgd.

Deze definitie benoemen en vervolgens onderstaande vragen stellen.

1. Ik geef aan hoe lang zij over de vragenlijst hebben gedaan en stel dan de vraag: Wat vind je van de tijdsduur dat je hebt gedaan over deze vragenlijst?
2. Wat is voor jou ongeveer de maximale tijdsduur om deze vragenlijst bereidwillig én tegelijk zorgvuldig te beantwoorden?
3. Wat vind je van het aantal vragen?
4. In hoeverre heb je alle vragen met evenveel zorg gelezen en beantwoord? *(NB ivm de betrouwbaarheid van de beantwoording is 'afraffelen' ongewenst. Vragen dienen aandachtig gelezen te worden en zorgvuldig te worden beantwoord)*
5. Wat is jouw bevinding op het aantal vragen dat je is gesteld versus de tijd die je erover hebt gedaan?

[9] Zonder er lang over na te denken (ter indicatie: 15 seconden ongeveer) kun je de vraag beantwoorden en geeft de antwoordoptie ook het antwoord weer dat je wil geven

Bijlage 11 Interviewverslagen met negental medewerkers samengevat

Per interviewvraag staan de antwoorden opgesomd die de medewerkers hebben gegeven.

Vragenlijst

Semigestructureerd interview
Onderstaande vragen stellen en hierop doorvragen indien relevant

Aspect 'Begrijpelijk'
Vragen om te beoordelen of de methodiek/vragenlijst begrijpelijk is.
Begrijpelijk is in de definitielijst gedefinieerd als:

Het model is eenvoudig toe te passen. De vragen en antwoordcategorieën uit de survey, welke zijn afgeleid van het model, zijn eenvoudig en helder voor de personen die de vragen moeten beantwoorden. Dit uit zich doordat de vragenlijst zelfstandig kan worden ingevuld zonder dat de vragen en antwoordcategorieën uitgelegd moeten worden.

Deze definitie benoemen en vervolgens onderstaande vragen stellen.
Algemeen
Voordat we de vragen één voor één doorlopen op begrijpelijkheid:

1. Wat is je algemene eerste indruk ten aanzien van de begrijpelijkheid van de totale vragenlijst?

Antwoord

- De vragen helder en begrijpelijk. Bij sommige gedragsvragen worden vragen gesteld in de hypothetische vorm 'als dit zich voordoet, wat doe je dan?'. Maar niet al die situaties hebben zich bij mij voorgedaan of slechts 1 keer. Hoe ga je dan met de antwoordcategorieën om van nooit en altijd. Dat moet bij de introductie dan worden aangegeven;
- Mijn eerste indruk is dat de vragenlijst begrijpelijk is. Ik begrijp de vragen en de onderwerpen die erin worden benoemd. Het is goed te volgen;
- De vraagstelling is helder en de manier om het in te vullen was prettig. Ook is het prettig om ruimte te hebben voor eventuele opmerkingen. Het opmerkingenveld wordt gebruikt om verbeteringen mee te geven voor de vragenlijst of om antwoorden wat meer te nuanceren. Zoals het antwoord geven op vragen of ik risico's ken of dat ik bepaald gedrag laat zien, dan moet ik een 'ja' of 'altijd' als antwoord iets nuanceren omdat ik bijvoorbeeld niet alle risico's ken of omdat ik maar eenmaal in een situatie ben terechtgekomen waarin ik dat specifieke gedrag hoefde te vertonen;
- Op zichzelf is de vragenlijst helder. Dit geldt idem dito voor de antwoord categorieën. Bij een aantal vragen heb ik een wat opmerkingen, die bij vraag 2 aan de orde komen.
- Mijn algemene indruk is dat de vragenlijst begrijpelijk is. Ik snap en begrijp de vragen, en kan deze in grote mate zelfstandig invullen. Er zijn een paar punten die de vragenlijst qua begrijpelijkheid kunnen verbeteren. Die staan bij vraag 2;
- De vragen zijn goed te doen. Een aantal vragen is niet op mijn situatie van toepassing en een aantal vragen is lastig te beantwoorden, doordat de tijdrange van invloed daarop is. Als ik naar het toilet ga dan laat ik mijn spullen wel even

onbeheerd, maar ga ik naar een overleg/vergadering dan ruim ik alles op. Dit aspect wordt bij vraag 2 behandeld.

- Mijn eerste indruk is dat de vragenlijst begrijpelijk is. Ik heb alle vragen kunnen beantwoorden;
- Er zijn een paar kleine opmerkingen (zie vraag 2). Overigens voor zowel de kennis, houdings- en gedragsvragen: de term 'kantoorpand' is niet gebruikelijk bij gemeenten. Deze term is gebruikelijk in het bedrijfsleven. Bij gemeenten spreekt men sneller over een stadhuis/gemeentehuis;
- De vragen en antwoordcategorieën zijn mij helder en duidelijk. Sommige gedragsvragen zijn lastig te beantwoorden omdat sommige situaties nooit of zelden voorkomen. Hoe past een antwoordcategorie als zelden, altijd of vaak dan op een vraag die gaat over een situatie die zich bijvoorbeeld maar eenmaal heeft voorgedaan?;
- Paar vragen zijn niet begrijpelijk (zie vraag 2). De rest van de vragen zijn helder, waar ook geen toelichting op nodig is.

2. Bij welke vragen en bij welke definities heb je een sterretje staan? *(deze sterretjes worden besproken als elke vraag uit de survey specifiek wordt bevraagd)*

Antwoord

- Kennisvragen:
    - Vraag 1 'Ik ken de 10 gouden gedragsregels':
        - wat is kennen? Ik weet dat ze er zijn, maar ik kan ze niet alle 10 opsommen;
        - wat is 'ken';
        - wat houdt 'kennen' in? Ik weet dat er 10 gouden regels zijn, maar ik kan deze niet alle 10 opsommen;
        - wat bedoel je met kennen? Er kennis van hebben genomen of is het de bedoeling om alle 10 de gouden regels te kunnen opsommen? Het begrip kan op meerdere manieren worden uitgelegd;
        - dit kan op verschillende manieren worden uitgelegd. Dit moet concreter worden aangegeven, dan wel gedefinieerd worden;
        - waar gaan de gouden regels over. Voeg toe dat het betrekking heeft op informatiebeveiliging.
    - Vraag 2 'Ik weet waar ik de CISO voor kan raadplegen':
        - wat of wie is een CISO;
        - waar staat CISO voor?;
        - de definitie CISO is onbekend. Deze definiëren of anders benoemen. Dit geldt ook voor houdingsvraag nr. 2;
        - de afkorting van CISO, en wat de CISO doet, is onbekend;
        - wat is een CISO;
        - waar staat CISO voor en wat doet deze doet.
    - Vraag 3 'Ik weet waarom er van mij wordt verwacht dat ik een collega aanspreek als ik zie dat deze collega onjuist omgaat met informatie(middelen)':
        - ingewikkeld. Twee dingen lopen door elkaar heen. Wil je weten waarom of dat er wat wordt gevraagd. Je veronderstelt dat er al iets van me wordt gevraagd;
        - de zinsnede is lastig: ik weet waarom.. dat.. als ik zie.. → te lange zin;

        - deze vraag komt iets te vroeg. De vervolgvragen geven namelijk voorbeelden over wat onjuist omgaan met informatie betekent. Beter kun je deze dus later stellen.
    - Vraag 4/5/6/7: vragen lijken op elkaar;
    - Vraag 6 ‘Ik weet waarom ik mijn toegangspas zichtbaar moet dragen’:
        - deze vraag is niet van toepassing op onze gemeente, want wij beschikken niet over toegangspassen.
    - Vraag 9 ‘Wanneer ik vertrouwelijke informatie ben verloren en vermoed dat het mogelijk is dat dit in handen is gekomen van onbevoegden dan weet ik aan wie ik dit (incident) moet melden’:
        - lange zin: verloren én vermoed. Ik ben iets verloren, dan kan het toch altijd dat het in handen is gekomen van onbevoegden (verloren betekent al dat ik niet weet in wiens handen het zich bevindt);
        - inhoudelijk vraag: waarom niet : als ik vertrouwelijke;
        - lange zin: in stukjes ‘hakken’. En als ik het verloren ben is al een probleem op zichzelf. Moet ik het ook vermoeden? Vermoeden kan eruit.
    - Vraag 12 ‘Ik kan de mogelijke schade overzien voor de organisatie of de burger als ik vertrouwelijke documenten op mijn bureau laat liggen als ik mijn werkplek verlaat’:
        - ik denk wel dat ik de schade kan overzien maar kan ze niet goed benoemen (nuancering op de ‘ja’).
    - Vraag 13 ‘Ik weet wat de gevolgen kunnen zijn als ik een usb/mobieltje/laptop/tablet op mijn werkbureau laat liggen als ik even in overleg ga’:
        - Ik weet een aantal gevolgen, maar kan ze niet alle benoemen en wil deze daarom nuanceren als ik ‘ja’ in vul.
    - Vraag 14 ‘Ik weet welke risico's het delen van mijn wachtwoord met collega's kan hebben voor de continuïteit van de dienstverlening en voor burgers’:
        - continuïteit en dienstverlening – vrij abstract (kan politieke rel veroorzaken, of op mijn kop krijgen. Imagoschade werk etc). Kan ellende uitkomen maar hoeven niet deze twee effecten te zijn. Is afhankelijk van de afdeling en soort informatie.
        - continuïteit van burgers en dienstverlening – waarom die toevoeging? Kan dit er ook af?;
        - ik weet wel een aantal risico’s, maar als ik ‘ja’ in vul wil ik deze nuanceren want ik ken niet alle risico’s.
    - Vraag 17 ‘Ik weet wanneer informatie vertrouwelijk is’:
        - is een hele absolute vraag. Bij de beantwoording wil ik het antwoord nuanceren. Ik weet het voor een groot deel.
    - Vraag 18 ‘Ik weet welke informatie(middelen) bedrijfskritisch zijn voor mijn organisatie (…)’:
        - de vraag impliceert dat je alle bedrijfskritische informatie(middelen) kent. Ik ken er een aantal, maar niet alle. Dit begrip meer afbakenen;
        - toevoegen ‘bijvoorbeeld’ →‘die BIJVOORBEELD een grote impact hebben op’.
    - Vraag 19 ‘Ik weet welke maatregelen ik kan treffen om te voorkomen dat iemand kan meekijken of meeluisteren als ik buiten het kantoor met vertrouwelijke informatie werk’:

        - gaat over meekijken/meeluisteren: de vergaderkamers bij onze gemeente zijn vrij gehorig;
        - ik weet wel een aantal maatregelen, maar als ik ‘ja’ in vul wil ik deze nuanceren want ik ken niet alle maatregelen.
    - Vraag 21 ‘Ik weet wat ik moet doen als ik vermoed dat iemand mijn wachtwoord heeft gezien doordat hij meekeek over mijn schouder op het scherm (van mijn laptop/mobiel etc.)’:
        - de tekst vanaf‘ mijn schouder’ zou eruit kunnen.
    - Vraag 23 ‘Ik weet wat het risico is als ik vertrouwelijke werkgerelateerde gesprekken voer buiten het kantoor met mensen die niet bij mij op het kantoor werken (bijvoorbeeld in de trein, op terras of op een verjaardagsfeestje)’:
        - situatie doet zich niet voor, ik heb het nooit inhoudelijk over mijn werk buiten het kantoor.
    - Vraag 24 ‘Een van de basisbeveiligingsmaatregelen is het hebben van een wachtwoord/toegangscode op (privé) mobiele apparaten (mobiel, laptop, tablet), zeker als ik deze gebruik om zakelijke informatie mee te lezen (zoals werkmail)’:
        - ik weet is weggelaten (consistentie);
        - in tegen stelling tot alle andere vragen is deze anders opgesteld. Ik mis ‘ik weet’. De vragen in dezelfde lijn met de andere vragen houden voor de leesbaarheid;
        - er staat een vraagteken – die kan eruit. Het is een stelling.
    - Vraag 27 ‘Ik weet waarom het belangrijk is dat bij reparatie of verkoop van een (mobiel) apparaat eerst de zakelijke gegevens van het apparaat moet worden zijn gewist’:
        - gaat het om privévragen of zakelijke mobiel? Ik verkoop niet de zakelijke mobiel. Deze vraag aanscherpen. Het gaat hierbij ook om het verwijderen/weggooien;
        - woordje ‘worden’ kan eruit.
    - Vraag 28 ‘Ik weet wat de gevolgen kunnen zijn als niet ICT maar ikzelf software installeer op mijn mobiele apparaten (laptop, mobiel, tablet e.d.)’:
        - is een lastige vraag. Voor een deel moet je zelf software installeren, zoals op de iPhone die je van het werk hebt gekregen. Op de vaste computers is het een ander verhaal, die worden beheerd door ICT;
        - taalfout – installeert –t;
        - spelfout bij installeert, moet zijn installeer.
    - Vraag 29 ‘Ik weet wat het belang is van een goede up-to-date-virusscanner en een firewall op mijn privé apparten ….’:
        - spelfout bij apparten, moet zijn apparaten.
    - Vraag 32 ‘Ik weet waarom ik de website op echtheid moet controleren als ik op de website wil inloggen als ik vanuit een email naar deze website wordt doorgestuurd (toegelinkt)’:
        - Waarom en dat – veronderstelt dat ze het moeten doen laat staan hoe ze het moeten doen. Maar deze kun je laten staan – ik weet wel waarom, maar niet dat en hoe;
        - taalopmerking: ‘de’ website vervangen voor ‘een’ website.
- Houdingsvragen:
    - Algemeen: kies voor één vorm: bij kennis is het ‘ik weet’ en kijk ik naar mijzelf. Bij houding is dit niet meer het geval. Dan kan ik niet meer naar

mijzelf, maar is de vraagvorm vanuit de ik-persoon omgezet naar ‘algemene’ stellingen. Het helpt als je mij als lezer echt aanspreekt door bijvoorbeeld de stellingen om te buigen naar ‘ik vind’;

- Vraag 1 ‘De 10 gouden regels zijn eenvoudig toe te passen’:
  - wat is toepassen? Begeleiden en aanspreken is goed toepasbaar. Maar het durven van aanspreken is een ander aspect.
- Vraag 2 ‘Vragen en onduidelijkheden over veilig en verantwoord werken met (vertrouwelijke) informatie(middelen) moeten aan de CISO gesteld worden’:
  - definitie CISO toelichten;
  - ik zou hem ook aan ICT of aan leidinggevende vragen. Wil niet per se zeggen dat ik het niet doe, maar dat ik het niet aan jou vraag;
  - taalfout omtrent stellen. Vragen stel je, onduidelijkheden meld je;
  - afkorting CISO onbekend;
  - definitie CISO onbekend;
  - waarvoor staat CISO? Dit specificeren.
- Vraag 4 ‘Elke personeelslid dat via de personeelsingang het pand betreedt richting de werkruimten, is er voor verantwoordelijk dat hij moet voorkomen dat onbevoegden met hem mee het pand in lopen’:
  - personeelslid is te nauw genomen. Het gaat ook om externen e.d. (alle gebruikers van het pand, die een toegangspas hebben voor de personeelsingang).
- Vraag 6 ‘Het is belangrijk om de toegangspas zichtbaar te dragen’:
  - toegangspas zichtbaar dragen: heb ik gewoon mee of in de tas zitten. Waarom is dat belangrijk? Vraag is terecht: maar vraag me dan af waarom iemand wil dat ik dat doe. Bij kennisvraag dan stellen: ik weet waarom ik het moet dragen;
  - we maken geen gebruik van toegangspassen.
- Vraag 8 ‘Toegangspassen mogen aan niemand uitgeleend mogen worden’:
  - niet altijd van toepassing (bij iedereen waarschijnlijk).
- Vraag 10 ‘Verdachte zaken en situaties moeten altijd aan de leidinggevende worden gemeld’:
  - inhoudelijk opmerking: een leidinggevende is er ook niet altijd. Wat doe je dan? Het gaat erom dat het wordt gemeld;
  - wat als een leidinggevende er niet is (dan aan een vervanger of een MT-lid of..?)?.
- Vraag 12 ‘Bij het verlaten van de werkplek moeten vertrouwelijke documenten altijd worden opgeborgen (achter slot en grendel)’: komt vaker terug deze manier:
  - wat is vertrouwelijk (definiëren);
  - soms berg ik spullen wel op, maar niet achter slot en grendel. Doordat dit achter haakjes staat, kun dit tot verwarring leiden hoe je de vraag moet beantwoorden;
  - ik werk hier met collega’s, dus ik vind het niet relevant. Moet elkaar ook vertrouwen.
- Vraag 14 ‘Wachtwoorden mogen niet gedeeld worden met een collega als de er iemand …’:
  - taalfout ‘als de er’.
- Vraag 15 ‘Vertrouwelijke printjes moeten altijd direct bij de printer worden weggehaald door de medewerker die de printopdracht heeft gegeven’:

        - hier niet meer van toepassing, kan alleen met code printen;
        - binnenkort kunnen we alleen nog maar beveiligd printen, dan is deze vraag hier niet van toepassing;
        - in de nabije toekomst kan er alleen beveiligd worden geprint. Dan is de vraag niet van toepassing of er moet een vraag gesteld worden over beveiligd printen.
    - Vraag 16 ‘Als er buiten het kantoor wordt gewerkt (bijvoorbeeld onderweg of thuis) dan moet die collega maatregelen treffen om te voorkomen dat iemand kan meekijken of meeluisteren als met vertrouwelijke informatie wordt gewerkt’:
        - het woord maatregelen doet aan technische maatregelen denken, terwijl ik er bijvoorbeeld voor zorg dat ik vertrouwelijke gesprekken niet in de tuin voer. Het woordje ‘maatregelen’ kan je op het verkeerde been zetten.
    - Vraag 17 ‘Als ik buiten het kantoorpand werk op een andere locatie, dan vind ik dat ik zakelijke informatie nooit onbeheerd mag laten als ik naar het toilet ga’:
        - wat bedoel je concreet met andere locatie? Op een terras is dat logisch, maar thuis is weer een andere situatie.
    - Vraag 18 ‘Wachtwoorden moeten gelijk gewijzigd worden als vermoed wordt dat iemand over de schouder heeft meegekeken welk wachtwoord er is ingetikt’:
        - vanaf vraag 19 is een andere vraagstelling waardoor de antwoorden omgedraaid worden omdat bijna alle vragen positief zijn geformuleerd. Wat is handig?.
    - Vraag 20 ‘Met mensen die niet op het kantoor werken, mogen geen vertrouwelijke werkgerelateerde gesprekken gevoerd worden (zoals thuis, met vrienden, op verjaardagsfeestjes etc.)’:
        - ik heb het wel eens met mijn partner over. Concreter maken. Met partner bespreek ik wel eens situaties/casussen om hart te luchten. Doe je het zorgvuldig en anonimiseer je het;
        - ook met mensen die wel op het kantoor werken bespreek ik niet alle vertrouwelijke zaken met iedereen.
    - Vraag 22 ‘Voordat een medewerker software (en/of apps) installeert, moet hij deze eerst gecontroleerd hebben op beveiligingsrisico's’:
        - moet hier niet staan dat het om nieuwe software gaat?
    - Vraag 23 ‘Het is belangrijk dat wanneer er een melding wordt gedaan op het mobiele apparaat van een software update, dat deze software update gelijk wordt doorgevoerd’:
        - vraag op zichzelf is helder, maar ICT heeft wel eens aangegeven dat ik met een iOS-update moest wachten, dus nu ben ik er wat minder snel mee.
    - Vraag 24 ‘Voordat een medewerker zijn (mobiel) apparaat laat repareren of verkoopt, moet hij er altijd eerst voor zorgen dat de zakelijke gegevens ervan zijn gewist’:
        - gaat het om alle gegevens of vertrouwelijke gegevens? Vooral dat laatste is namelijk belangrijk. De vraag kan hier gespecificeerd worden.

- Vraag 25 ‘Medewerkers moeten op mobiele apparaten (laptops, tablets, mobieltjes e.d.) die zij gebruiken voor hun werk, kunnen installeren wat zij willen’:
  - wat bedoel je precies? Een app voor het weer, mag ik die niet op mijn tablet zetten en moet ik hiervoor ICT benaderen? Over welke software en apps gaat het hier? Dit moet een verschil voor een interpretatie van de vraag.
- Vraag 29 ‘Als een medewerker een mail ontvangt met een linkje daarin naar een website waarop men kan inloggen, dan moet een medewerker altijd voor het inloggen eerst de website op echtheid controleren (door te kijken of de url correct is weergegeven (url is http:www.'NAAM'.nl))’:
  - weet niet of het handig is of de toevoeging tussen haakjes wat toevoegt.
- Vraag 30 ‘Medewerkers mogen er blindelings op vertrouwen dat men veilig kan internetten op het werk, omdat ICT hiervoor moet zorgen’:
  - heeft een dubbele lading. ICT moet wel zorgen voor veilige wifi-verbinding. Maar ik ben verantwoordelijk voor mijn gedrag, welke e-mails ik open e.d. Vraag iets aanscherpen.

- Gedragsvragen:
  - Algemene opmerking:
    - vragen zijn helder, alleen hoe beantwoord ik een gedragsvraag als de situatie zelden of vaak voor doet?.
  - Vraag 1 ‘Ik pas de 10 gouden regels toe’:
    - ik pas toe: verschilt per regel of ik het vaak doe of niet;
    - veel pas ik wel toe, maar sommigen niet. Hoe interpreteer ik dan een antwoordcategorie als vaak.
  - Vraag 2 ‘Als er onduidelijkheden zijn omtrent het veilig en verantwoord werken met (vertrouwelijke) informatie(middelen) dan raadpleeg ik de CISO (adviseur informatiebeveiliging)’:
    - kan ook iemand anders raadplegen dan CISO (ICT, leidinggevende);
    - CISO specificeren/definiëren.
  - Vraag 4 ‘Mensen die ik niet ken, laat ik niet toe om met mij mee het pand binnen te lopen naar de werkruimten’:
    - niet altijd toepasbaar. Als ik de persoon niet ken dan vraag ik het wel en loop ik met deze persoon mee, maar ik kan de identiteit niet controleren, dus ben genoodzaakt om hun verhaal dan te geloven (als zij zeggen dat zij bijvoorbeeld hier werken of van een andere gemeente zijn);
    - dubbele ontkenningen lezen niet fijn en vergroten de kans op foutieve antwoorden.
  - Vraag 7 ‘Onbekende personen op mijn afdeling spreek ik aan’:
    - aanspreken klinkt negatief. Dit kan vervangen worden door ‘vragen’. Dat klinkt vriendelijker.
  - Vraag 9 ‘Als ik vermoed dat vertrouwelijke informatie (door bijvoorbeeld diefstal of verlies) in handen is gekomen van een onbevoegde, dan meld ik dit (incident) direct aan mijn leidinggevende’:
    - vermoeden vind ik niet van belang. Er dient gemeld te worden.
  - Vraag 11 ‘Als ik mijn werkplek verlaat dan vergrendel ik mijn computerscherm’:

        - ik mis hier een tijdrange.
    - Vraag 13 ‘Als ik mijn werkplek verlaat, voor bijvoorbeeld een overleg, dan laat ik mijn mobieltje/usb-stick/laptop/tablet (of andere digitale gegevensdrager, nooit onbeheerd achter’:
        - de dubbele ontkenning leest niet fijn;
        - dubbele ontkenning leest lastig.
    - Vraag 15 ‘Mijn vertrouwelijke printjes haal ik direct weg bij de printer’:
        - niet van toepassing.
    - Vraag 20 ‘Ik neem vertrouwelijke informatie mee naar huis als ik hiervoor expliciete toestemming heb van mijn leidinggevende’:
        - ik neem vertrouwelijke informatie ALLEEN mee naar huis. Alleen toevoegen;
        - woordje toevoegen als ‘pas of alleen’. Dat is waarschijnlijk wat met de vraag wordt bedoeld.
    - Vraag 21 ‘Ik voer met mensen die niet mijn collega zijn vertrouwelijke gerelateerde gesprekken (thuis/met vrienden/etc)’:
        - dit doe ik ook niet eens met al mijn collega’s.
    - Vraag 25 ‘Als ik mijn (mobiel) apparaat verkoop of laat repareren, dan zorg ik ervoor dat eerst de zakelijke gegevens er vanaf zijn gewist’:
        - gaat het hier ook om privé apparaten? Bij devices die je van het werk krijgt, laat je dit door ICT doen. Bij privé apparaten kun je dit niet aan ICT vragen en is de veronderstelling dat mensen dit zelf kunnen. Het is beter om de vraag te verscherpen om hetzelfde te meten. Deze opmerking geldt ook voor de vergelijkbare houdings- en gedragsvraag.
    - Vraag 26 ‘Als ICT mij niet wil helpen om software te installeren op mijn laptop dan ga ik op zoek naar hoe ik dit kan installeren zonder ICT’:
        - mijn privé of zakelijke laptop?
    - Vraag 27 ‘Mijn privé apparaten die ik gebruik voor mijn werk beschikken over een virusscanner die ik tevens regelmatig update:
        - bij de introductie van de vragenlijst aangeven dat bij dergelijke en vergelijkbare vragen het antwoord ‘nooit’ voor nee staat en ‘altijd’ voor ja als uiterste schalen. Dat maakt het eenvoudiger te beantwoorden.
3. In hoeverre is het mogelijk alle vragen te beantwoorden zonder dat je nog een toelichting of uitleg nodig hebt over wat er met een vraag of antwoordcategorie wordt bedoeld?

Antwoord

- Bijna alle vragen konden zelfstandig en eenvoudige beantwoord worden met de gegeven antwoordopties. Bij een aantal vragen twijfelde ik over het antwoord of kon de vraag op meerdere manieren worden geïnterpreteerd. Deze zijn besproken bij vraag 2;
- Ik kon alle vragen beantwoorden en begreep ook de strekking van de vraag. Ditzelfde geldt voor de antwoordcategorieën. Een toelichting of uitleg op de vragen of de antwoordcategorieën was niet nodig;
- Voor grootste gedeelte is het mogelijk om de vragen zelfstandig te beantwoorden. De vragen zijn namelijk herkenbaar;
- Er was geen toelichting nodig om alle vragen zelfstandig te beantwoorden (behoudens de opmerkingen bij vraag 2);

- De vragen konden zelfstandig beantwoord worden zonder dat een toelichting nodig was, behoudens de opmerkingen bij vraag 2, en dan specifiek over het beantwoorden van de gedragsvragen welke over situaties gaan die niet vaak voorkomen;
- Dat valt af te leiden aan de opmerkingen, waarbij het gaat om de opmerkingen die betrekking hebben op de begrijpelijkheid van de vraag. In grote lijn kon ik het zelfstandig invullen;
- Alle vragen zijn zonder toelichting te beantwoorden. Er is bij de vragen geen introductie nodig. De vragen zijn namelijk duidelijk en de antwoorden spreken voor zichzelf;
- Alle vragen kon ik zelfstandig invullen. De antwoordcategorieën, meerpuntsschaal antwoorden, begrijp ik ook en gebruik ik zelf ook bij het uitzetten van vragenlijsten. Die antwoorden zijn herkenbaar voor gemeentelijke medewerkers.
- Los van de gemaakte opmerkingen bij vraag 2, kon de lijst zelfstandig ingevuld worden. Hiervoor is geen toelichting nodig op de vragen of de antwoordcategorieën.

Per vraag uit de survey de volgende vragen stellen:

4. In hoeverre is de vraag op jouw werksituatie van toepassing?

Antwoord

- Alle vragen zijn van toepassing. Ik herken de situaties die hierin zijn beschreven. Dit is de dagelijkse praktijk/omgeving waarin ik werk;
- Alle vragen zijn van toepassing op mijn werk. Ik gebruik verschillende mobiele devices en werk veel met vertrouwelijke informatie. Daarbij denk ik dat alle ambtenaren, in verschillende mate, met vertrouwelijke informatie/gegevens werken. Gemeenten beschikken over veel persoonsgegevens;
- Sommigen waren niet van toepassing of een vraag is binnenkort niet meer van toepassing (zoals onbeveiligd printen) en sommige gedragsvragen hebben zich nog niet in mijn situatie voor gedaan. Verder waren alle vragen van toepassing. Nogmaals: het is goed om aan te geven hoe met dergelijke gedragsvragen moet worden omgegaan als de situatie zich niet tot nauwelijks heeft voorgedaan;
- Alle vragen zijn van toepassing behalve de vragen over het dragen en tonen van een toegangspas en het printen met code. Hier kun je niet printen zonder code en wij beschikken hier niet over toegangspassen;
- Alle vragen zijn op de werksituatie van toepassing. Juist heel erg vanuit mijn vakgebied waarin ik veel met vertrouwelijke informatie werk. Daarnaast beschik ik over zakelijke en privé mobiele devices. De punten uit de 10 gouden regels zijn dan ook goed herkenbaar voor mijn praktijksituatie;
- Zie vraag 2. Niet alle vragen waren op mijn werksituatie van toepassing doordat ik niet buiten kantoor werk en niet beschik over zakelijke mobiele apparaten, die ik van mijn werkgever heb gekregen;
- Bijna alle vragen zijn op mijn situatie van toepassing. Daarnaast heb ik niet vertrouwelijke stukken maar ook geheime stukken. Dat maakt vragen soms lastig te beoordelen, want voor geheime stukken tref je andere en striktere beveiligingsmaatregelen dan bij vertrouwelijke stukken. Daarnaast gaat de vragenlijst ervan uit dat je geen vertrouwelijke zaken met anderen mag bespreken, maar ik doe ook aan collegiale consultatie; Die vragen moeten iets aangescherpt worden, dan wel moet uitgelegd worden bij de introductie van de vragenlijst hoe bepaalde vragen geïnterpreteerd moeten worden;

- Alle vragen waren van toepassing op mijn werk. Ik zou niemand kunnen bedenken op wie al deze vragen (of in ieder geval de meeste) niet van toepassing zouden zijn;
- Er was maar één vraag die niet relevant was en dat ging over het laten liggen van papieren bij de printer. Wij printen met codes dus dat kan niet.

5. Ten aanzien van de begrippen in de vraag: welke begrippen in deze vraag moeten uitgewerkt worden omdat de vraag anders niet eenduidig te beantwoorden is?

Antwoord

- CISO;
- CISO;
- Het begrip CISO;
- Het ‘kennen’, ‘toepassen’ en de afkorting CISO;
- CISO;
- definitie CISO
- Het ‘kennen’ van de 10 gouden regels en de definitie CISO;
- CISO definiëren.

6. Wat vind je van de helderheid van de vraag?

Antwoord

- De vragen zijn helder geformuleerd, behoudend de gemaakte opmerkingen bij vraag 2. Voorkom dubbele ontkenningen en formuleer de vragen positief. Dat maakt het gemakkelijker en eenvoudiger om de vraag te lezen en te begrijpen – wat de kans op fouten verminderd;
- Voor grootste gedeelte zijn de vragen helder gesteld. Een aantal vragen dient scherpen gemaakt te worden (zie antwoorden bij vraag 2);
- Ik vond de vragen helder. Ik begreep wat ermee wordt bedoeld. De opbouw van de lijsten en de vragen (per categorie en vorm is fijn). Het is ook prettig dat er per vraag een opmerkingenveld aanwezig is om een antwoord te kunnen nuanceren;
- De vragen waren helder, behoudens de opmerkingen bij vraag 2;
- De vragen zijn helder en eenduidig, behoudens de vragen waarbij definitie CISO of de 10 gouden regels onbekend zijn. Deze vraag haakt aan op vraag 3 dit gaat over het zelfstandig kunnen invullen van de lijst;
- In de regel zijn de vragen helder;
- De vragen zijn helder en alle vragen zijn eenduidig uit te leggen – behoudend de eerder gemaakte opmerkingen bij vraag 2;
- Er is 16 minuten over de vragenlijst gedaan. Omdat ik nu een afspraak met je heb ingepland vind ik 16 minuten goed te doen. Maar als dit een externe vragenlijst zou zijn of het zou op intranet aangekondigd worden dan is 16 minuten aan de lange kant. Dan ga je sneller lezen en sneller antwoord geven;
- Let erop dat alle vragen positief zijn geformuleerd. Er staat ergens een vraag met een dubbele ontkenning, die extra tijd kost om hem begrijpelijk te lezen. De rest van de vragen zijn helder van aard;
- Over het algemeen zijn de vragen helder. Er zijn echter een aantal vragen geformuleerd in lange zinnen. Deze kunnen het beste worden ‘opgehakt’ of worden opgesplitst in meerdere zinnen. Dat leest prettiger.

7. In hoeverre kun je op basis van de gegeven antwoordopties de vraag eenvoudig[10] beantwoorden?

Antwoord

- De antwoordcategorieën zijn helder en passen bij de wijze waarop de vragen zijn gesteld. Wel is het prettig om een toelichting op een antwoord te kunnen geven. Daar had ik wel behoefte aan, zodat een antwoord genuanceerd kon worden;
- Opmerkingen veld is fijn, maar hoe interpreteer je een situatie die niet vaak voorkomt en wat geef je als antwoord bij gedrag;
- De antwoordopties pasten bij de gestelde vragen;
- De antwoordopties zijn helder en duidelijk. Hiermee kunnen de vragen beantwoord worden. Bij de houdingsvragen met de categorieën van helemaal oneens tot helemaal eens (5 punt schaal) kun je overwegen om maar drie antwoordopties te geven. Het verschil tussen eens en helemaal eens is namelijk nogal een grijs gebied;
- Dit is het geval. Met de antwoordopties kan ik ook uit de voeten op de vragen die zijn gesteld;
- Ik miste de 'niet van toepassing'. De rest van de vragen sloten aan op de antwoordcategorieën;
- De vragen konden allemaal beantwoord worden met de gegeven antwoordopties. Alleen doordat een aantal vragen niet op de organisatie of mijn functie van toepassing zijn, was het lastiger of niet mogelijk om daar antwoord op te geven;
- De antwoordcategorieën pasten bij de vragen. De midden categorie is wellicht voor de onderzoeker een lastige categorie om te analyseren, maar als gebruiker wil ik deze categorie ook niet missen omdat op sommige houdingsvragen ik 'eens/oneens' wil invullen en niet perse moet kiezen voor eens óf oneens;
- De vragen kon ik snel beantwoorden, omdat deze niet voor meerdere uitleggen vatbaar zijn en de antwoordcategorieën sluiten aan op de vragen.

<u>Aspect 'Haalbaar'</u>

Vragenlijst om te beoordelen of de methodiek/vragenlijst haalbaar is.
Haalbaar is in de definitielijst gedefinieerd als:

De verhouding tijdsduur versus het aantal vragen is voor de onderzoeker en de personen die de surveyvragen beantwoorden acceptabel, waardoor de betrouwbaarheid van de antwoorden zoveel mogelijk wordt gewaarborgd.

Deze definitie benoemen en vervolgens onderstaande vragen stellen.

6. Ik geef aan hoe lang zij over de vragenlijst hebben gedaan en stel dan de vraag: Wat vind je van de tijdsduur dat je hebt gedaan over deze vragenlijst?

Antwoord

- (18 minuten over gedaan). Dit is precies genoeg. Langer hoefde het ook niet te duren;
- (30 minuten over gedaan). Een kwartier is het maximale wat gevraagd kan worden. Dit i.v.m. concentratie en bereidwilligheid om eraan deel te nemen. Omdat ik nu ook keek naar de begrijpelijkheid van de vragen, kostte dit mij meer tijd. Normaal zou ik over deze vragenlijst ongeveer 20 minuten hebben gedaan;

[10] Zonder er lang over na te denken (ter indicatie: 15 seconden ongeveer) kun je de vraag beantwoorden en geeft de antwoordoptie ook het antwoord weer dat je wil geven

- Het invullen van de vragenlijst duurde 20 minuten. Omdat ik het nu heb ingepland, zijn 20 minuten goed te doen, maar als dit een externe vragenlijst was geweest die ik over de mail had gekregen, dan waren 20 minuten te lang;
- (26 minuten). Het waren veel vragen en 26 minuten is te lang voor een normale vragenlijst die ik ontvang (van derden of intern) per mail. Het is wel situatieafhankelijk, want nu ik het voor jou doe, vind ik 26 minuten acceptabel;
- 22 minuten over een vragenlijst doen is wel lang. Ik heb overigens ook gekeken naar de vraagstelling ten behoeve van dit interview, waarbij ik kritisch heb gekeken naar definities en onduidelijke vragen. Daardoor heb ik er ook langer over gedaan dan dat ik normaal over een vragenlijst doe;
- (16 minuten over gedaan). Ik was blij dat het afgelopen was. De tijdsduur was niet te lang, je moet er goed over nadenken, maar het had niet langer moeten duren.
  Ik vond het fijn dat achter iedere vraag een hokje voor opmerking zat, zodat je je ideeën en gedachtes bij die vraag kwijt kon.
- (25 minuten). Als ik van te voren zou vinden dat ik er 25 minuten over zou doen had ik dat lang gevonden. Het voelde niet als 25 minuten. Het voelde korter aan. Ik vond het acceptabel, maar vooraf bepalend vind ik 15 minuten de grens. Sommige vragen lijken zich te herhalen, waardoor ik dacht ‘hé daar heb je weer zo’n vraag’. Het is goed om daar aandacht aan te besteden (bijvoorbeeld in de intro van de vragenlijst) omdat deze vragen toch wat anders beogen te meten (bijvoorbeeld het kennisniveau en de andere vraag het houdingsniveau).
- (18 minuten over gedaan). Mijn aandacht begon ik na 10 minuten te verliezen. Voor mijn gevoel duurde het te lang.

7. Wat is voor jou ongeveer de maximale tijdsduur om deze vragenlijst bereidwillig én tegelijk zorgvuldig te beantwoorden?

Antwoord

- 15 minuten is acceptabel;
- Ik vind een kwartier het maximum om bereidwillig tijd vrij te maken tussen de werkzaamheden door;
- 10 minuten vind ik acceptabel. Als een onderwerp echt mijn interesse heeft dan is meer dan 10 minuten ook acceptabel voor mij. Maar omdat de vragenlijst voor alle medewerkers geldt, is mijn advies om 10 minuten aan te houden.
- 15 minuten vind ik acceptabel;
- 15 minuten;
- 10 minuten is prettig. Dat kun je dan nog wel tussen door zijn. De vragen moeten dan helder zijn en de vragen moet je eenvoudig kunnen beantwoorden, zodat het niet te veel moeite kost. Bij 20 minuten moet ik er een belang bij hebben, anders ga ik er niet aan beginnen;
- Hangt van onderwerp af en mijn agenda. Ken ik de persoon die het vraagt en vind ik het onderwerp interessant? Een vragenlijst die via intranet wordt uitgezet zal ik minder snel invullen dan wanneer het mij persoonlijk wordt gevraagd. Daarnaast is het prettig dat er gesloten vragen zijn gesteld. Ik ben dan sneller geneigd de vragen te beantwoorden dan wanneer ik open vragen moet beantwoorden;
- Een kwartier klinkt voor de meeste medewerkers acceptabel;
- 10 minuten vind ik de maximale tijd om bereidwillig de vragenlijst te behandelen en de vragen zorgvuldig te beantwoorden.

8. Wat vind je van het aantal vragen?

Antwoord

- Het gaat vooral om de tijdsduur. Het aantal vragen is minder relevant. Doordat de vragen op elkaar leken, kon het ook sneller beantwoord worden. Het waren niet compleet nieuwe vragen. Het onderwerp kwam steeds terug;
- Ik heb niet het gevoel gehad dat het ongeveer 100 vragen waren. Het waren ook verschillende vragen. Het fijne was dat de vragen gecategoriseerd waren op onderwerp (over toegang, mobiele devices, privé apparaten e.d.) en antwoordcategorie. Een duidelijke structuur maakt het prettig invullen;
- Het zijn niet te veel vragen. Het scheelt dat de vragenlijst in drieën is opgesplitst. Hierdoor voelt het dan minder 'zwaar' aan dan wanneer je bijvoorbeeld 95 vragen onder elkaar zet. Binnen de tijdseenheid is dit aantal vragen voldoende en acceptabel;
- Te veel. Je kan het meer afbakenen op onderzoeksonderwerp of aantal gedragsrisico's;
- Het aantal vragen is prima, maar past niet binnen die 15 minuten. De vragen per sessie (per periode) uitzetten, of via versnellingskamersessies maakt het acceptabeler. Sowieso is het idee van versnellingskamersessies een goede, omdat je dan de mogelijkheid hebt om met elkaar in gesprek te gaan en de vragen uit te diepen;
- Ik had niet door dat het er ongeveer 100 waren. Het ging voor mijn gevoel sneller. Het gaat niet om het aantal vragen, maar om hoeveel tijd men kwijt is aan de vragenlijst;
- Met het aantal vragen is op zich niets mis, maar deze kun je dus niet binnen 10 minuten zorgvuldig beantwoorden. Je kan dan de vragenlijst opknippen of versnellingskamersessies gebruiken. Dan hebben mensen het ook in hun agenda staan en hoef het niet tussen het werk door ingevuld worden. Dan zijn 16 minuten heel acceptabel. Mensen die daarbij deelnemen aan zo'n sessie zijn ook bereidwillig om geconcentreerd en met veel aandacht de vragenlijst te behandelen – want anders zouden zij daar niet zitten;
- Soms heb ik het gevoel dat de vragen worden herhaald, maar is de antwoordstructuur anders. Ik heb geen specifieke opmerkingen over het aantal vragen. Het scheelt dan ook dat het gesloten vragen zijn, wat het eenvoudiger maakt om het in te vullen. De structuur van de vragenlijst is ook fijn, waarbij de vragen zijn gecategoriseerd naar antwoordcategorie.
- Ik had niet het gevoel dat het er zo veel waren. De vragen waren ook niet lastig gesteld waardoor je de vragen redelijk snel kon beantwoorden en waarbij ik tevens over elk antwoord heb nagedacht.

9. In hoeverre heb je alle vragen met evenveel zorg gelezen en beantwoord? *(NB ivm de betrouwbaarheid van de beantwoording is 'afraffelen' ongewenst. Vragen dienen aandachtig gelezen te worden en zorgvuldig te worden beantwoord)*

Antwoord

- Aan het einde ging ik sneller lezen en met minder zorg. Nu las ik de vragen om te beantwoorden én te gelijk voor je interview of ik deze ook begreep. Dat kostte ook meer tijd. Dat ik op een gegeven moment sneller ging lezen, kwam door de tijdsduur;
- Na 10 minuten verloor ik mijn aandacht. Daarna ben ik minder zorgvuldig antwoorden gaan geven, wat inhoudt dat ik niet zorgvuldig na denk over het

antwoord dat specifiek past bij de vraag. Waardoor ik soms eerder ‘eens’ invul dan ‘helemaal eens’, wat dan niet altijd terecht is;

- In de 16 minuten heb ik het aandacht gelezen, maar dat had onder andere ook te maken met het feit dat ik de vragen interessant vond en deze afspraak in mijn agenda had staan. Doordat de vragen per onderwerp afwisselden, ging het lezen ook niet vervelen;
- Ik heb alle vragen met evenveel zorg gelezen en beantwoord. Dat had er mee te maken dat ik geen tijdsdruk heb. Nu zit ik alleen in afgesloten ruimte waarbij ik geen collega’s om me heen heb en tevens niet gestoord kan worden door telefoontjes, gesprekken, e-mail e.d. Dat maakt het wel prettig;
- Ik heb alle vragen met evenveel zorg gelezen en heb op het eind niet versneld. Ik heb alles wel met evenveel zorg gelezen, maar dat had te maken met dat ik weet waarvoor en voor wie ik de vragenlijst in vul. Een VNG-vragenlijst doe ik sneller. Belangrijk is dus om dat in de introductie van de vragenlijst mee te geven;
- Alle vragen zijn met evenveel zorg gelezen en beantwoord. Aan het einde is niet versneld. Het is goed om bij de introductie van de vragenlijst te vermelden dat een aantal vragen op elkaar lijken, maar dat deze verschillende facetten meten. Het lijkt er anders op alsof je dezelfde vragen krijgt. Daarnaast is het goed om bij de introductie te vermelden wat zij eraan hebben om de bereidwilligheid te stimuleren;
- Ik heb alle vragen met evenveel zorg gelezen, maar ook omdat ik het voor jou doe en het mij speciaal is gevraagd. Anders zou ik zijn afgehaakt op het aantal vragen en de tijdsduur;
- Elke vraag heb ik goed gelezen, over nagedacht en op het einde heb ik niet versneld en de vragen niet afgeraffeld. Het is niet van invloed dat ik het nu voor jou doe en dat deze afspraak in onze agenda is ingepland;
- Ik heb aan het einde iets versneld, maar heb de vragenlijst niet ‘afgeraffeld’. Ik heb versneld omdat de inhoud van de vragenlijst qua onderwerp zich ging herhalen en daardoor werd het bekender. Daarbij heb ik geconcentreerder gelezen omdat de vraag was om ook te kijken of de vragen begrijpelijk en helder waren;
- Qua tijdsduur had ik het gevoel dat ik sneller was dan die 25 minuten en dat het minder vragen waren dan +/- 100 vragen. Ik vond die verhouding daarom wel goed. Hierover heb ik geen opmerkingen. Mijn voorkeur gaat verder ook uit naar een vragenlijst i.p.v. een werksessie, omdat een werksessie meer tijd kost. Dan zou ik een werksessie sneller laten ‘lopen’. Daarbij zou aansluitend op de vragenlijst een gesprek met een aantal medewerkers kunnen worden gedaan, om zo meer informatie en context uit de gegeven antwoorden te krijgen.

10. Wat is jouw bevinding op het aantal vragen dat je is gesteld versus de tijd die je erover hebt gedaan?

Antwoord

- De tijdsduur is voornamelijk van belang, waarbij er ook geen tijdsdruk moet zijn. Interviews en sessies ervaar ik prettiger dan vragenlijsten over de mail. Het voordeel is dat je dan ook bereidwillige mensen aan tafel hebt, waardoor antwoorden toegelicht kunnen worden en medewerkers waarschijnlijker nauwkeuriger die vragen beantwoorden. Dat komt de kwaliteit van de antwoorden ten goede;
- Het gaat om de tijdsduur;

- Allebei acceptabel. Hierover geen specifieke opmerkingen. Dit is al grotendeels bij de voorgaande vragen behandeld;
- Het gaat niet zo zeer om het aantal vragen, maar meer over hoe lang er over wordt gedaan – de tijd die iemand eraan kwijt is. Op basis daarvan zullen wat vragen of onderdelen geschrapt moeten worden om binnen de acceptabele 15 minuten te blijven, dan wel moet de vragenlijst worden opgeknipt of ingezet worden via versnellingskamerssies;
- Voor een willekeurige vragenlijst is het aantal vragen te veel en de tijdsduur te lang;
- Ik vind het acceptabel – zolang de totale vragenlijst binnen de 15 minuten kan worden ingevuld, waarbij ruimte is om vragen op gemak te kunnen lezen om binnen de 15 minuten te blijven. Anders zal het waarschijnlijk ten koste gaan van de betrouwbaarheid van de antwoorden;
- De vragenlijst kun je niet in 10 minuten zorgvuldig invullen. Ik denk ook dat je via een digitale (of schriftelijke) vragenlijst minder aandacht besteedt aan de vragenlijst dan wanneer dit via een workshop wordt gedaan. Als het puur gaat om een eerste indruk te krijgen van het bewustzijn dan is een vragenlijst goed, maar als je met hen erin over in gesprek gaat dan krijg je meer onderbouwde (betrouwbaardere) antwoorden dan via een vragenlijst. En dat bevordert tegelijk ook meer het bewustzijn;
- Als de vragenlijst organisatiebreed wordt uitgezet, dan zal die ingekort moeten worden qua aantal vragen. Daarnaast biedt een versnellingskamersessie goede mogelijkheden om toch de hele vragenlijst uitgebreid te behandelen, waarmee het bewustzijn goed in kaart kan worden gebracht.

Bijlage 12 Model Kruger & Kearney (uitgebreide beschrijving)

Kruger en Kearney (2006) hebben een model ontwikkeld om het informatiebeveiligingsbewustzijn te meten bij een internationaal mijnbouwbedrijf. Zij geven aan dat het belangrijk is om te werken aan het informatiebeveiligingsbewustzijnniveau van medewerkers, omdat medewerkers een grote rol spelen bij de effectiviteit van de implementatie van technische en organisatorische (procedurele) maatregelen. Hoe effectief deze beveiligingsmaatregelen zijn hangt dus af van de creatie van een security positive environment, waarbij een ieder het gedrag vertoont en begrijpt dat van hem verwacht wordt (Kruger & Kearney, 2006). Cultuur is dus een belangrijke factor bij het creëren van een dergelijke omgeving. Kruger en Kearney geven aan dat er in de praktijk veel middelen zijn die helpen bij het creëren van zo'n omgeving, maar dat er in de literatuur weinig te vinden is over hoe de effectiviteit van bewustwordingsprogramma's gemeten kan worden. Het werken aan bewustwording is een continu proces en moet niet alleen bijdragen aan het bewust worden, maar ook in het bewust blijven en uiteindelijk in het bewust zijn.

Bij het internationaal mijnbouwbedrijf is eerst een bewustwordingsprogramma opgezet dat na een zorgvuldige selectie bestond uit zes kritische risicogebieden, waarbij het zesde risicogebied het centraal stond in het programma:

1. Volg altijd de procedures van de organisatie;
2. Houd wachtwoorden en persoonlijke identificatienummers geheim;
3. Gebruik e-mail en internet zorgvuldig;
4. Wees zorgvuldig met mobiel gereedschap (door mij vertaald als mobiele devices);
5. Meld incidenten;
6. Wees bewust, alle acties dragen consequenties met zich mee.

Na het volgen van het programma, was er behoefte om het programma te evalueren en het succes te meten. Bij het uitwerken van een model om het bewustzijn te meten, is het uitgegaan van drie te meten componenten - op basis van technieken die geleend zijn uit het Sociaal Psychologische veld en vaker zijn toegepast bij de evaluatie van bewustwordingsprogramma's:

1. Kennis: wat weet een persoon;
2. Houding: welk gevoel (welke gedachte) roept een onderwerp op bij een persoon;
3. Gedrag: wat passen zij toe.

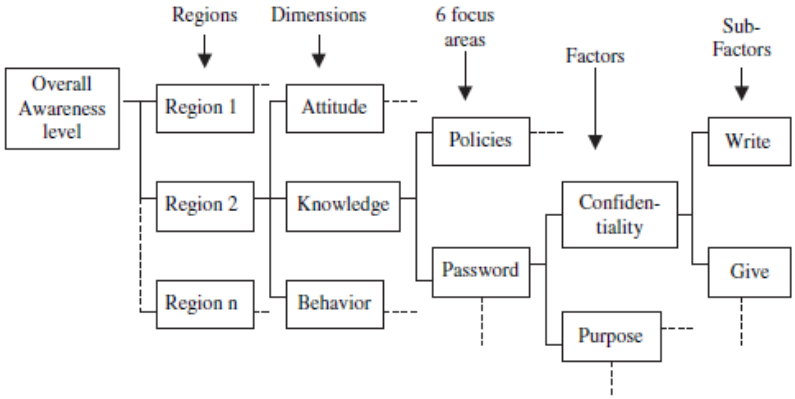
Bij het ontwikkelen van een methodiek om het bewustzijn te meten, is niet alleen gekeken naar wat er moet worden gemeten, maar ook hoe er moet worden gemeten. Bij dit laatste is rekening gehouden met:

- De duurzaamheid van de methode (herbruikbaarheid);
- Het gebruiksgemak;
- Het gebruik van wetenschappelijke methoden;
- De specifieke eigenschappen van de organisatie.

De ontwikkelde methode van Kruger & Kearney moest daarbij een hoofdmeting zijn, rekening houdend met de diverse organisaties van het mijnbouwbedrijf die gevestigd waren in verschillende regio's. Dit betekent dat er een methode is ontwikkeld, waarbij de wegingsfactoren per regio en per organisatie kunnen verschillen. Deze zwaarte van de weging wordt door het management toegekend met behulp van Analytic Hierarchy Process (AHP), dat subjectiviteit probeert te voorkomen en uitgaat van de professionele

mening van het management. Kruger & Kearney merken op dat het toepassen van AHP tijdrovend kan zijn – afhankelijk van het aantal te meten subcategorieën

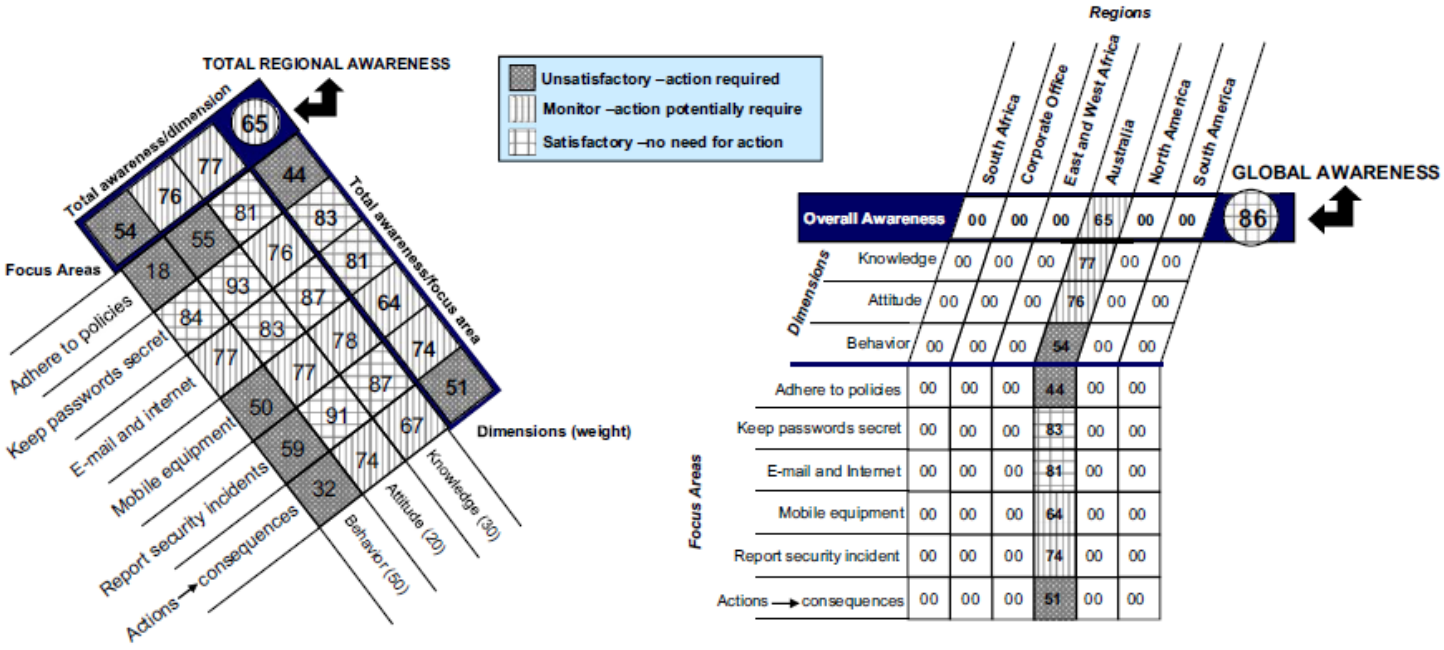
Het opgezette model bestaat uit het meten van elk gekozen risicogebied afgezet tegen elk te meten component (kennis, houding en gedrag). Hierbij zijn de risicogebieden uitgewerkt in subcategorieën. Figuur 6 geeft het model weer.



Figuur 6 Model om bewustwording te meten (Kruger & Kearney, 2006)

Het bewustwordingsniveau kan berekend worden met de geaccepteerde formule voor de waardefunctie: $V(a) = \sum_{i=1}^{n} v_i(a) w_i$.
V(a) staat voor de totale score, waarbij vi(a) staat voor de score van a op criterium i, die gemeten kan worden met een vragenlijst. Wi vertegenwoordigt de zwaarte per criterium.

In het model van Kruger en Kearney (2006) zijn in totaal 35 vragen geformuleerd, waarbij de meeste vragen een driepuntsschaal als antwoord hadden (waar, niet waar en weet niet) en een aantal uitsluitend alleen de antwoordmogelijkheden ‘waar’ en ‘niet waar’. Dit komt overeen met vergelijkbare toegepaste methodieken om bewustzijn te meten en andere metingen uit het Sociaal Psychologisch veld (Kruger & Kearney, 2006). Kruger & Kearney merken terecht op dat de vragenlijst om het gedrag te meten anders kan worden ingevuld dan in werkelijkheid het geval is. Daarom is het raadzaam om aanvullend ook in de praktijk te meten, zodat de betrouwbaarheid van de vragenlijst kan worden bepaald.Het toepassen van georganiseerde social engineering en het inzetten mysterie guests behoren tot de mogelijkheden. Een voorbeeld van het weergeven van de uitslagen van de meting is weergegeven in figuur 7.



Figuur 7 Voorbeeld weergave van de uitslagen van de bewustwordingsmeting.

Met deze methodiek kan per gemeente een meting worden gedaan en deze worden opgeteld om te komen tot een totale uitslag van alle gemeenten (in figuur 7 is dit als voorbeeld de global awareness).

Kruger en Kearney hanteerde tot slot de volgende schaal voor bewustwording, zie tabel 4, om waarde toe te kennen aan de totale uitslag:

Tabel 4 Schaal voor bewustwording

Bewustwordingsniveau (overall)	Uitslag van meting
Goed	90-100
Gemiddeld	70-89
Slecht	69 en minder

Bijlage 13 Verdieping resultatenanalyse empirisch onderzoek fase 1 voor onderzoeksvraag 2

In hoofdstuk 4.1. zijn de resultaten van de eerste fase uit het empirisch onderzoek beschreven. Hierin is aangegeven dat tijdens de vier interviews met deskundigen detaillistische opmerkingen zijn gemaakt ten aanzien van de opbouw van de voorgelegde methodiek. Deze bijlage geeft de specifieke opmerkingen (interviewresultaat) weer met aansluitend een onderbouwde reactie (analyse) in hoeverre de opmerking is verwerkt (conclusie) in de methodiek voor de tweede fase van het empirisch onderzoek. Deze opmerkingen zijn gecategoriseerd. Voor de conclusie wordt gebruik gemaakt van smileys die in één oogopslag weergeven of een opmerking is verwerkt in de methodiek of niet. Tabel 5 geeft de betekenis van de smileys weer.

Tabel 5 Interpretatie smileys

☺	Opmerking *volledig* verwerkt in de methodiek ten behoeve van fase 2 van het empirisch onderzoek	😐	Opmerking *deels* verwerkt in de methodiek ten behoeve van fase 2 van het empirisch onderzoek	☹	Opmerking *niet* verwerkt in de methodiek ten behoeve van fase 2 van het empirisch onderzoek

Tabel X Verdiepende resultatenanalyse van de eerste fase uit het empirisch onderzoek voor onderzoeksvraag 2 ter verwerking van het model voor de tweede fase van het empirisch onderzoek

Relatie	Interviewresultaat	Analyse	Conclusie
Relatie Thema - Gouden regels	De IBD geeft aan dat het model een zekere mate van hiërarchie kent, waarbij de thema's van gelijke orde behoren te zijn. De vijf genoemde thema's zijn van verschillend niveau en onlosmakelijk met elkaar verbonden, wat het lastig maakt om een scheiding aan te brengen (dat wat in het voorgelegde model wel is gedaan). De gedragsrisico's die hieruit voortvloeien zijn volgens de IBD niet altijd aan één thema toe te kennen, maar hebben raakvlakken met meerdere thema's. Het model houdt daar geen rekening mee.	De kolom 'thema's' in het model bepaalt vanuit welk perspectief de belangrijkste gedragsrisico's (gouden regels) worden bepaald. Daaruit vloeit een een-op-een verband tussen de thema's en de gouden regels. Dit verband is gelegd vanuit het thema geredeneerd. Als het verband wordt beschouwd vanuit de gouden regels richting de thema's geven dan valt op dat de thema's een zekere overlap hebben. De thema's 'binnen' en 'buiten' kennen een duidelijke scheiding aangezien dit gaat over de omgeving waarin wordt gewerkt. De andere thema's zijn van een andere categorie waardoor er een overlap bestaat tussen de thema's.	☺ De thema's zorgen niet voor eenduidigheid in het model, waardoor de verbanden tussen de thema's en de gouden regels onzuiver zijn. De thema's worden uit het model gehaald en vervangen door een kolom 'focus'. Deze kolom bepaalt vanuit welke focus de belangrijkste gedragsrisico's worden bepaald. Bij het empirisch onderzoek is dit gedaan door te kijken naar actuele trends en ontwikkelingen op internationaal, landelijk en lokaal gebied. De CISO van Edam-Volendam heeft aangegeven dat dit ook kan vanuit de hoofdstukcategorieën uit de BIG. Uit het interview met betrokkenen uit de campagne iBewust Overheid is aangegeven dat de risico's ook bepaald kunnen worden vanuit opgestelde (organisatie) leerdoelen. Afhankelijk van de focus kunnen andere

			gedragsrisico's van belang zijn. De kolom 'focus' biedt die ruimte om te bepalen vanuit welke 'bril' de gedragsrisico's worden bepaald.
Relatie Gouden Regels - Bepalende factoren	In twee interviews is opgemerkt dat de geheimhoudingsplicht vervallen als bepalende factor, omdat deze te algemeen is en daardoor niet expliciet in dit model hoeft te worden gemeten.	De geheimhoudingsplicht heeft betrekking op het vertrouwelijk omgaan met informatie. De geheimhoudingsplicht is een basis gedragselement dat in het model abstract is geformuleerd en in het model via andere bepalende factoren al specifieker is gemaakt	 Bepalende factoren dienen niet abstract maar concreet te zijn geformuleerd, waarmee de gouden regels kunnen worden gemeten. De geheimhoudingsplicht is te abstract voor een bepalende factor en heeft geen toegevoegde waarde in het model. Deze bepalende factor wordt verwijderd.
Relatie Gouden Regels - Bepalende factoren	In twee interviews is opgemerkt dat medewerkers waarschijnlijk niet het verschil weten tussen technische en overige incidenten. Het voorstel is om het enkel te hebben over incidenten en deze niet te verbijzonderen. Daarbij is de vraag of medewerkers weten wat een incident is. Voorstel is om toe te voegen dat ook verdachte zaken moeten worden gemeld. Het gedragsrisico is namelijk dat er melding wordt gemaakt indien de informatiebeveiliging in het geding is, dan wel kan zijn.	De onderbouwing is legitiem. Het risico is namelijk dat medewerkers bepaalde zaken niet melden, waardoor niet onderzocht kan worden of bepaalde acties moeten worden ondernomen om de kans dat een risico zich gaat voordoen te minimaliseren, dan wel dat de impact van het opgetreden incident niet verder kan escaleren.	 Beide opmerkingen worden verwerkt aangezien het erom gaat dat meldingen tijdig moeten worden gedaan.
Relatie Gouden Regels - Bepalende factoren	De CISO van Edam-Volendam merkt op dat gouden regel 2 gemeten kan worden door een bepalende factor op te nemen omtrent het dragen van een toegangspas. Dit bepaalt mede namelijk of mensen andere aanspreken of niet.	Tijdens de interviews is opgemerkt dat het belangrijk is om een cultuur te hebben waarin men elkaar aanspreekt, er commitment is en men informatiebeveiligingsbewust is. Dit zijn belangrijke (gedrags)elementen om beveiligingsrisico's aan te pakken. De voorgestelde bepalende factor draagt bij aan het creëren van een dergelijke cultuur en is voor medewerkers een hulpmiddel om te voorkomen dat zij onbevoegden toegang verschaffen tot het pand .	 Opmerking wordt overgenomen omdat het niet dragen van een toegangspas de kans vergroot dat onbevoegden toegang krijgen tot het pand en de werkruimten.

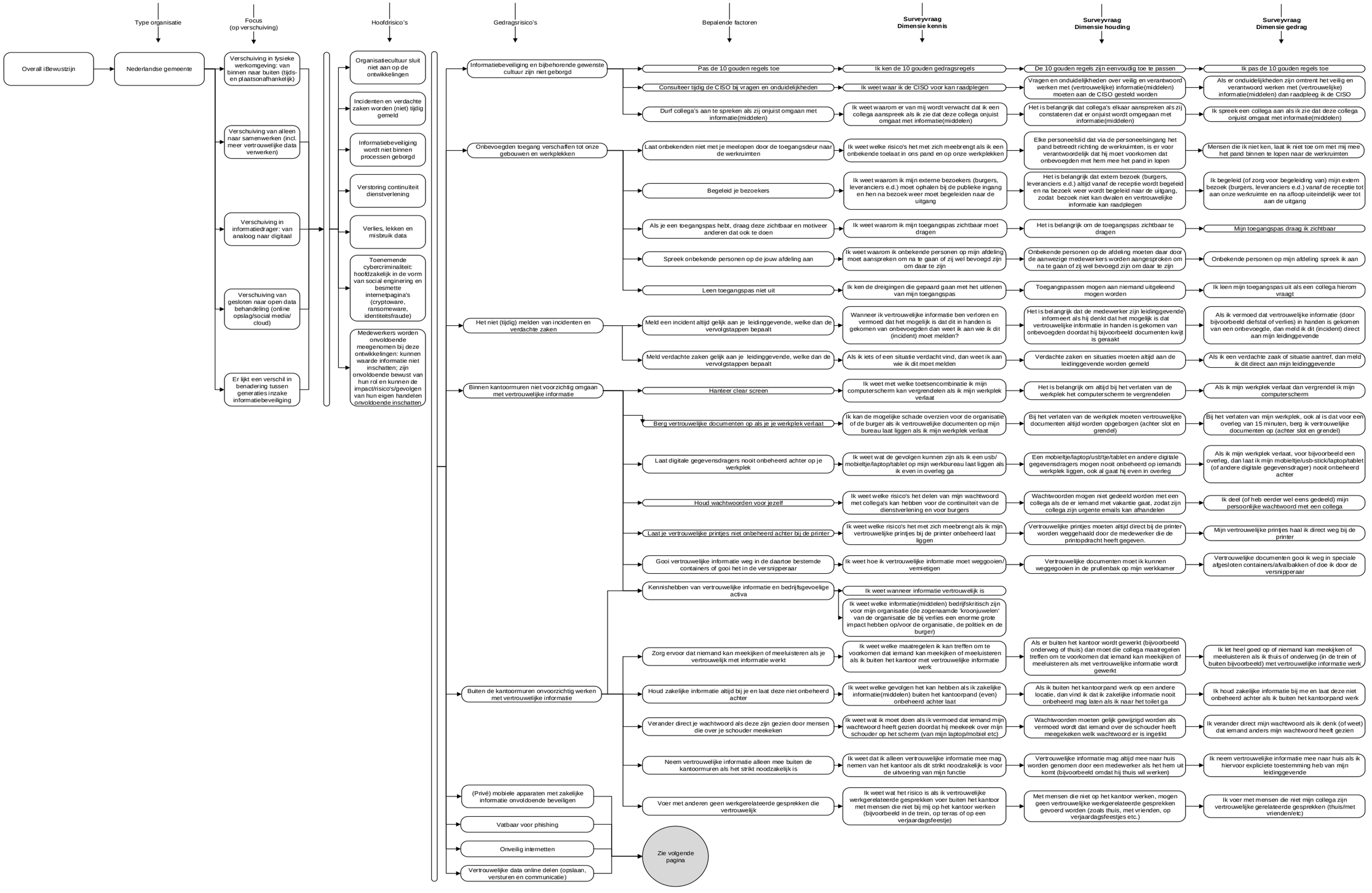
Relatie Gouden Regels - Bepalende factoren	De CISO van Edam-Volendam geeft aan dat voor gouden regel 6 een bepalende factor kan worden toegevoegd, welke aangeeft dat bij reparatie of verkoop van een mobiel device, eerst alle zakelijke gegevens moeten worden gewist.	Met de vluchtigheid van de ontwikkeling van nieuwe (versies van) devices komt het met regelmaat voor dat gebruikte devices worden verkocht. Daarnaast komt het met regelmaat voor dat devices moeten worden gerepareerd. Vooral bij verkoop is het belangrijk dat gegevens zijn gewist om 'informatie lekken' te voorkomen.	 Bepalende factor wordt toegevoegd omdat deze gouden regel 6 meet.
Relatie Gouden Regels - Bepalende factoren	De CISO van Edam-Volendam geeft aan dat bij gouden regel 10 de bepalende factor omtrent het lezen van algemene voorwaarden kan vervallen. Het heeft weinig toegevoegde waarde om dit te meten, omdat algemeen bekend is dat men dit niet uitvoerig doet.	De invloed van het wel of niet lezen van algemene voorwaarden zijn klein zijn op risico's van cloudgebruik en online communicatie. De andere bepalende factoren bij gouden regel 10 zijn qua gedragsmaatregelen van grotere invloed op de kans dat een beveiligingsincident optreed. Als organisatie wil men eerder sturen op die factoren dan het verplichten om voorwaarden te lezen bij het gebruik van bijvoorbeeld Dropbox.	 Bepalende factor wordt verwijderd, aangezien de aanname is dat de invloed zeer klein is en dat bovendien algemene voorwaarden slecht tot niet worden gelezen.
Relatie Gouden Regels - Bepalende factoren	De CISO van Edam-Volendam merkt op dat voor gouden regel 4 een bepalende subfactor kan worden toegevoegd omtrent het voorkomen van incidenten door beveiligingseisen vast te leggen in contracten e.d. bij het inkopen en inhuren.	Het is belangrijk dat beveiligingseisen ook aan derden worden opgelegd, zodat er vertrouwelijk (namens de opdrachtgever) met informatie wordt omgegaan. Alleen dit geldt voor medewerkers die kunnen en mogen inkopen en inhuren. Dit is dus een specifieke doelgroep. Het model heeft als doelgroep alle medewerkers.	 De opmerking is terecht maar past niet binnen de gestelde kaders van het model dat alle medewerkers als doelgroep heeft.
Relatie Bepalende factoren – Surveyvraag	De CISO van Edam-Volendam geeft aan dat de bepalende factor 'Spreek onbekende personen op jouw afdeling aan', de kennisvraag 'ik weet welke informatie op mijn afdeling niet openbaar mag worden' niet de lading dekt van de bepalende factor.	De kennisvraag komt niet overeen met de bepalende factor.	 Kennisvraag wordt aangepast.
Gouden regels Opbouw	De IBD merkt op dat gouden regel 3 en 4 elkaar overlappen en dus samengevoegd kunnen worden.	De bepalende factoren van deze twee gouden regels richten zich allen op het vertrouwelijk omgaan met informatie(middelen) om misbruik, diefstal e.d. te voorkomen. Gouden regel 3 is een gevolg van gouden regel 4.	 Gouden regels worden samengevoegd tot een nieuwe gouden regel die zich richt op het vertrouwelijk omgaan met informatie.

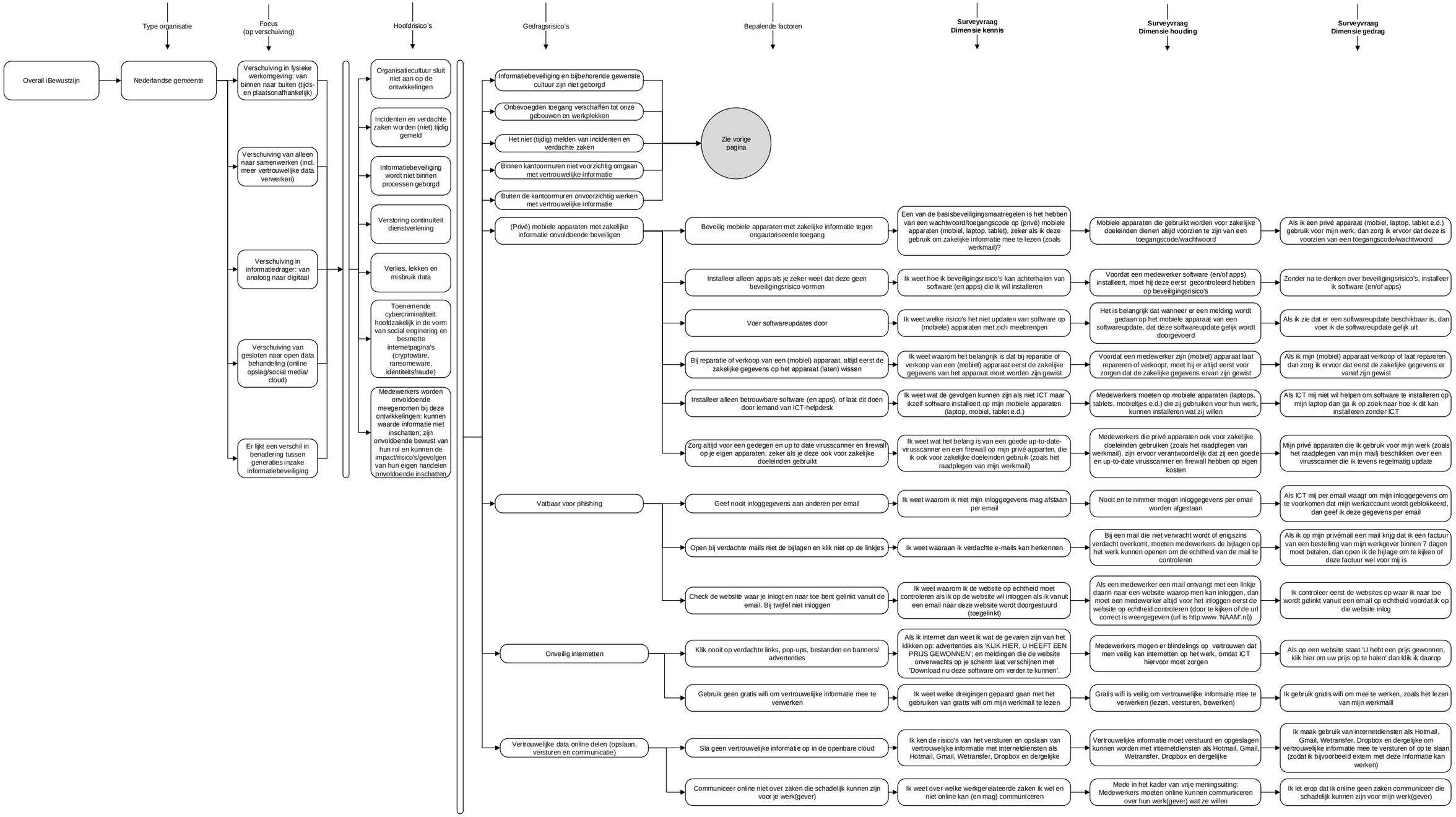
Gouden regels Opbouw	De IBD geeft aan dat de gouden regels 8 en 9 kunnen worden samengevoegd omdat deze van gelijk niveau zijn en hetzelfde meten, namelijk het voorzichtig omgaan met digitale zaken.	Gouden regel 8 is erop gericht dat medewerkers geen inloggegevens afstaan en besmette emails openen. Gouden regel 9 is erop gericht dat geen besmette internetsites worden bezocht. Er is een zekere overlap, maar de gouden regels meten beide een ander risico.	 De kolom gouden regels moet expliciet duidelijk maken welke gedragsrisico's worden gemeten. Dit is voor de eenduidigheid van het model van belang, zodat helder is welke risico's worden gemeten. De kolom met bepalende factoren vertaalt dit door in gedragsrisico's waardoor helder is welke gedrag wordt gemeten ten aanzien van welk risico.
Bepalende factor	De voorzitter van de domeingroep Awareness van het CIP en de IBD geven aan dat clear desk en clear screen niet als één bepalende factor moet worden opgenomen, maar dat dit moet worden gesplitst. Dit zijn namelijk twee verschillende gedragsmaatregelen.	Clear desk en clear screen zijn inderdaad twee gedragsmaatregelen waar anders op gescoord kan worden.	 Bepalende factor wordt opgesplitst.
Bepalende factor	De IBD geeft aan dat de bepalende factor omtrent wifi aangescherpt dient te worden, waarbij wordt aangegeven dat men zich bewust moet zijn van de risico's van het gebruik van gratis/onbeveiligde wifi voor het werken met zakelijke vertrouwelijke gegevens.	Het model dient het bewustzijn te meten omtrent de grootste gedragsrisico's. Het gebruik van onbeveiligde/gratis wifi op zichzelf vormt niet direct het risico met een mogelijke grote impact, maar dat is wanneer met zakelijke vertrouwelijke gegevens op die wifi wordt gewerkt.	 Bepalende factor wordt aangescherpt op het vlak waar het risico zich bevindt met de impact die men wil voorkomen.
Bepalende factor	De IBD geeft aan dat de bepalende factor omtrent het hebben van een gedegen up to date virusscanner en firewall op je eigen apparaten als je deze voor zakelijke doeleinden gebruikt, aangescherpt dient te worden door het woord 'zeker' eraan toe te voegen ('zeker als je deze ook voor zakelijke doeleinden gebruikt')	De bepalende factor dient te meten dat medewerkers een gedegen en up to date virusscanner en firewall hebben op hun persoonlijke apparaten die zij voor hun werk gebruiken. Het toevoegen van het woord 'zeker' verandert dat niet, maar dan is deze meer directief en in lijn met de vorm van de andere bepalende factoren.	 Bepalende factor wordt aangescherpt en is hiermee meer in lijn qua vorm met de andere bepalende factoren.
Survey Vraagstelling	De IBD geeft aan dat bewustzijn zich moeilijk laat meten door o.a. sociaal wenselijk gedrag. Zeker bij de kennisvragen, doordat dit ja/nee vragen zijn, komt dit sterker aan de orde. Door controlevragen of door een toelichting te vragen krijg je mee inzicht in de kennis.	Door controlevragen toe te voegen neemt het aantal surveyvragen toe. Het vragen van een toelichting betekent dat de onderzoeker meer verwerkings- en analysetijd nodig heeft wat niet strookt met onderzoeksvraag 3, dat erop gericht is dat de gegeven antwoorden direct kunnen worden gekwantificeerd en geanalyseerd.	 I.v.m. de haalbaarheid (effectiviteit van het model) wordt dit niet verwerkt. De opmerking is terecht. Om dit te kunnen realiseren zouden de surveyvragen ook ingezet kunnen worden via versnellingskamers.

Survey Vraagstelling	De voorzitter van de domeingroep Awareness van het CIP geeft aan dat de houdingsvragen stelliger mogen worden neergezet omdat de houding gemeten moet worden. Tevens dienen de houdingsvragen dezelfde vorm aan te houden (positief en negatief geformuleerd).	Het deponeren van stellingen dwingt medewerkers meer om een standpunt in te nemen dan de wijze waarop de houdingsvragen nu zijn geformuleerd. Voor de eenduidigheid van de vragen is het ook wenselijk om één vorm qua vraagformulering aan te houden.	 Beide opmerkingen worden verwerkt.
Survey Vraagstelling	De CISO van Edam-Volendam geeft aan dat ten aanzien van de bepalende factor 'Laat digitale gegevensdragers nooit onbeheerd achter', bij de vraagstelling moet worden toegevoegd dat men dit niet onbeheerd achter laat *los van het feit of een of meerdere collega's nog op de afdeling aanwezig zijn*. Medewerkers zullen de vraag anders interpreteren dat onbeheerd betekent dat dit enkel geldt als zij hun werkplek verlaten en ook hun collega's niet meer aanwezig zijn.	De bepalende factor is erop gericht dat medewerkers geen gegevensdragers onbeheerd achter laten om diefstal en of misbruik te voorkomen. Dit kan ook door collega's.	 Opmerking van de CISO Edam-Volendam is terecht en in lijn met hetgeen dat de vraagstelling beoogt te meten.
Survey Vraagstelling	De CISO van Edam-Volendam geeft aan dat de kennisvraag 'ik ken de dreigingen die gepaard gaan met het uitlenen van mijn toegangspas aan een collega (of aan anderen)', de kans bestaat dat dit de verwachting kan wekken bij medewerkers dat toegangspassen mogen uitlenen.	Dat is een aanname. Belangrijk is dat medewerkers weten hoe de vragen gelezen moeten worden, dat zij deze begrijpen en betrouwbare antwoorden kunnen geven.	 Om sociaal wenselijkheid zo veel mogelijk te beperken is het belangrijk om bij de inleiding van de survey duidelijk aan te geven wat het doel van de vragenlijst is, dat anonimiteit wordt gewaarborgd en hoe de vragen gelezen moeten worden.
Survey Vraagstelling	In het interview met betrokkenen van de campagne iBewust Overheid wordt opgemerkt dat aan de kennisvragen die gericht zijn op de drie elementen uit de literatuur, een specifieke vraag vooraf kan worden gesteld, zoals: ik weet dat ik mijn bezoekers moet aanmelden. Dit gaat vaak vooraf aan de waarom vraag.	Door aan alle bepalende factoren de vraag te koppelen 'ik weet dat ik iets wel of niet mag' gevolgd door 'ik weet wat het effect is van mijn gedrag wanneer ik dat gedrag wel of niet vertoon' betekent dat er voor elke bepalende factor twee kennisvragen worden gesteld. Hierdoor neemt het aantal vragen van de survey met tientallen toe.	 Dit tast de bruikbaarheid van de survey toe. Medewerkers zullen minder bereidwillig zijn om een survey in te vullen als de survey veel tijd in beslag neemt. Daarnaast is de kans dat bij veel vragen de vragen onzorgvuldig worden gelezen en minder wordt nagedacht over het te geven antwoord, waardoor de betrouwbaarheid van de antwoorden afzwakt.

Survey Vraagstelling	De voorzitter van de domeingroep Awareness van het CIP geeft aan dat bij de kennisvraag omtrent het doorvoeren van software-updates erbij vermeld moet worden dat het gaat om de door de organisatie aangereikte software-updates. Dit heeft te maken met de Baseline Informatiebeveiliging die er vanuit gaat dat wat de organisatie aanreikt aan zijn medewerkers, dat dit veilig/verantwoord is. Dan moet een medewerker de updates krijgen aangereikt en deze moet hij dan vervolgens ook doorvoeren.	Medewerkers gebruiken niet alleen zakelijke mobiele devices maar ook privé devices voor zakelijke doeleinden. Op de privé devices krijgen zij van hun werkgever ook geen software-updates aangereikt.		Vraagstelling wordt niet aangescherpt/aangevuld.
Survey Vraagstelling	De voorzitter van de domeingroep Awareness van het CIP merkt op bij de kennisvraag omtrent de wachtwoorden voor je zelf te houden, dat het delen van wachtwoorden niet alleen gevolgen hoeft te hebben voor burgers en dienstverlening, maar het kan ook persoonlijke gevolgen hebben (bijvoorbeeld als iemand onder jouw account naar porno kijkt). Hij adviseert om dat bij deze en vergelijkbare vragen aan te vullen. Daarbij sluit de houdingsvraag niet aan op de kennisvraag. Tevens wordt voorgesteld om hierbij ook te meten dat wachtwoorden met regelmaat moeten worden vervangen. Dat laatste stelt ook de IBD voor.	De BIG maakt duidelijk dat informatiebeveiliging bij gemeenten zich richt op burgers en dienstverlening. Verder geven gemeentelijke organisaties medewerkers toegang tot systemen, waar vanuit bepaald kan worden om de hoeveel tijd een wachtwoord gewijzigd dient te worden. Medewerkers krijgen dan vanzelf een melding. De kennisvraag is inderdaad niet in lijn met de houdingsvraag.		Kennisvraag wordt in lijn gebracht met de houdingsvraag. De vraagstelling wordt niet aangevuld met persoonlijke consequenties. Het is terecht maar de BIG richt zich op consequenties voor de dienstverlening en burgers. Tot slot wordt niet de vraagstelling uitgebreid met het regelmatig wijzigen van wachtwoorden. Dit is namelijk geen gedragsmaatregelen maar moet gefaciliteerd worden via de systemen.
Survey Vraagstelling	De voorzitter van de domeingroep Awareness van het CIP merkt op omtrent het gebruik van gratis wifi ten behoeve van webmail, dat het voorbeeld aangevuld kan worden met internetbankieren.	Dat is mogelijk, maar een concreet voorbeeld waarvoor medewerkers gebruik maken van gratis wifi om hun zakelijke mail op mobiele devices te kijken, maakt dat de vraag overeenkomt met de subfactor en gouden regel. Deze gaan namelijk over zakelijke informatie op mobiele devices. Internetbankieren valt hier niet onder.		De vraagstelling wordt niet aangescherpt.

Bijlage 14 Methodiek ter validatie bij empirisch onderzoeksfase 2

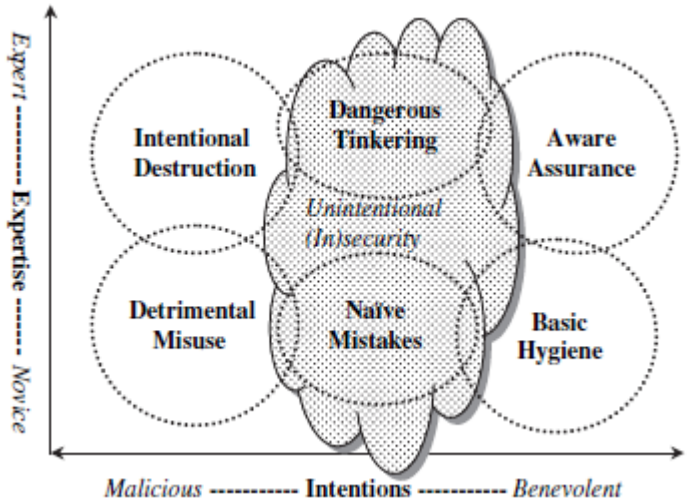



Type organisatie
Focus (op verschuiving)
Hoofdrisico's
Gedragsrisico's
Bepalende factoren
Surveyvraag Dimensie kennis
Surveyvraag Dimensie houding
Surveyvraag Dimensie gedrag
Overall iBewustzijn
Nederlandse gemeente
Verschuiving in fysieke werkomgeving: van binnen naar buiten (tijds- en plaatsonafhankelijk)
Verschuiving van alleen naar samenwerken (incl. meer vertrouwelijke data verwerken)
Verschuiving in informatiedrager: van analoog naar digitaal
Verschuiving van gesloten naar open data behandeling (online opslag/social media/ cloud)
Er lijkt een verschil in benadering tussen generaties inzake informatiebeveiliging
Organisatiecultuur sluit niet aan op de ontwikkelingen
Incidenten en verdachte zaken worden (niet) tijdig gemeld
Informatiebeveiliging wordt niet binnen processen geborgd
Verstoring continuïteit dienstverlening
Verlies, lekken en misbruik data
Toenemende cybercriminaliteit: hoofdzakelijk in de vorm van social enginering en besmette internetpagina's (cryptoware, ransomeware, identiteitsfraude)
Medewerkers worden onvoldoende meegenomen bij deze ontwikkelingen: kunnen waarde informatie niet inschatten; zijn onvoldoende bewust van hun rol en kunnen de impact/risico's/gevolgen van hun eigen handelen onvoldoende inschatten
Informatiebeveiliging en bijbehorende gewenste cultuur zijn niet geborgd
Onbevoegden toegang verschaffen tot onze gebouwen en werkplekken
Het niet (tijdig) melden van incidenten en verdachte zaken
Binnen kantoormuren niet voorzichtig omgaan met vertrouwelijke informatie
Buiten de kantoormuren onvoorzichtig werken met vertrouwelijke informatie
Zie vorige pagina
(Privé) mobiele apparaten met zakelijke informatie onvoldoende beveiligen
Beveilig mobiele apparaten met zakelijke informatie tegen ongautoriseerde toegang
Een van de basisbeveiligingsmaatregelen is het hebben van een wachtwoord/toegangscode op (privé) mobiele apparaten (mobiel, laptop, tablet), zeker als ik deze gebruik om zakelijke informatie mee te lezen (zoals werkmail)?
Mobiele apparaten die gebruikt worden voor zakelijke doeleinden dienen altijd voorzien te zijn van een toegangscode/wachtwoord
Als ik een privé apparaat (mobiel, laptop, tablet e.d.) gebruik voor mijn werk, dan zorg ik ervoor dat deze is voorzien van een toegangscode/wachtwoord
Installeer alleen apps als je zeker weet dat deze geen beveiligingsrisico vormen
Ik weet hoe ik beveiligingsrisico's kan achterhalen van software (en apps) die ik wil installeren
Voordat een medewerker software (en/of apps) installeert, moet hij deze eerst gecontroleerd hebben op beveiligingsrisico's
Zonder na te denken over beveiligingsrisico's, installeer ik software (en/of apps)
Voer softwareupdates door
Ik weet welke risico's het niet updaten van software op (mobiele) apparaten met zich meebrengen
Het is belangrijk dat wanneer er een melding wordt gedaan op het mobiele apparaat van een softwareupdate, dat deze softwareupdate gelijk wordt doorgevoerd
Als ik zie dat er een softwareupdate beschikbaar is, dan voer ik de softwareupdate gelijk uit
Bij reparatie of verkoop van een (mobiel) apparaat, altijd eerst de zakelijke gegevens op het apparaat (laten) wissen
Ik weet waarom het belangrijk is dat bij reparatie of verkoop van een (mobiel) apparaat eerst de zakelijke gegevens van het apparaat moet worden zijn gewist
Voordat een medewerker zijn (mobiel) apparaat laat repareren of verkoopt, moet hij er altijd eerst voor zorgen dat de zakelijke gegevens ervan zijn gewist
Als ik mijn (mobiel) apparaat verkoop of laat repareren, dan zorg ik ervoor dat eerst de zakelijke gegevens er vanaf zijn gewist
Installeer alleen betrouwbare software (en apps), of laat dit doen door iemand van ICT-helpdesk
Ik weet wat de gevolgen kunnen zijn als niet ICT maar ikzelf software installeert op mijn mobiele apparaten (laptop, mobiel, tablet e.d.)
Medewerkers moeten op mobiele apparaten (laptops, tablets, mobieltjes e.d.) die zij gebruiken voor hun werk, kunnen installeren wat zij willen
Als ICT mij niet wil helpen om software te installeren op mijn laptop dan ga ik op zoek naar hoe ik dit kan installeren zonder ICT
Zorg altijd voor een gedegen en up to date virusscanner en firewall op je eigen apparaten, zeker als je deze ook voor zakelijke doeleinden gebruikt
Ik weet wat het belang is van een goede up-to-date-virusscanner en een firewall op mijn privé apparten, die ik ook voor zakelijke doeleinden gebruik (zoals het raadplegen van mijn werkmail)
Medewerkers die privé apparaten ook voor zakelijke doeleinden gebruiken (zoals het raadplegen van werkmail), zijn ervoor verantwoordelijk dat zij een goede en up-to-date virusscanner en firewall hebben op eigen kosten
Mijn privé apparaten die ik gebruik voor mijn werk (zoals het raadplegen van mijn mail) beschikken over een virusscanner die ik tevens regelmatig update
Vatbaar voor phishing
Geef nooit inloggegevens aan anderen per email
Ik weet waarom ik niet mijn inloggegevens mag afstaan per email
Nooit en te nimmer mogen inloggegevens per email worden afgestaan
Als ICT mij per email vraagt om mijn inloggegevens om te voorkomen dat mijn werkaccount wordt geblokkeerd, dan geef ik deze gegevens per email
Open bij verdachte mails niet de bijlagen en klik niet op de linkjes
Ik weet waaraan ik verdachte e-mails kan herkennen
Bij een mail die niet verwacht wordt of enigszins verdacht overkomt, moeten medewerkers de bijlagen op het werk kunnen openen om de echtheid van de mail te controleren
Als ik op mijn privémail een mail krijg dat ik een factuur van een bestelling van mijn werkgever binnen 7 dagen moet betalen, dan open ik de bijlage om te kijken of deze factuur wel voor mij is
Check de website waar je inlogt en naar toe bent gelinkt vanuit de email. Bij twijfel niet inloggen
Ik weet waarom ik de website op echtheid moet controleren als ik op de website wil inloggen als ik vanuit een email naar deze website wordt doorgestuurd (toegelinkt)
Als een medewerker een mail ontvangt met een linkje daarin naar een website waarop men kan inloggen, dan moet een medewerker altijd voor het inloggen eerst de website op echtheid controleren (door te kijken of de url correct is weergegeven (url is http:www.'NAAM'.nl))
Ik controleer eerst de websites op waar ik naar toe wordt gelinkt vanuit een email op echtheid voordat ik op die website inlog
Onveilig internetten
Klik nooit op verdachte links, pop-ups, bestanden en banners/ advertenties
Als ik internet dan weet ik wat de gevaren zijn van het klikken op: advertenties als 'KLIK HIER, U HEEFT EEN PRIJS GEWONNEN'; en meldingen die de website onverwachts op je scherm laat verschijnen met 'Download nu deze software om verder te kunnen'.
Medewerkers mogen er blindelings op vertrouwen dat men veilig kan internetten op het werk, omdat ICT hiervoor moet zorgen
Als op een website staat 'U hebt een prijs gewonnen, klik hier om uw prijs op te halen' dan klik ik daarop
Gebruik geen gratis wifi om vertrouwelijke informatie mee te verwerken
Ik weet welke dreigingen gepaard gaan met het gebruiken van gratis wifi om mijn werkmail te lezen
Gratis wifi is veilig om vertrouwelijke informatie mee te verwerken (lezen, versturen, bewerken)
Ik gebruik gratis wifi om mee te werken, zoals het lezen van mijn werkmaill
Vertrouwelijke data online delen (opslaan, versturen en communicatie)
Sla geen vertrouwelijke informatie op in de openbare cloud
Ik ken de risico's van het versturen en opslaan van vertrouwelijke informatie met internetdiensten als Hotmail, Gmail, Wetransfer, Dropbox en dergelijke
Vertrouwelijke informatie moet verstuurd en opgeslagen kunnen worden met internetdiensten als Hotmail, Gmail, Wetransfer, Dropbox en dergelijke
Ik maak gebruik van internetdiensten als Hotmail, Gmail, Wetransfer, Dropbox en dergelijke om vertrouwelijke informatie mee te versturen of op te slaan (zodat ik bijvoorbeeld extern met deze informatie kan werken)
Communiceer online niet over zaken die schadelijk kunnen zijn voor je werk(gever)
Ik weet over welke werkgerelateerde zaken ik wel en niet online kan (en mag) communiceren
Mede in het kader van vrije meningsuiting: Medewerkers moeten online kunnen communiceren over hun werk(gever) wat ze willen
Ik let erop dat ik online geen zaken communiceer die schadelijk kunnen zijn voor mijn werk(gever)

Bijlage 15 De methodiek om het informatiebeveiligingsbewustzijn te meten bij medewerkers van Nederlandse gemeenten

De volgende stappen dienen te worden ondernomen om het informatiebeveiligingsbewustzijn (iBewustzijn) te meten (de methodiek, met bijbehorende kaders is weergegeven in figuur 5):

1. Van welke (doel)groep wordt het iBewustzijn gemeten? Management, ICT-ers, eindgebruikers of anderen? In dit onderzoek is de methodiek gericht op eindgebruikers (alle medewerkers);
2. Welk type gedrag wil je meten? Neutral en beneficial intentions, zie figuur 8, laten zich het beste meten via vragenlijsten, omdat medewerkers hierbij geen kwaadwillende intenties hebben en bereidwillig zijn om dit gedrag te laten meten. In dit onderzoek hebben de eindgebruikers geen kennis van IT en is de vragenlijst gericht op de intenties 'neutral/benevolent'. Figuur 8 laat zien welke zes gedragscategorieën er zijn. In dit onderzoek lag de focus op de gedragscategorieën 'naïve mistakes' / 'basic hygiene';



Figuur 8 Positionering van de gedragscategorieën (Stanton et al., 2005)

3. Vanuit welke focus worden de hoofdrisico's en vervolgens de gedragsrisico's gemeten? Oftewel, op welk vlak wil je het informatiebeveiligingsbewustzijn meten? Vanuit een project als Het Nieuwe Werken, vanuit leerdoelen, vanuit de hoofdstukindeling van de BIG of anders? In dit onderzoek ligt de focus op interne en externe ontwikkelingen die van invloed zijn op het functioneren van een gemeente;
4. Bepaal de hoofdrisico's (met betrokkenen/stakeholders) vanuit de focus. Welke risico's brengt deze focus met zich mee voor de organisatie;
5. Bepaal vervolgens hoe het gedrag van medewerkers hierop van invloed is en dus welke gedragsrisico's er gemeten moeten worden. Indien er een één op één relatie gelegd kan worden tussen een hoofdrisico en een gedragsrisico, dan is het mogelijk om het iBewustzijn niet alleen op gedragsniveau te analyseren, maar ook op niveau van hoofdrisico's (zie ter illustratie figuur 4);

6. Bepaal per gedragsrisico de factoren die dit risico typeren om vervolgens per factor surveyvragen op te stellen;
7. Houd bij het opstellen van de survey rekening met de kaders die in figuur 5, bij de methodiek, zijn beschreven;
8. Zet de survey uit. Dit kan via een enquête, maar de survey kan ook behandeld worden in een bijeenkomst met een groep die representatief is voor de organisatie;
9. Kwantificeer de resultaten met de formule van de waardefunctie;
10. Analyseer het gekwantificeerde informatiebeveiligingsbewustzijn vanuit meerdere perspectieven om tot slot de conclusies te trekken.