UNIVERSITEIT TWENTE

veiligheidsregio limburg-noord

Het verhogen van het informatieveiligheidsgedrag van medewerkers van Veiligheidsregio Limburg-Noord

Auteur	:	Mevr. D.J.A.M. Jetten - von der Haar
Faculteit	:	Faculteit Behavioral, Management and Social Sciences Master Risicomanagement Universiteit Twente
Begeleiders	:	Dr. Ir. J.W. Bulleé, Universiteit Twente Dr. Ir. M.T. van Staveren MBA, Universiteit Twente Prof. Dr. Ir. J.I.M. Halman, Universiteit Twente Dr. P. van Mullekom, Veiligheidsregio Limburg Noord Mevr. M. Meijer, Veiligheidsregio Limburg Noord
Versie	:	1.0

Voorwoord

Met trots presenteer ik u mijn afsluitende masterscriptie risicomanagement aan de Universiteit Twente over het actuele en te bevorderen informatieveiligheidsgedrag in de organisatie van de veiligheidsregio Limburg-Noord. De scriptie is een sluitstuk van een periode waarin ik een aantal mensen tot “last” ben geweest, maar ontzettend wil bedanken voor hun hulp, bereidheid en geduld: de opdrachtgever Veiligheidsregio Limburg-Noord, maar ook de universiteit, mijn familie en studiegenoten.

Het onderwerp informatieveiligheid is de afgelopen jaren steeds belangrijker geworden in onze digitale samenleving en is van cruciaal belang voor het waarborgen van de veiligheid van persoonlijke gegevens en het beschermen van organisaties tegen cyberaanvallen. Het doel van deze scriptie is om inzicht te krijgen in het huidige informatieveiligheidsgedrag van medewerkers werkzaam bij de Veiligheidsregio Limburg -Noord en te onderzoeken hoe dit gedrag verder kan worden verbeterd.

In deze scriptie is er gebruik gemaakt van de wetenschappelijke “Human Aspect of Information Security Questionnaire” (de zogenaamde HAIS-Q vragenlijst). Met deze vragenlijst kan het niet alleen het informatieveiligheidsgedrag, maar ook de kennis en de houding van medewerkers ten aanzien informatieveiligheid in een organisatie worden gemeten. Hiernaast is gebruik gemaakt van het zogenoemde “Capability, Opportunity, Motivation-Behaviour” (COM-B) model, om te onderzoeken welke interventiemogelijkheden in te zetten zijn voor het bevorderen van het informatieveiligheidsgedrag van de medewerkers in de organisatie van de Veiligheidsregio Limburg-Noord.

Deze scriptie beoogt een bijdrage te leveren tot de verdere ontwikkeling van wetenschappelijke en maatschappelijke inzichten op het gebied van informatieveiligheidsgedrag. Op basis van de resultaten van dit afstudeerproject, zijn in 2023 door de Veiligheidsregio Limburg-Noord stimulerende leerprogramma’s geïmplementeerd die erop gericht zijn het informatieveiligheidsgedrag van medewerkers verder te verhogen.

Inhoudsopgave

Samenvatting

Op verzoek van de Veiligheidsregio Limburg-Noord (VRLN) is een afstudeeronderzoek uitgevoerd naar het bevorderen van het informatieveiligheidsgedrag van medewerkers in de organisatie. Informatieveiligheidsgedrag verwijst naar het gedrag van medewerkers dat gericht is op het beschermen van vertrouwelijke en gevoelige informatie van een organisatie tegen ongeautoriseerde toegang, de vernietiging of het wijzigen van bedrijfsinformatie. De toenemende stroom aan cyberaanvallen gaat niet aan veiligheidsregio's voorbij. De VRLN kreeg in 2022 nog te maken met een 'hack. En recent, in opdracht van de VRLN uitgevoerd onderzoek naar informatieveiligheid noemt het onvoldoende monitoren van het informatieveiligheidsgedrag van medewerkers als één van de belangrijkste aandachtspunten voor verbetering. Naar aanleiding van deze ontwikkelingen werd als doel van dit afstudeeronderzoek *het verhogen van de informatieveiligheid van de Veiligheidsregio Limburg-Noord geformuleerd* met als hoofdvraag voor dit onderzoek: *Op welke wijze is het informatieveiligheidsgedrag van medewerkers bij de VRLN op structurele wijze te bevorderen?* Om deze hoofdvraag te kunnen beantwoorden, werd het onderzoek opgedeeld in een drietal deelonderzoeken:

- Het in kaart brengen van de variabelen die te gebruiken zijn voor het beoordelen van de effectiviteit van het informatieveiligheidsgedrag. Hiertoe heeft een uitgebreide verkenning plaatsgevonden naar relevante wetenschappelijke literatuur. Deze literatuurstudie maakte duidelijk dat met behulp van de 'Human Aspects of Information Security Questionnaire', de HAIS-Q, het informatieveiligheidsgedrag van medewerkers kan worden gemeten en geclassificeerd. Voor het bestuderen van gedragsveranderingen werd gekozen voor het 'Capability Motivation Behaviour (COM-B) model' omdat dit model het beste blijkt aan te sluiten op de HAIS-methodiek.
- Het uitvoeren van een 0-meting en analyse naar het informatieveiligheidsgedrag van medewerkers van de VRLN. Hierbij is gebruik gemaakt van een op de specifieke VRLN context aangepaste HAIS-vragenlijst. De 0-meting maakte duidelijk dat van de 69 gestelde vraagstellingen naar veiligheidsgedrag, er vier als kritisch kunnen worden gelabeld en op korte termijn noodzaken tot gerichte interventie. Een nadere analyse van deze vier vraagstellingen maakte duidelijk dat de scores demografisch verschillend zijn voor de vijf in het onderzoek onderscheiden leeftijdsgroepen. Deze demografische verschillen wijzen op de noodzaak van een gedifferentieerde aanpak bij het bevorderen van het informatieveiligheidsgedrag bij medewerkers van de VRLN.

- Een aanvullende literatuurstudie maakte duidelijk dat een door Susan Michie, Lou Atkins en Robert West (2014) ontwikkelde methode voor het ontwerpen van gedragsveranderingsinterventies passend voor de specifieke situatie bij de VRLN. Deze methode is vervolgens toegepast om mogelijke interventies af te leiden om het informatieveiligheidsgedrag bij E-mail gebruik bij de VRLN te bevorderen. Daarnaast is met behulp van een door Van Staveren (2018) ontwikkelde vragenlijst nagegaan, welke risicovaardigheden er binnen de organisatie verder ontwikkeld dienen te worden.

Op basis van de uitgevoerde deelonderzoeken, kan worden gesteld dat het informatieveiligheidsgedrag van medewerkers bij de VRLN op structurele wijze kan worden bevorderd door:

- De voor de 0-meting aangepaste HAIS-Q vragenlijst, periodiek opnieuw uit te zetten in de organisatie. Op basis hiervan kan niet alleen worden vastgesteld welke vorderingen er zijn gemaakt op het gebied van het informatieveiligheidsgedrag bij medewerkers bij de VRLN, maar ook wat de volgende te nemen prioriteiten zijn ten aanzien van het bevorderen van de informatieveiligheid.
- Een vervolg van de toepassing van de door Michie et al. (2016) ontwikkelde methode voor het ontwerpen en implementeren van gedragsveranderingsinterventies.
- Het op continue wijze bevorderen van het informatieveiligheidsgedrag in de organisatie door het implementeren van een cyclisch Plan-Do-Check-Act leerproces voor de te implementeren en de al geïmplementeerde interventies ter bevordering van het informatieveiligheidsgedrag bij medewerkers van de VRLN.

Het afstudeeronderzoek sluit af met een discussie van de wetenschappelijke en maatschappelijke bijdrage van het onderzoek, de beperkingen onderzoek en doet een aantal aanbevelingen voor het vervolg.

Trefwoorden: Informatieveiligheidsgedrag, HAIS-Q, COM-B, BCW, 0-meting, gedragsinterventies.

Summary

At the request of the Limburg-North Safety Region (LNSR), a master study was carried out investigate the information security behaviour of employees in the organization. Information security behaviour refers to employee behaviour aimed at protecting an organization's confidential and sensitive information from unauthorized access, destruction, or alteration of company information. The increasing stream of cyberattacks has not gone unnoticed by security regions. Recently, the LNSR also had to deal with a hack in 2022. And information security research, commissioned by the LNSR, mentions insufficient monitoring of the information security behaviour of employees at LNSR as one of the most important points for improvement. As a result of these developments, the main research question for this master thesis study was formulated as: *How can the information security behaviour of employees at the LNSR be structurally promoted?*

To answer this main research question, three sub-studies were conducted by:

- Finding out the variables that can be used to assess the effectiveness of information security behaviour. To this end, an extensive exploration of relevant scientific literature has taken place. This literature study made it clear that the information security behaviour of employees can be measured and classified using the 'Human Aspects of Information Security Questionnaire', the so-called 'HAIS-Q'. The 'Capability Motivation Behaviour (COM-B) model' was chosen to study behavioural changes because this model appeared to be the best match with the HAIS method.
- Conducting a baseline measurement and analysis of the information security behaviour of VRLN employees. A HAIS questionnaire adapted to the specific VRLN context was used for this. The baseline measurement made it clear that of the 69 questions asked about safety behaviour, four can be labelled as critical and require targeted intervention in the short term. A closer analysis of these four questions made it clear that the scores differ demographically for the five age groups distinguished in the study. These demographic differences indicate the need for a differentiated approach in promoting information security behaviour among LNSR employees.
- An additional literature study made it clear that a method developed by Susan Michie, Lou Atkins and Robert West (2014) for designing behaviour change interventions is appropriate for the specific situation at the LNSR. This method was then applied to derive possible interventions to promote information security behaviour in E-mail use at the LNSR. In addition, a questionnaire developed by Van Staveren (2018) was used to determine which risk skills should be further developed within the organization.

Based on the three conducted sub-studies, it can be said that the information security behaviour of employees at the LNSR can be structurally promoted by:

- Periodically redistributing the adapted HAIS questionnaire in the organisation. This will not only make it possible to determine what progress has been made in the field of information security behaviour among LNSR employees, but also what the next priorities are to be taken regarding promoting information security behaviour.
- A continued application of the method developed by Michie et al. (2016) for designing and implementing behavioural change interventions for all critical security behaviour issues.
- The continuous promotion of information security behaviour in the organization by implementing a cyclical Plan-Do-Check-Act learning process for the interventions to be implemented and those already implemented. This to further promote information security behaviour among LNSR employees.

The master graduation research concludes with a discussion of the scientific and societal contribution of the research, the limitations of the research and makes several recommendations for follow-up.

Keywords: Information security behaviour, HAIS-Q, COM-B, BCW, Baseline measurement, Behavioural security interventions.

H1: Inleiding en onderzoekopzet

In dit hoofdstuk wordt een eerste schets gegeven over informatieveiligheid en de belangrijke rol die het gedrag van medewerkers speelt bij het borgen van de informatieveiligheid in een organisatie. Na een toelichting over Veiligheidsregio Limburg-Noord, wordt nader ingegaan op een aantal problemen die spelen met betrekking tot informatieveiligheid. Dit resulteert in de probleemstelling en de doelstelling van en in dit onderzoek en in de hoofdvraag en deelvragen die in dit onderzoek zullen worden beantwoord.

1.1 Achtergrond

"Without data you're just another person with an opinion" W. Edwards Deming

Zonder data geen informatievoorziening.

Verreweg de meeste organisaties zijn tegenwoordig afhankelijk van IT (informatietechnologie) en de bescherming ervan is dan ook een cruciale factor voor deze organisaties. Het borgen van de informatieveiligheid in een organisatie omvat het tegen ongeautoriseerde gebruikers beschermen van de data en informatie van een organisatie. Met het beschermen van de veiligheid van data en informatie, wordt de vertrouwelijkheid, de integriteit en de beschikbaarheid van de data en informatie voor daartoe geautoriseerde medewerkers zeker gesteld (Dhakal,2018; NEN 7510,2019; BIO,2020). Informatieveiligheidsgedrag verwijst naar het gedrag van medewerkers dat gericht is op het beschermen van vertrouwelijke en gevoelige informatie van een organisatie tegen ongeautoriseerde toegang, vernietiging of wijziging van bedrijfsinformatie (Parsons et al.,2017).

Met de voortgaande digitalisering van onze samenleving, is het de verwachting dat alle organisaties vroeg of laat te maken krijgen met cyberaanvallen (Van Der Kleij & Leukfeldt, 2019). In het recent uitgegeven Global Risks Report 2023 (Global Risks Report 2023 | World Economic Forum, z.d.), wordt de kans op het zich voordoen van cyberaanvallen en de soms wereldwijde impact hiervan als één van de top-10 risico's van deze tijd benoemd. Mede door een ontwikkeling zoals de oorlog in Oekraïne en de hiermee gepaard gaande toenemende cyberaanvallen, is in organisaties het besef gegroeid van de noodzaak tot het beschermen van de informatieveiligheid van de organisatie. Het gedrag van de medewerkers in de organisatie spelen in dit kader spelen een belangrijke rol, vaak zijn zij immers de veroorzaker van een informatieveiligheidsincident (Bulleé et al, 2015). De cascade van mogelijke effect-risico's en gedragingen zijn daarbij vaak moeilijk voorspelbaar (Slovic,2002; Taleb,2008). Uit verschillende studies, zowel gebaseerd op zelf-gerapporteerd gedrag als werkelijk gedrag in

experiment-setting, is gebleken dat veel mensen zich slechts in beperkte mate veilig online gedragen en zelfs ronduit onveilig gedrag vertonen online (Het Hoff-de Goede et al, 2019).
Om als organisatie weerbaar en wendbaar te zijn is informatie over informatieveilig en -onveilig gedrag van medewerkers onontbeerlijk om doeltreffende interventies op te zetten.

1.2 Case-organisatie Veiligheidsregio Limburg-Noord (VRLN)

Veiligheidsregio Limburg-Noord (VRLN) is een van de 25 Veiligheidsregio's in Nederland. Als veiligheidsregio speelt VRLN een belangrijke rol in de crisisbeheersing en rampenbestrijding in Limburg-Noord. Bijzonder aan de organisatieopzet van de VRLN is dat de GGD onderdeel uitmaakt van de VRLN. De VRLN beschikt anno 2023 over 636 werknemers en 774 (brandweer)vrijwilligers.
De VRLN werkt nauw samen met de brandweer, de politie, de gemeenten, de defensie, de waterschappen, het Rijkswaterstaat, de Ambulancezorg Limburg en met Prorail.
Om rampen en crises zoveel mogelijk te voorkomen, brengt VRLN veiligheidsrisico's in kaart en neemt op basis hiervan preventieve maatregelen. Daarnaast vinden regelmatig oefeningen plaats zodat een eventuele ramp of crisis zo effectief mogelijk kan worden bestreden. De belangrijkste risico's voor de regio Limburg Noord zijn volgens de VRLN: Potentiële aardbevingen; Brand en instortingsgevaar; Stralingsincidenten: Ongevallen met gevaarlijke stoffen; Extreem weer en overstromingen; Terrorisme; Natuurbranden; Ziektegolven; Ernstige Verkeersongvallen; Uitval van Nutsvoorzieningen en; Digitale ontwrichting en cyber risico's.
Natuurrampen zoals overstromingen, maar ook branden stellen vaak niet alleen de veiligheidsregio's en waterschappen aan Nederlandse zijde op de proef. Ook de Belgische en Duitse hulpdiensten en crisisstructuren worden in zulke situaties uitgedaagd. Internationale samenwerking is in zulke situaties noodzakelijk. Deze samenwerking is geregeld in verdragen die zijn omgezet in afspraken (convenanten) met Kreisen (districten in Duitsland) en Hulpverleningszones (België). En in 'burenhulpovereenkomsten' tussen brandweerkorpsen in Duitsland en in België.
In het beleidsplan 2020-2023 van de VRLN staat omschreven dat de organisatie *afhankelijk is van een betrouwbare informatievoorziening.* De VRLN wil dit realiseren in nauwe samenwerking met haar stakeholders: burgers, bedrijven, instellingen en partners. Voor het zekerstellen van een betrouwbare informatievoorziening is het noodzakelijk dat naast gedegen kennis over de regio, de bestaande samenwerkingsnetwerken worden onderhouden en dat mensen en middelen zich met elkaar verbonden voelen. Het gaat hier o.a. om gevoelige informatie over inwoners en gebouwen in de regio. Daardoor is er steeds een publieke en politieke belangstelling en zal interne en externe informatieverstrekking veilig moeten plaastvinden. De VRLN moet binnen dit kader voldoen aan de

richtlijnen voor informatieveiligheid vanuit de landelijke GGD en de Wet veiligheidsregio's (Ministerie van Justitie en Veiligheid, 2021). Het landelijk besluit van de brandweer en crisisorganisatie van 2021 heeft de richtlijnen gewijzigd van 32 controls op niveau 2 naar 137 controls op niveau 4. De landelijke GGD heeft in 2021 besloten om de certificering eis van de NEN7510 te behalen. De VRLN heeft hiertoe een document opgesteld waarin het te realiseren informatieveiligheidsbeleid is beschreven.

1.2.1 Het informatieveiligheidsbeleid van Veiligheidsregio Limburg-Noord

Veiligheidsregio Limburg-Noord (VRLN) erkent het belang van informatieveiligheid en is zich bewust van de potentiële ernstige gevolgen bij een gebrek aan een adequate informatiebeveiliging. Mede door de aangescherpte landelijke kwaliteitseisen en een aantal veiligheidsincidenten die zich de afgelopen paar jaar hebben voorgedaan, heeft er in de organisatie een versnelde doorontwikkeling plaatsgehad in de aanscherping van het informatiebeleid 2020-2024 van de VRLN met als doel:

1. *Preventie*, het voorkomen van veiligheidsincidenten. De VRLN wil dit doen door te voldoen aan de certificering criteria 's van de NEN 7510, een BIO volwassenheid niveau 4 eind 2023 en op ICT-niveau een detectiemethode die (automatisch) reageert op bedreigingen (SIEM)
2. *Detecteren*, het ontdekken van een besmetting of performance issues of het creëren van mogelijkheden om achteraf vast te kunnen stellen of er sprake is geweest van een inbreuk en monitoringsprocedures.
3. *Isoleren*, het beperken van de gevolgen van een succesvol veiligheidsincident.
4. *Repareren*, wanneer een "besmetting" plaats heeft gevonden dan moet herstel mogelijk zijn zoals back-up en re-store maar ook uitwijkprocedures en externe inhuur van bewaking/bescherming.

Om sturing te geven aan dit proces, heeft de VRLN een security board opgericht om bovenstaande beveiligingsmaatregelen uit te voeren, inclusief de wijze van het omgaan met datalekken. Een extern bedrijf ondersteunt de VRLN in het implementeren van de NEN 7510 en de BIO. In 2023 worden onder meer technische systemen aangekocht en geïnstalleerd. Het is daarbij de ambitie om vanuit een leercurve (Kotter, 1995) ook een bewustwording en gedragsverandering te creëren bij de medewerkers van de VRLN. In het strategisch informatiebeleid zijn ook tien principes opgenomen voor informatieveiligheidswaarden die het bestuur zichtzelf heeft opgelegd. Dit is een top-down benadering door het bestuur gericht op het bewerkstelligen van een vanuit risicosturing veilige cultuur. Daarbij worden standaarden voor informatieveiligheid risicogestuurd weergegeven. Die beginnen met verificatie voor vertrouwen (Zero Trust), waarin nooit (impliciet) vertrouwen is te geven, en het naleven van veiligheidsprincipes zoals het altijd verifiëren van de gegevens. Het beschermen van die gegevens

vindt plaats door naast het verzamelen van informatie ook het gewenste beschermingsniveau te bepalen. De wijze van veilige informatie-uitwisseling leidt tot aanpassingen in situaties dat er sprake is van een potentiële bedreiging. De kennis over zo'n potentiële dreiging wordt ook (vertrouwelijk) gedeeld met stakeholders buiten de organisatie. Het is de bedoeling om vanuit een leercurve (Kotter, 1995), informatieveilig gedrag risicogestuurd (Van Staveren, 2018) te verankeren in de gedragswaarden van de VRLN. Om deze leercurve succesvol te implementeren in de organisatie, is inzicht nodig in het huidige informatieveiligheidsgedrag. Dit vereist een 0-meting (IST-situatie) van het informatieveiligheidsgedrag in de organisatie.

1.3 Probleemstelling en doelstelling

De toenemende stroom aan cyberdreigingen gaat niet aan veiligheidsregio's voorbij. In dit verband kunnen genoemd worden de cyberaanval in 2020 met gijzelsoftware bij Veiligheidsregio Noord- en Oost Gelderland (VNOG), Log4J incidenten die zich voordeden in december 2021 en een recente 'hack' begin van januari 2022 bij Veiligheidsregio Limburg-Noord. Door eerdere, binnen VRNL in 2019 en 2021 uitgevoerde externe onderzoeken bestond weliswaar kennis en inzicht over potentiële cybergedrag-gerelateerde risico's, maar deze inzichten werden helaas niet benut voor gerichte gedragsinterventies. Tijdsdruk, onvoldoende kennis van effectieve interventies, het ontbreken van voldoende commitment en prioritering van het management en de beperkte (financiële) middelen waren belangrijke redenen voor het onvoldoende inzetten van gerichte gedragsinterventies.
In de meest recente onderzoeken naar informatieveiligheid, uitgevoerd door twee externe bedrijven, is het onvoldoende systematisch monitoren van het informatieveiligheidsgedrag van medewerkers als één van de belangrijkste aandachtspunten aangedragen (M&I/Partners, 2019; Securesult, 2021). Geadviseerd wordt tot het uitvoeren van een 0-meting (GAP-analyse) om zodoende te kunnen bepalen welke interventiemaatregelingen noodzakelijk zijn.
Samenvattend luidt de probleemstelling:

Veiligheidsregio Limburg-Noord heeft onvoldoende inzicht in het informatieveiligheidsgedrag van haar medewerkers en de mogelijkheden tot het plegen van effectieve interventies.

Het doel *van* dit onderzoek is:
Het verhogen van de informatieveiligheid van Veiligheidsregio Limburg-Noord
En het doel *in* dit onderzoek is:
Het verhogen van het informatieveiligheidsgedrag van medewerkers door:

- Het uitvoeren van een 0-meting van het informatieveiligheidsgedrag van medewerkers van Veiligheidsregio Limburg-Noord en
- Effectieve interventies voor te stellen voor het bevorderen van informatieveiligheidsgedrag van medewerkers

1.4 Afbakening van het onderzoek

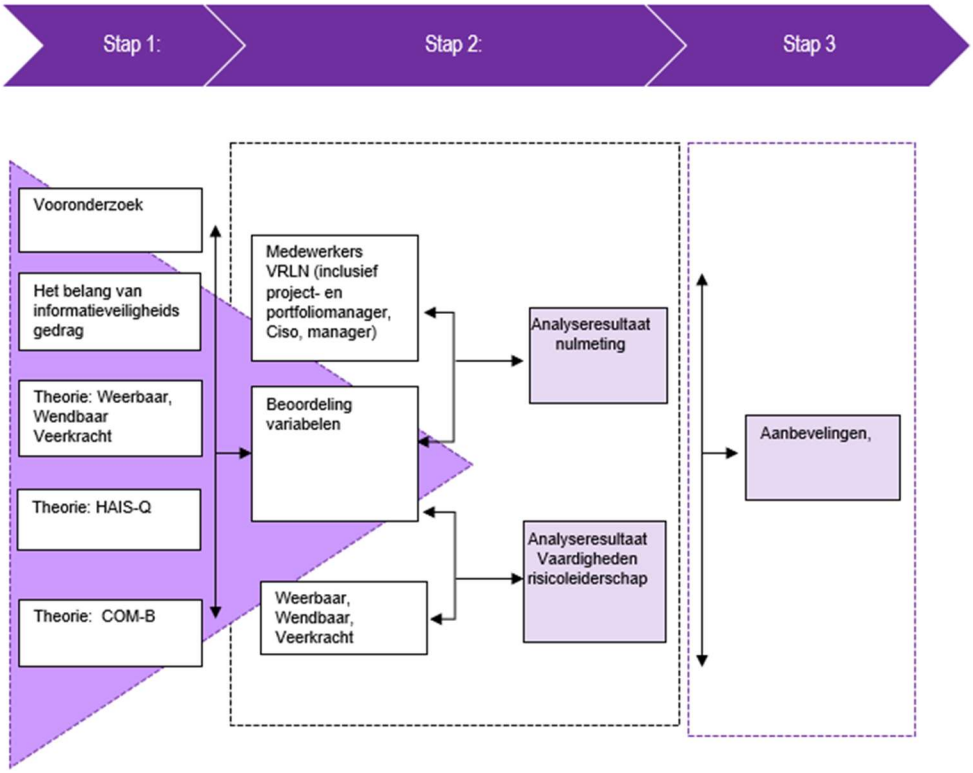
Het managen van informatieveiligheid gaat over meerdere aspecten. Echter, dit onderzoek beperkt zich tot het gedrag van de medewerkers van VRLN met betrekking digitale informatieveiligheid. Daarnaast heeft het onderzoek een afbakening in tijd, omdat de data verzameling plaats vond in de tweede helft van 2022. Hierdoor zijn nieuwe ontwikkelingen die plaatsvonden na deze periode niet meegenomen. Voor de analyse van de case-organisatie zijn geen andere veiligheidsregio(s) meegenomen en er heeft vanwege de beperkt beschikbare tijd, een selectie plaatsgevonden van een beperkt aantal maar relevante publicaties.

1.5 Hoofdvraag, deelvragen en onderzoeksopzet

De hoofdvraag vanuit de probleemstelling en doelstelling is:

Op welke wijze is het informatieveiligheidsgedrag van medewerkers bij VRLN op structurele wijze te bevorderen?

Om de hoofdvraag van dit onderzoek te beantwoorden, is een procesmodel voor het te voeren onderzoek opgesteld. (zie figuur 1.1). Hierin worden een drietal stappen onderscheiden. Voor elke stap is een deelvraag geformuleerd. Tezamen leiden de beantwoording van de drie deelvragen tot de beantwoording van de hoofdvraag (Verschuren & Doorewaard, 2021).



Figuur 1.1 Een procesmodel voor de uitvoering van het onderzoek

Deelvraag voor Stap 1:

Welke variabelen zijn te gebruiken voor het beoordelen van de effectiviteit van het informatieveiligheidsgedrag?

Het onderzoek is gestart met een vooronderzoek naar het informatieveiligheidsgedrag bij de VRLN. Tijdens dit vooronderzoek zijn relevante bedrijfsdocumenten doorgenomen en hebben er een aantal gesprekken plaats gehad met deskundigen in de organisatie. Het vooronderzoek heeft geleid tot het formuleren van de probleemstelling en doelstelling van het onderzoek en de op basis hiervan afgeleide hoofdvraag en deelvragen. Voor het beantwoorden van de eerste deelvraag, heeft er een verkenning plaatsgevonden naar relevante wetenschappelijke literatuur. Op basis van deze literatuurstudie werd duidelijk dat met behulp van de Human Aspects of Information Security Questionnaire (HAIS-Q) het informatieveiligheidsgedrag van medewerkers in een organisatie kan worden gemeten en geclassificeerd. De literatuurstudie maakte ook duidelijk dat er diverse gedragsmodellen zijn ontwikkeld voor het bestuderen van gedragsveranderingen in organisaties. Uiteindelijk is gekozen voor het Capability, Opportunity, Motivation Behaviour (COM-B) model omdat dit model het beste aansluit op de HAIS-Q meetmethodiek.

In hoofdstuk 2 is nader ingegaan op het uitgevoerde literatuuronderzoek en de op basis van dit onderzoek afgeleide variabelen voor het beoordelen van de effectiviteit van het informatieveiligheidsgedrag van medewerkers.

Deelvraag voor Stap 2*:*

> *Wat zijn de resultaten van een 0-meting en analyse van het informatieveiligheidsgedrag van medewerkers werkzaam bij Veiligheidsregio Limburg-Noord?*

Voorafgaande aan de 0-meting, zijn er een zevental semigestructureerde interviews[1] in de organisatie afgenomen. Doel van de interviews was om de validiteit en betrouwbaarheid van de HAIS-Q vragenlijst als meetinstrument te verifiëren. Daarnaast werd tijdens de interviews ook gevraagd naar interventiemogelijkheden om het veiligheidsgedrag van medewerkers te bevorderen. Eén geïnterviewde betrof de Gegevensbeschermer en project- en portfoliomanager van VRLN, drie interviews betroffen willekeurige respondenten in de organisatie en drie interviews vonden plaats met leden van een focusgroep bestaande uit leidinggevenden die betrokken zijn bij het bewaken van de informatieveiligheid in de organisatie. De semigestructureerde interviews hebben geleid tot een op beperkt aantal onderdelen aangepaste en uitgebreide HAIS-Q vragenlijst. Voorafgaande aan de daadwerkelijke uitvoering van het empirische onderzoek, is het onderzoek voorgelegd aan de Ethische commissie van de faculteit Behavioural, Management and Social Sciences (BMS). Door de commissie werd de methode voor data verzameling via de aangepaste HAIS-Q goedgekeurd. De interviews en de dataverzameling uit de enquête zijn volgens de ethische code van de Universiteit Twente en de privacyrichtlijnen van de VRLN uitgevoerd.
In hoofdstuk 3 is nader ingegaan op de resultaten van de gehouden interviews en de 0-meting en in hoofdstuk 3 is ook een analyse opgenomen van de resultaten.

Om de validiteit van het onderzoek te waarborgen, is gebruik gemaakt van een representatieve steekproef van de populatie van medewerkers van de VRLN. Hierbij de toepassing van de wetenschappelijke literatuur en een gevalideerd meetinstrument, de HAIS-Q. Daarnaast heeft triangulatie van de data plaatsgevonden door zowel kwantitatieve als kwalitatieve data te verzamelen en te analyseren.

[1] Bij semigestructureerde interviews worden vooraf gestructureerde vragen afgenomen. Maar tijdens de interviews wordt ook ruimte gegeven voor open antwoorden en discussie (Verschuren & Doorewaard, 2021).

Deelvraag voor Stap 3:

Hoe kan, gegeven de uitkomsten van de literatuurstudie en de gehouden 0-meting en analyse, het informatieveiligheidsgedrag in de organisatie verder worden bevorderd?

Op basis van de resultaten van de literatuurstudie (Stap 1, hoofdstuk 2) en de gehouden 0-meting en analyse van het informatieveiligheidsgedrag bij VRLN (Stap 2, hoofdstuk 3), zijn verbeterpunten afgeleid voor het bevorderen van het informatieveiligheidsgedrag bij medewerkers van VRLN.
In hoofdstuk 4 is op basis van een door Michie et al (2016) ontwikkelde methode voor het ontwerpen van gedragsveranderingsinterventies één van de vier te verbeteren aandachtsgebieden op het gebied van het informatieveiligheidsgedrag nader uitgewerkt.

1.6 Leeswijzer

In hoofdstuk 1 is eerst een toelichting gegeven over de achtergrond en aanleiding van dit afstudeeronderzoek. Ook zijn de probleemstelling, doelstelling, hoofdvraag en de aanpak die gevolgd is om de hoofdvraag te beantwoorden uiteen gezet. Hoofdstuk 2 beschrijft het theoretisch kader van dit onderzoek. In hoofdstuk 3 wordt ingegaan op de resultaten en de analyse van de onder medewerkers van Veiligheidsregio Limburg-Noord uitgevoerd onderzoek. De focus hiervan betreft het informatieveiligheidsgedrag van medewerkers werkzaam bij Veiligheidsregio Limburg-Noord. Op basis van de uitkomsten van de literatuurstudie (hoofdstuk 2) en het empirische onderzoek (hoofdstuk 3) wordt in hoofdstuk 4 een eerste aanzet gemaakt tot een plan voor het bevorderen van het informatieveiligheidsgedrag van medewerkers van Veiligheidsregio Limburg-Noord. Hoofdstuk 5 sluit af met een discussie van de wetenschappelijke en maatschappelijke bijdrage en de beperkingen van dit onderzoek en Hoofdstuk 6 sluit dit onderzoeksrapport af met de belangrijkste conclusies en met aanbevelingen voor het vervolg.

H2: Theoretisch kader

In dit hoofdstuk is de eerste deelvraag van het onderzoek beantwoord: *Welke variabelen zijn te gebruiken voor het beoordelen van de effectiviteit van het informatieveiligheidsgedrag?*
De structuur van dit hoofdstuk is als volgt. In paragraaf 2.1 wordt de aanpak van de uitgevoerde literatuurstudie uiteengezet. In paragraaf 2.2 wordt toegelicht dat binnen het kader van de (informatie)veiligheid en de continuïteit van een organisatie een vijftal factoren een cruciale rol vervullen. Het gaat om de Weerbaarheid, de Wendbaarheid, de Veerkracht, de Stuurbaarheid en de Inzetbaarheid van de capaciteit van medewerkers en hulpmiddelen van een organisatie (Halman en Huisman, 2021). De focus van dit onderzoek spitst zich toe op het gedrag van de medewerkers om de informatieveiligheid van de organisatie in positieve zin te beïnvloeden. In paragraaf 2.3 wordt daarom ingegaan op wetenschappelijke publicaties waarin het belang van het informatieveiligheidsgedrag in organisaties is onderzocht.
In paragraaf 2.4 wordt het "Human Aspects of Information Security Questionnaire" (HAIS-Q) toegelicht. Dit is een gevalideerd wetenschappelijk meetinstrument dat ontworpen is om het informatieveiligheidsgedrag van medewerkers te meten en te classificeren. In paragraaf 2.5 worden een viertal gedragsmodellen voor het onderzoeken van gedragsveranderingen toegelicht. Dit zijn respectievelijk de: Protectie Motivatie Theorie (PMT) van Rogers (1975); het Health Belief Model (HBM) (Dodel & Mesch, 2017); Het Theory of Planned Behaviour (TPB) model van Ajzen (1991) en het Capability, Opportunity, Motivation Behaviour model (COM-B) van Michie et al., (2011). Het COM-B model vormt de kern van het Behaviour Change Wheel (BCW) model. Het BCW model wordt nader in paragraaf 2.6 toegelicht. In paragraaf 2.7 wordt ingegaan op het door Van Der Kleij & Leukfeldt (2019) voorgestelde cyclische leerproces dat gericht is op het bevorderen van de (informatie)veiligheid. Het hoofdstuk sluit af met een antwoord in paragraaf 2.8 op de eerste deelvraag van dit onderzoek.

2.1 De gevolgde aanpak van het uitgevoerde literatuuronderzoek

De wetenschappelijke literatuur is verkend om inzicht te krijgen in de bestaande kennis over informatieveiligheidsgedrag. Om hiervoor een zo breed mogelijk inzicht te krijgen is tijdens het literatuuronderzoek gebruik gemaakt van een drietrap gestructureerde aanpak (Van Aken & Berends, 2018, p179). In de eerste fase is een oriëntatie uitgevoerd naar mogelijk relevante informatie. Hierbij is gebruik gemaakt van de zoekmachine Google Scholar, de eigen organisatie, de bibliotheek van de

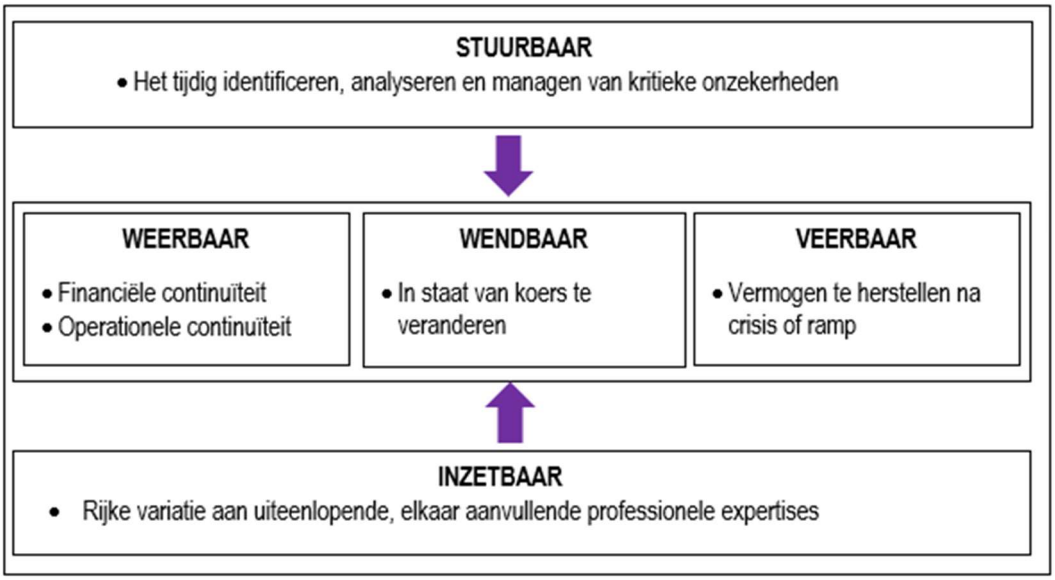
Universiteit Twente, lesstof en artikelen die verstrekt zijn gedurende de studie. Hierbij zijn de volgende zoektermen in willekeurige volgorde en sommige gecombineerd gebruikt in het Engels (niet weergegeven) en het Nederlands: informatieveiligheid, informatieveiligheidsgedrag, HAIS-Q, gedragsmodel, risicoleiderschap en veerkracht. In de tweede fase is de techniek backward reference searching gebruikt, waarbij vanuit de gevonden literatuurlijst gekeken is naar eerdere relevante publicaties. In de derde fase zijn de meeste recente studies (forward reference searching) geraadpleegd, waarbij ook contact is gelegd met professionals in de organisatie. Het geheel volgens een inductief proces waarna de belangrijkste gevonden literatuur voor het beantwoorden van de onderzoekvragen opgenomen zijn in deze scriptie.

2.2 De (informatie)veiligheid en de continuïteit van een organisatie

Zoals in de inleiding gesteld is het voor de (informatie)veiligheid van een organisatie van belang dat deze beschikt over een voldoende niveau van weerbaarheid, wendbaarheid en veerbaarheid en dat de organisatie in crisistijd niet alleen stuurbaar is, maar is ook de inzetbaarheid van sterk gedreven, gemotiveerde en veelzijdige medewerkers cruciaal (zie ook figuur 2.1) (Halman & Huisman, 2021).

Een *voldoende niveau van weerbaarheid*.

Een organisatie zal dienen te beschikken over een voldoende niveau van weerbaarheid om bij een informatieveiligheid incident deze te weerstaan, Voor de operationele continuïteit van een organisatie is de beschikbaarheid van een robuuste IT infrastructuur en de cyberweerbaarheid van de IT-infrastructuur van eminent belang (Halman & Huisman,2021; Van Der Steen & Van Twist, 2014).



Figuur 2.1 Een conceptueel model voor het evalueren van de (informatie)veiligheid van een organisatie (Halman & Huisman, 2021)

Een voldoende niveau van wendbaarheid

Bij onverwachte veranderingen zoals een naderende ramp of crisis (pandemie, oorlog, natuurramp, cyberaanval) is het belangrijk dat een organisatie het vermogen heeft om hierop te reageren en tijdig de koers te veranderen om doelen te blijven behalen of/en te blijven overleven (Halman, 2021).

Een voldoende niveau van veerbaarheid

Veerkracht is het vermogen om te herstellen na een grote persoonlijke tegenslag of tragedie. En voor een organisatie is dit het vermogen om te herstellen van de schade nadat zich een grote ramp zoals een grootschalige hack, een oorlogssituatie, een natuurramp of een pandemie heeft voorgedaan. Het stelt vele organisaties voor de vraag of zij wel na afloop van een ramp of crisis weer gewoon de oude draad kunnen oppakken (Het Hoff-de Goede et al.,2019; Leukfeldt, 2017; Halman,2021).

Een voldoende niveau van stuurbaarheid

Voor een organisatie is het essentieel dat deze beschikt over een goed overzicht en inzicht over hetgeen zich in haar directe interne en externe omgeving afspeelt. Bij stuurbaarheid gaat het in essentie om het vermogen van de leiding tot het tijdig identificeren, analyseren en managen van kritieke onzekerheden.

Een voldoende niveau van professionele inzetbaarheid

Voor het kunnen beheersen van de informatieveiligheid van een organisatie is ook de professionele van de medewerkers van essentieel belang. Dit vereist de inzetbaarheid van sterk betrokken medewerkers met elkaar aanvullende expertises en competenties.

2.3 Het belang van Informatieveiligheid gedrag

Informatieveiligheidsgedrag verwijst naar het gedrag van medewerkers dat gericht is op het beschermen van vertrouwelijke en gevoelige informatie van een organisatie tegen ongeautoriseerde toegang, vernietiging of wijziging (Parsons et al.,2017). Voor het beschermen van informatieveiligheid, moet de mens proactief gedrag uitvoeren. Als medewerker in een organisatie, is het individu ook een belangrijke schakel voor het beschermen van de informatieveiligheid van een organisatie (Bulleé,2017; Häussinger,2015). Dhakal (2018) omschrijft dit gedrag als het cyclisch bewust omgaan met het informatieveiligheidsbeleid, risico's kennen, begrijpen en informatieveilig gedrag toepassen op de werkplek. Hierbij zijn de beïnvloedbare factoren voor gedrag voornamelijk de kennis, de houding en de omgeving. In navolging van Dhakal (2018) wordt in dit onderzoek informatieveilig gedrag omschreven als: *De gedragingen om informatieveilig met gegevens om te gaan. Die gedragingen zijn*

in overeenstemming met het beleid en de procedures van de organisatie(omgeving); dit beleid en de bijbehorende procedures zijn op verzoek van een daartoe bevoegde persoon of organisatie zo nauwkeurig en compleet mogelijk samengesteld. De operationele definitie of standaard voor informatieveiligheidsgedrag is niet wetenschappelijk onderbouwd, maar is onder te brengen in acht gedragsgebieden (Het Hoff-de Goede et al.,2019). Deze zijn in paragraaf 2.4 toegelicht.

2.4 Human Aspects of information Security Questionnaire (HAIS-Q)

De Human Aspects of Information Security Questionnaire (HAIS-Q) is een gevalideerd wetenschappelijk meetinstrument ontworpen om het informatieveiligheidsgedrag van medewerkers te meten en te classificeren. Het meetinstrument bestaat uit acht aandachtspunten (Parsons et al.,2017; Verbeek, 2021; Clarke &Furnell, 2020,2022) (bijlage A):

1. Authenticatiemiddelen (Bewust van hoe de (digitale) gegevens en apparaten te beschermen)
2. E- mail gebruik (Bewust van veilig gebruik van Email en verstrekte informatie in bijlagen)
3. Internet gebruik (Bewust van veilig internetten, downloaden en websites)
4. Social media (Bewust van privacy-instellingen en nettiquette)
5. Gebruik van mobiele apparatuur (Bewust van duurzaam, toegankelijkheid en fysiek veiligheid)
6. Informatieverwerking (Bewust van informatie opslaan, weggooien of elders opslaan)
7. Incidenten management (Bewust van het beperken en melden incidenten)
8. Privacy (Bewust van de etiquette van privacy en daarnaar handelen)

Bovenstaande acht aandachtsgebieden zijn in Bijlage A nader toegelicht.

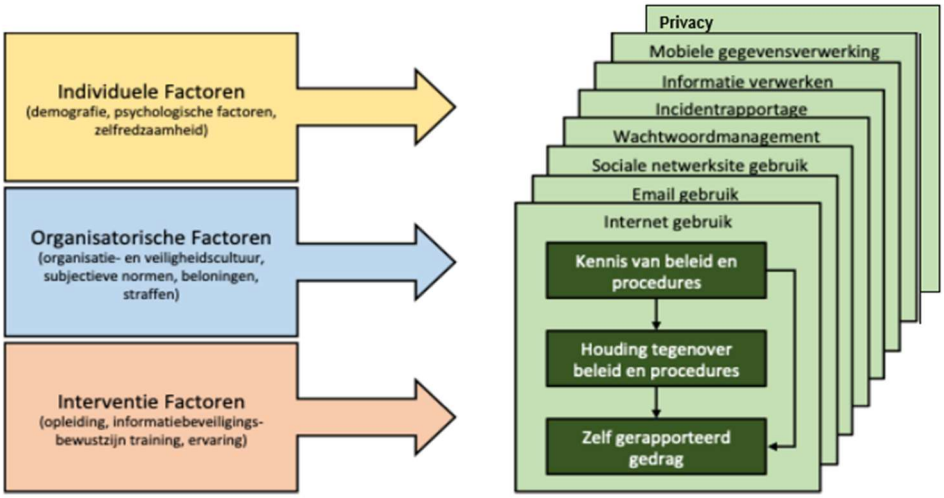
De aandachtsgebieden zijn in de HAIS-Q geclassificeerd in een drietal gedragsvariabelen: Houding, Kennis en Gedrag. De toepasbaarheid van de drie gedragsvariabelen geldt voor alle lagen en functies in een organisatie (Het Hoff-de Goede et al.,2019).

Houding: De houding van medewerkers ten opzichte van informatieveiligheid is van invloed op hun gedrag. Als medewerkers het belang van informatieveiligheid inzien en zich verantwoordelijk voelen voor het beschermen van bedrijfsinformatie, zullen ze eerder veilig gedrag vertonen. De (werk)omgeving en de cultuur van een organisatie beïnvloeden de houding van medewerkers ten opzichte van informatieveiligheid.

Kennis: De mate waarin medewerkers kennis hebben over informatieveiligheid en ook de procedures en de beleidsmaatregelen die daarbij horen kennen, is van invloed op het veiligheidsgedrag van medewerkers. Bijvoorbeeld, als medewerkers onvoldoende kennis hebben over de risico's van het delen van wachtwoorden, kan dit leiden tot onbewust risicovol gedrag.

Gedrag: Dit betreft het daadwerkelijke gedrag van medewerkers ten aanzien van de informatieveiligheid, zoals het regelmatig wijzigen van wachtwoorden, het voorkomen van ongeautoriseerde toegang tot systemen en het melden van verdachte activiteiten.

Door het aan de hand van de drie gedragsvariabelen onderzoeken van de informatieveiligheid in een organisatie, kan duidelijk worden waarom een individu zich (niet) houdt aan specifieke beveiligingsmaatregelen (Siponen et al., 2010). In het model van Parsons et al (2014) is ook een relatie weergegeven tussen de acht aandachtsgebieden met een drietal factoren: Individuele factoren (demografische, psychologische en zelfredzaamheid); Organisatorische factoren (de organisatie- en veiligheidscultuur, subjectieve normen, beloningen en straffen) en; Interventiefactoren (door opleiding, training en ervaring ontwikkeld bewustzijn over informatieveiligheid). De HAIS-Q is door Schaeken (2018) en Verbeek (2021) in het Nederlands vertaald en aangevuld met het aandachtsgebied Privacy. In **Fout! Verwijzingsbron niet gevonden.**2.2 is het model van Parsons et al. (2014) daarom voor dit onderzoek aangevuld met het aandachtsgebied Privacy.



Figuur 2.2 Aangepaste HAIS-Q met aandachtsgebieden vanuit Parson et al.(2014)

2.5 Gedragsmodellen die aansluiten bij de HAIS-Q

In de wetenschappelijke literatuur zijn er diverse gedragsmodellen beschreven voor het onderzoeken van gedragsveranderingen. De reden dat in dit onderzoek is gekozen voor een vergelijking van de PMT (Protectie Motivatie Theorie model) van Rogers (1975); de HBM (het Health Belief Model) (Dodel & Mesch,2017); de TPB (het Theory of Planned Behaviour) van Ajzen (1991) en; het COM-B (Capability Opportunity, Motivation Behaviour mode) van Michie et al. (2011) is dat deze vier modellen het meest frequent zijn toegepast om gezondheidsgedrag en veiligheidsgedrag te verklaren. Voor het verklaren van de factoren die van invloed zijn op gedragsverandering zijn deze

vier modellen ook wetenschappelijk gevalideerd. Tabel 2.1 geeft een vergelijkend overzicht van de vier modellen.

Tabel 2.1 Vergelijkend overzicht van vier gedragsmodellen t.b.v. informatieveiligheidsgedrag

Gedragsmodel	Elementen	Voordeel	Nadeel
Protectie motivatie Theorie (PMT) Rogers (1975)	Fear- control: Angst (Fear) control process Effectinschatting (risicoperceptie/gedrag) Respons-effectiviteit (reactievermogen)/ Eigen effectiviteit Cognitief gedrag vanuit sociale perceptie en verwachting	Werkt vanuit Angst Beloning op korte termijn.	Angst is suggestief en slecht meetbaar. Overtuiging/willen Gericht op kort termijn. Fear werkt niet als er overdrijving is (Rogers, 1975)
Health belief model (HBM) Abraham & Sheeran,2015)	Cognitief gedrag vanuit een positieve instelling vanuit motivatie (willen) Risicoperceptie	Werkt vanuit motivatie/willen.	Geen omgevingsfactoren Geen zelf-effectiviteit (Conner & Norman,2022; Parsons et al,2017
Theory of planned behavior, (TPB) Ajzen(1991)	Gepland gedrag (intentie) Houding Risicoperceptie vanuit bekende risico's	Werkt vanuit houding/intentie/ verwacht gedrag.	Geen omgevingsfactoren en 'zwarte zwanen'. Gaat om verwacht gedrag en niet het gedrag zelf. (Verbeek, 2021)
COM-B model Michie, Van Strale, & West (2011)	Kennis, omgeving, motivatie (risicotolerantie) naar gedrag (risicoperceptie) reflectie motivatie	Werkt vanuit meerdere invalshoeken	Afhankelijk van inzicht in invalshoeken. (Michie,2014)

2.5.1 Protectie- Motivatietheorie (PMT)

Het gedragsmodel van Rogers (1975) kijkt vanuit de Protectie-Motivatie-theorie (voortaan PMT) naar twee processen: 'Danger control' door het beheersen van het risico. 'Fear control is vanuit de emotionele actie gericht op het verminderen van het angstgevoel (Engels fear-appeal)'. Hierbij ontstaat het vertrouwen door een inschatting te maken van de ernst van het gevaar (threat appeal), de kwetsbaarheid(perceptie) en de aanwezigheid van een effectiviteitsinschatting (coping appraisal) voor het maken van een inschatting van het eigen kunnen. Bij het PMT zijn drie elementen zichtbaar: risicoperceptie, respons-effectiviteit en eigen effectiviteit en die zijn weer afhankelijk van elkaar. Hierbij geeft de theorie aan dat een hoge risicoperceptie alleen tot preventief gedrag zal leiden wanneer de respons-effectiviteit en de eigen effectiviteit hoog is (Kasperson, et al., 1998). Het nadeel van de PMT is dat deze uitgaat van angst-aantrekkingskrachtmanipulaties dat beperkt meetbaar is.

2.5.2 Health belief model (HBM)

Het Health belief gedragsmodel (HBM) is ontwikkeld om gezondheidsproblemen aan te pakken (Abraham & Sheeran, 2015). Het maakt gebruik van de perceptie van de mens over hoe

groot deze het probleem ervaart en het risico inschat. Uitgangspunt is de perceptie van de mogelijke voordelen van de te nemen maatregelingen en de mogelijke te nemen barrières. Het HBM kenmerkt zicht als een praktisch model voor de ontwikkeling van de eigen percepties en gaat uit van een rationele benadering (Mukhtar, 2020). Het HBM houdt geen rekening met de dynamische aspecten van gedragsverandering en het verschil in motivatie-, emotionele- en omgevingsfactoren (Conner & Norman, 2022). Door deze tekortkomingen wordt er onvoldoende rekening gehouden met de complexiteit van informatieveiligheidsgedrag.

2.5.3 Theory of Planned Behavior (TPB)

In het gedragsmodel van Ajzen (1991) de Theorie of Planned Behavior (TPB), wordt ervan uit gegaan dat het menselijk gedrag te verklaren is vanuit de intentie die een persoon heeft om een bepaald gedrag ook daadwerkelijk te tonen (Ajzen,1991; Dhakal, 2018; Häussinger,2015).

Bij 'intentie' gaat het om de persoonlijke houding of mening die iemand heeft om bepaald gedrag te tonen. Deze intentie betekent echter niet dat dit gedrag daadwerkelijk plaatsvindt. Individueel getoond gedrag wordt namelijk ook beïnvloed door de opvattingen van andere personen en de wens om bij een bepaalde groep te horen. Het overschatten van de groepsdruk en de wens om bij een bepaalde groep te willen horen kan weer leiden tot een verkeerde inschatting van het werkelijk door een individu vertoond gedrag. Hierdoor kunnen de verwachtingen niet in overeenstemming zijn met de werkelijkheid.

Het TPB heeft daardoor beperkte interventiemogelijkheden en is niet holistisch, omdat het model zich voornamelijk richt op individuele overtuigingen en niet op kennisvergroting en ook geen rekening houdt met onverwachte gebeurtenissen (de 'grijze en zwarte zwanen'), die een grote invloed hebben op het gedrag van mensen (Parsons et al. 2017; Taleb, 2008).

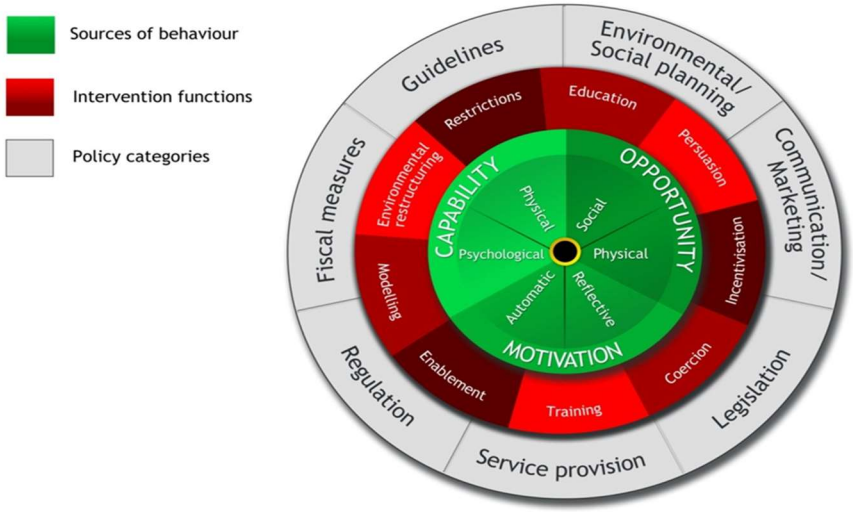
2.5.4 De Capability, Opportunity, Motivation behavior (COM-B) model

In tegenstelling tot de voorgaande drie modellen, geeft het Capability, Opportunity, Motivation Behaviour gedragsmodel (COM-B) inzicht in de wisselwerking tussen de risicoperceptie van een individu en de mate van diens risicotolerantie. Het COM-B model vormt de kern van de door Michie et al. (2011) ontwikkelde BCW, de "Behavior Change Wheel" (zie paragraaf 2.2.5) . Het COM-B model richt zich op de interactie tussen variabelen: "Capability", i.e. de vaardigheden die nodig zijn om een bepaald gedrag uit te kunnen voeren; "Opportunity", i.e. de omgevingsfactoren die het gedrag van een individu beïnvloeden en; "Motivation" i.e. de intrinsieke factoren die het gedrag van een individu beïnvloeden. Tezamen zorgen deze drie variabelen voor een breder inzicht in het gedrag van een

individu. Door ook de interactie tussen de drie variabelen op het menselijk gedrag te bestuderen, houdt de COM-B rekening met de complexiteit van het menselijk gedrag.

2.6 Behavior Change Wheel (BCW)

Het Behaviour Change Wheel (BCW) model (Michie et al. 2011) is een model dat zowel de factoren probeert vast te leggen die gedrag beïnvloeden (het COM-B model), als negen verschillende soorten interventies die kunnen worden gebruikt om gedrag te veranderen (zie ook figuur 2.3, de "rode ring"). Elke interventiefunctie heeft het vermogen om een of meer van de onderliggende gedragsfactoren (COM) te beïnvloeden. Deze interventiefuncties zijn geschikt voor zowel kleinschalige als individuele gedragsveranderingen, of kunnen worden toegepast bij grotere populaties. Het gaat om de volgende interventiefuncties:



Figuur 2.3 Het gedragsmodel Behaviour Change Wheel BCW (Michie et al., 2011)

- *Onderwijs* heeft het vermogen om de psychologische en fysieke mogelijkheden en de motovatie van een individu tot gedragsverandering te vergroten
- *Overtuiging,* heeft het vermogen om de automatische en reflectieve motivatie van een individu tot gedragsverandering te vergroten
- *Training* heeft het vermogen om het fysieke en psychologische vermogen van een individu, zijn fysieke mogelijkheden en de motivatie van een individu tot gedragsverandering te vergroten.
- *Beperking* heeft het vermogen om de fysieke en sociale mogelijkheden van een individu tot gedragsverandering te wijzigen.

- *Omgevingsherstructurering* heeft het vermogen om de fysieke en sociale kansen van een individu te wijzigen, evenals haar/zijn automatische motivatie.
- *Dwang* heeft het vermogen om de automatische en reflectieve motivatie van een individu tot gedragsverandering te vergroten.
- *Modellering* heeft het vermogen om de automatische en reflectieve motivatie van een individu tot gedragsverandering te vergroten, evenals hun sociale kansen
- *Enablement* heeft het vermogen om fysieke en psychologische capaciteiten, fysieke en sociale kansen en de automatische motivatie van een individu tot gedragsverandering te vergroten.
- *Stimulering* heeft het vermogen om de automatische en reflectieve motivatie van een individu tot gedragsverandering te vergroten.

Elk van de negen interventiefuncties speelt een rol bij het ontwerpen van een gedragsveranderingsinterventie. Het derde deel van het BCW-model wordt in figuur 2.3 weergegeven als de grijze buitenste ring van de cirkel. Dit deel bestaat uit zeven beleidscategorieën die kunnen worden gebruikt om interventies mogelijk te maken die gedrag beïnvloeden. Hoewel deze beleidscategorieën misschien zijn ontworpen met nationaal beleid in het achterhoofd, kunnen ze ook van groot nut zijn bij het ondersteunen van gedragsverandering op organisatieniveau.

2.7 Een cyclisch leerproces tot het bevorderen van de informatieveiligheid

In paragraaf 2.1 is toegelicht dat het voor de (informatie)veiligheid van een organisatie van belang is dat deze beschikt over een voldoende niveau van weerbaarheid, wendbaarheid en veerbaarheid. Die mede bepaald is door de medewerkers (Van Der Kleij & Leukfeldt, 2019) Dit vereist het continu bevorderen van de (informatie)veiligheid in een cyclisch proces van Anticiperen, Monitoren, Leren en Aanpassen of Verbeteren.

Door Van Der Kleij en Leukfeldt (2019) is dit cyclische leerproces van het bevorderen van de (informatie)veiligheid in een conceptueel raamwerk geïntegreerd met de drie variabelen van het COM-B model (zie tabel 2.2). Dit raamwerk kan dienen als hulpmiddel voor de ontwikkeling van gedragsinterventieprogramma's en zich op deze wijze beter voor te bereiden op mogelijke cyberdreigingen.

Tabel 2.0.1 Conceptueel raamwerk voor gedragsinterventie (Van Der Kleij en Leukfeldt, 2019)

Leercyclus	Capability (Kennis)	Opportunity (Omgeving)	Motivation (Motivatie)
Anticiperen	Weten wat te verwachten	Middelen hebben om toekomstige ontwikkelingen te verkennen	Bereid om te zoeken naar potentiële verstoringen, nieuwe eisen of beperkingen, nieuwe kansen, of veranderende bedrijfsomstandigheden
Monitoren	Weten wat te zoeken	Middelen hebben om de externe omgeving maar ook de eigen organisatie te monitoren	Bereid om te monitoren wat mogelijk ernstige gevolgen op de korte termijn kan hebben voor de informatieveiligheid
Leren	Weten wat te doen	Middelen hebben om de voorbereide acties uit te voeren	Bereid om te reageren regelmatige en onregelmatige veranderingen, storingen en kansen
Aanpassen en verbeteren	Weten wat er gebeurd is	Middelen hebben om te leren van de opgedane ervaringen	Bereid om te leren van opgedane ervaringen

Antwoord op deelvraag 1 van het onderzoek

Op basis van de uitgevoerde literatuurstudie werd duidelijk dat met behulp van de Human Aspects of Information Security Questionnaire (HAIS-Q) het informatieveiligheidsgedrag van medewerkers in een organisatie kan worden gemeten en geclassificeerd. De literatuurstudie maakte ook duidelijk dat er weliswaar diverse gedragsmodellen zijn ontwikkeld voor het bestuderen van gedragsveranderingen in organisaties, maar dat het Capability, Opportunity, Motivation Behaviour (COM-B) model het beste aansluit op de HAIS-Q meetmethodiek. Tenslotte blijkt het evidence-based Behaviour Change Wheel (BCW) model en het door Van Der Kleij & Leukfeldt (2019) ontwikkelde conceptuele raamwerk voor gedragsinterventie voldoende aanknopingspunten te bieden om als basis te dienen voor het uitwerken van interventies ter bevordering van het informatieveiligheidsgedrag in organisaties. Hierbij zijn de variabelen kennis (capability), omgeving (opportunity), houding (Motivation) en gedrag (behaviour) te gebruiken voor de wendbaarheid, weerbaarheid van de medewerker om veerkrachtig te kunnen reageren op een informatieveiligheid incident.

In het volgende derde hoofdstuk is de tweede deelvraag beantwoord vanuit het veldonderzoek.

H3: Veldonderzoek

In dit hoofdstuk wordt de tweede deelvraag van dit onderzoek beantwoord:

Wat zijn de resultaten van een 0-meting en analyse van het informatieveiligheidsgedrag van medewerkers werkzaam bij Veiligheidsregio Limburg-Noord?

De structuur van dit hoofdstuk is als volgt. In paragraaf 3.1 wordt de aanpak en onderbouwing van de uitgevoerde 0-meting uiteengezet. Paragraaf 3.2 geeft een toelichting op de doorgevoerde aanpassingen in en aanvullingen op de oorspronkelijke HAIS-Q vragenlijst. In pararagraaf 3.3. een verdere validatie en in paragraaf 3.4. zijn de resultaten van de 0-meting opgenomen. Een analyse van de in paragraaf 3.5. Het hoofdstuk sluit af met een antwoord op de tweede deelvraag van dit onderzoek in paragraaf 3.6.

3.1 Aanpak en onderbouwing van de uitgevoerde 0-meting bij VRLN

De uitgevoerde 0-meting betreft een enkelvoudige geclusterde steekproef waarbij alleen de populatie bestaande uit werknemers van de organisatie die toegang tot de intranet pagina (digitale interne mededelingen site) hebben, ook toegang tot de enquête kregen. De 0-meting is uitgevoerd in de derde helft van het jaar 2022 en de enquête is verstuurd naar ongeveer achthonderd potentiële respondenten.

Voorafgaande aan de feitelijke 0-meting zijn er semigestructureerde interviews uitgevoerd. Doel van de interviews was om de validiteit en betrouwbaarheid van de enquête als meetinstrument te valideren en bij te dragen aan het verzamelen van interventiemogelijkheden voor het eigen gedrag van medewerkers in de organisatie. Op basis van de gehouden interviews heeft aan aanpassing plaatsgevonden van de HAIS-Q vragenlijst (zie paragraaf 3.2).

Voor het verzamelen van kwantitatieve gegevens is gebruik gemaakt van de wetenschappelijk gevalideerde HAIS-Q vragenlijst. Deze vragenlijst is zoals verder toegelicht in paragraaf 3.2, op een beperkt aantal onderdelen aangepast.

De aangepaste HAIS-Q vragenlijst bestaat uit 69 vraagstellingen, waarbij een likertschaal van zeven is toegepast: van helemaal mee eens, meestal mee eens, beetje eens, neutraal, beetje oneens, meestal oneens en helemaal oneens. De ordinale data zijn omgezet naar een somscore door een systematische analyse van gradaties in procenten naar demografie, aandachtsgebieden en variabelen. De maximale somscore bestaat uit per vraagstelling de maximale score van de likertschaal ‘7’ x de gevalideerde respondenten x ‘69’ vraagstellingen. Hierbij zijn de gespiegelde vragen negatief omgescoord, zodat de vragen op eenzelfde manier te meten en waarderen zijn. Daardoor is een

effectievere kwantitatieve informatie te verkrijgen voor stuurmogelijkheden, waarbij hoe hoger de score, hoe beter het informatieveiligheidsgedrag. Hierin is groen 'er is aandacht' > 75%, oranje 'nog aandacht nodig' 51-76% en rood 'heeft aandacht nodig'< 50%. Het geheel kenmerkend als een serie gesloten vragen met een serie antwoordalternatieven waaruit de respondent kan kiezen (Verschuren & Doorewaard,2021). De enquêtes zijn ingevoerd in Microsoft Forms en indien nodig omgezet in Excel voor de analyse en verdere classificatie. Voordat de pilot als steekproef is afgenomen zijn twee willekeurige respondenten benaderd om de constructvalidatie en de inclusie- en exclusie criteria tijdsbesteding te valideren van 15-30 minuten, in overeenstemming met eerder onderzoek van Parsons et al. (2017).

Tijdens het openstellen van de enquête in het vierde kwartaal voor de pilot groep heeft een willekeurige focusgroep (die de 1e enquête ingevuld hebben) een interview met drie open vragen voor een verdere construct- en betrouwbaarheidsvalidatie van de HAIS-Q ontvangen. De pilotgroep voor de steekproef is ook gebruikt voor de validatie en om inzicht te krijgen in de IST-situatie van de organisatie.

De constructvalidatie is volgens van Aken en Berends (2018) te krijgen door de resultaten van de enquête te vergelijken met eerder onderzoek en door te testen. Dit is gedaan vanuit eerdere onderzoeken van McCormac et al. (2016), Parsons et al. (2017) en aanpassingen van Verbeek (2021).

Tabel 3.1 Consistentie Cronbach's Alpha (Van Heijst,2021)

Cronbach's alpha	Internal consistency
$\alpha \geq 0.9$	Excellent
$0.9 > \alpha \geq 0.8$	Good
$0.8 > \alpha \geq 0.7$	Acceptable
$0.7 > \alpha \geq 0.6$	Questionable
$0.6 > \alpha \geq 0.5$	Poor
$0.5 > \alpha$	Unacceptable

Door het berekenen van de Cronbach's Alpha voor de variabelen en de aandachtsgebieden. Een methodiek om de interne consistentie (of mate van samenhang) te berekenen tussen meerdere enquêtevragen en te vergelijken. De betrouwbaarheidsscore is beoordeeld volgens Tabel 3.1 afkomstig van Van Heijst (2021).

Daarnaast is van de HAIS-Q de correlatiecoëfficiënt(r) berekend, waarbij deze aangeeft hoe sterk het verband (de effectgrootte) is tussen 2 variabelen. De waarde van r kan variëren van -1 (negatief) tot +1 (positief), waarbij een correlatie van 0 aangeeft dat er geen verband bestaat tussen de variabelen en hoe dichter bij de 1 (of -1), hoe sterker het verband is. Bij een correlatietoets wordt geen onderscheid gemaakt tussen een afhankelijke en onafhankelijke variabele. De variabelen zijn onderling verwisselbaar en er is geen sprake van causaliteit. Als een correlatie is wil dit niet zeggen dat het ene kenmerk het andere veroorzaakt. Alleen kan geconcludeerd worden dat de variabelen samen optrekken of juist tegengesteld zijn aan elkaar. De indeling van Cohen (2003) is hierbij aangehouden. Hierbij is een *r* -waarde (Correlatie) van 0,1=zwak, =>0,3=medium en =>0,5=is sterk.

Voordat de pilot als steekproef is afgenomen zijn twee willekeurige respondenten benaderd om de constructvalidatie en de enquête-tijdsbesteding te valideren van 20-25 minuten, in overeenstemming met eerder onderzoek van Parsons et al. (2017).

In lijn met dat onderzoek is de betrouwbaarheidsvalidatie getoetst bij een willekeurige groep respondenten, zijnde medewerkers van de organisatie (Van Aken en Berends,2018; Verschuren & Doorewaard,2021). Daarnaast is deze gebruikt voor inzicht in het informatieveiligheidsgedrag bij de case-organisatie.

3.2 Een aanpassing van de HAIS-Q vragenlijst

Zoals eerder in hoofdstuk 1 en in paragraaf 3.1. toegelicht, heeft er voorafgaande aan de 0-meting met de HAIS-Q vragenlijst, een validatie van de vragenlijst plaatsgehad op construct en toepasbaarheid van de vragenlijst. Deze validatie heeft geleid tot de volgende aanpassingen in de vragenlijst:

- Een toevoeging van een welkomsttekst om meer context aan de HAIS-Q te geven.
- Een gesloten ethische vraag voor toestemming die verplicht met 'ja' is te beantwoorden om door te mogen gaan:

  Vraag 1 : Ik geef toestemming om de gegevens anoniem te gebruiken (Ethiek)
- De tekst in de enquête is compacter uitgeschreven voor een betere leesbaarheid en positieve beschermingsintenties van medewerkers met behoud van de context **(In groen aangegeven)**
- Het onderdeel 'Het plaatsen van verwijderbare media' aandachtsgebied informatieverwerking is niet meegenomen omdat deze technisch ingeregeld is (rood doorgestreept).
- Het onderdeel 'Privacygevoelige gegevens verzamelingen buiten de applicaties is verwijderd, omdat het met het aandachtsgebied informatieverwerking overlapt (rood doorgestreept).

Verder is de HAIS-Q vragenlijst aangevuld met de volgende demografische en interventievragen:

Vraag 25: Over welk onderwerp van informatieveiligheidsgedrag wil je meer weten? (interventie). Met zeven keuzemogelijkheden waaruit maximaal twee keuzes zijn.

Vraag 26: Om het gedrag over informatieveiligheid te vergroten, willen we verschillende communicatiemiddelen inzetten. Op welke manier wil jij deze graag ontvangen? (interventie). Met acht keuzemogelijkheden waaruit maximaal twee keuzes zijn.

Vraag 27: Betrokkenheid van de afdeling bij informatieveiligheid. (interventie) met vier keuzemogelijkheden waaruit maximaal één keuze is.

Vraag 28: Bij welke afdeling ben je werkzaam? Keuze uit de vier afdelingen.

Vraag 29: Tot welke leeftijdscategorie behoor je? 4 categorieën in stappen van 10 jaar, waarbij de laatste > 60 jaar is

Vraag 30: Hoelang ben je werkzaam voor de VRLN? (Open vraag)

Vraag 31: Heb je naar aanleiding van deze vragen, opmerkingen of suggesties? (Open vraag)

De aangepaste HAIS-Q vragenlijst is opgenomen in Bijlage B van dit afstudeerrapport.

3.3 Een verdere validatie van de aangepaste HAIS-Q vragenlijst

Voor de verdere validatie van de aangepaste HAIS-Q vragenlijst zijn tijdens de enquête vijf willekeurige respondenten benaderd met drie aanvullende vragen. Drie van de respondenten hebben hierop gereageerd. Onderstaand zijn de vragen en de reacties weergegeven:

Vragen	Reactie
Waren de vragen niet te complex?	• Pittige vragen • Sommige vragen herhalen zich
Wat vond je van de lengte/duur van de enquête?	• Lengte van de enquête goed tot best lang
Welke vraag is bij je blijven hangen?	• Authenticatiemiddelen: registratie wachtwoorden • Privacy: Het afdrukken van gevoelige documenten • Social media gebruik: social media

De validatie van de aangepaste vragenlijst is ook onderzocht door gebruik te maken van eerdere analyses in andere onderzoeken van de HAIS-Q en zijn deze onderling vergeleken (Parsons et al., 2017; McCormac et al., 2016; Verbeek, 2021). De resultaten van dit vergelijkend onderzoek zijn weergegeven in Tabel 3.2.

Tabel 3.2 Resultaat Cronbach's Alpha HAIS-Q, Aandachtsgebieden en variabelen van onderzoeker

Diverse onderzoeken Cronbach's alfa scores	**von der Haar (2022)**	**McCormac et al. (2016) T1 en T2 groep**		**Parsons et al. (2017)**	**Wissen (2017)**	**Verbeek (2021)**	
Deelnemers	75	197		505	58	42	
Aandachtsgebieden							
Wachtwoord management	0,87	0,83	0,84	0,82	0,60	0,679	
Email gebruik	0,83	0,77	0,81	0,78	0,70	0,602	
Internetgebruik	0,95	0,79	0,80	0,78	0,69	0,698	
Social media gebruik	0,79	0,75	0,78	0,75	0,70	0,621	
Mobiele apparaten	0,89	0,83	0,82	0,71	0,69	0,556	
Informatieverwerking	0,84	0,76	0,79	0,79	0,59	0,679	
Melden van incidenten	0,85	0,78	0,78	0,79	0,66	0,832	
Privacy	0,85	-	-	-	-	0,676	
Totaalscore	0,84	0,79	0,80	0,77	0,66	0,66	

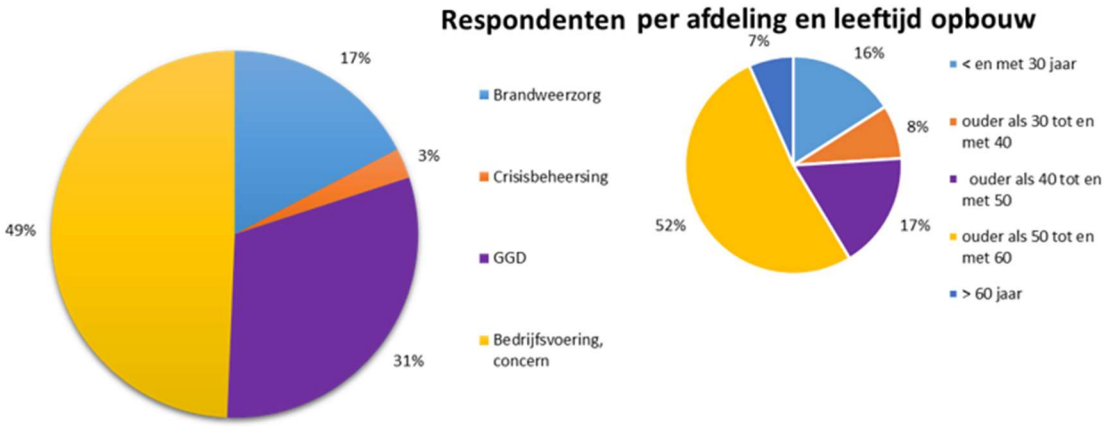
Dimensies	**von der Haar (2022)**	**Verbeek (2021)**	**McCormac et al. (2016) T1 en T2 groep**		**Schaeken (2018)**
Kennis	0,85	0,808	0,84	0,86	0,77
Houding	0,85	0,765	0,93	0,92	0,73
Gedrag (Risico-eigenaarschap)	0,83	0,733	0,90	0,91	0,72
Totaal gemiddeld	0,84	0,77	0,89	0,90	0,74

Voor de verdere constructvalidatie is de Pearson Correlatie berekend als een productmomentcorrelatie of de drie belangrijkste constructen in relatie zijn. Het HAIS-Q construct is aangetoond doordat de kernvariabelen significant correleerden bij 0,3 en hoger:

a) Gedrag versus houding heeft een waarde 0,64 sterk
b) Gedrag versus kennis heeft een waarde 0,55 sterk
c) Houding versus kennis heeft een waarde 0,45 matig

3.4 Het resultaat van de 0-meting met de aangepaste HAIS-Q vragenlijst

De 636 via het intranet verzonden vragenlijsten hebben 80 reacties opgeleverd, waarvan 75 valide ingevulde vragenlijsten. Vijf respondenten voldeden namelijk niet aan de inclusie- en exclusie criteria van een tijdsbesteding van 15-30 minuten. Dit betekent een respons van 11,8%.
Bijna de helft (49%) van de respondenten is werkzaam bij bedrijfsvoering/concern. Ook valt op dat de leeftijdsgroep 'tussen de 50 tot en met 60 jaar' de meeste respons heeft opgeleverd (52%) (Figuur 3.1).



Figuur 3.1 Resultaat respondenten per afdeling en leeftijd opbouw

De resultaten van de enquête zijn opgenomen in Tabel 3.4 en zijn per aandachtsgebied, vraagstelling en de variabelen kennis, houding en gedrag weergegeven.
Het maximaal per vraagstelling te behalen punten vanuit de likertschaal is 7. Voor de 75 respondenten tezamen is dat per vraagstelling: 7 x 75 = 525 punten. In Tabel 3.4 is het resultaat van elke vraagstelling als een percentage van het per vraagstelling maximaal te behalen aantal punten weergegeven en is afgerond op een heel getal.
De maximale mogelijk te behalen totaalscore over alle stellingen is:
525 punten x 69 vraagstellingen = 36225 punten. Het resultaat van de 0-meting voor alle vragen tezamen levert een somscore op van 77% ten opzichte van de maximaal haalbare totaalscore.

In tabel 3.3 is vanuit de aandachtsgebieden en variabelen het aantal vraagstellingen weergegeven per score 'aandacht' en vanuit gemiddelde score voor aandacht van het totaal. Aan de onderzijde is de legenda voor de waarde in % voor aandacht weergegeven.

Tabel 3.3 Resultaat vraagstelling per aandachtsgebied en variabelen

Aandachtsgebied	Voldoende aandacht	Nog aandacht nodig	Heeft aandacht nodig	Gemiddelde score
authenticatiemiddelen	5	3	1	71%
E- mail gebruik	3	4	2	67%
Internet gebruik	4	5	0	77%
Social media	8	0	1	81%
Gebruik van mobiele apparatuur	8	1	0	83%
Informatieverwerking	5	1	0	82%
Incidenten management	4	8	0	74%
Privacy	5	1	0	85%
Variabelen	42	23	4	Aantal vragen
Gedrag	**13**	**7**	**3**	76%
Houding	**17**	**6**	**0**	80%
Kennis	**12**	**10**	**1**	75%
Totaal aantal stellingsvragen	42	23	4	77%
Waarde in % voor aandacht				
Voldoende aandacht	>75%			
Nog aandacht nodig	51-76%			
Heeft aandacht nodig	<50%			

Vier vraagstellingen vanuit drie aandachtsgebieden scoren minder dan 50%. Drie vraagstellingen hebben betrekking op "Gedrag" en de vraagstelling "Ik mag op links in e-mails klikken van mensen die ik ken" heeft betrekking op "Kennis". Dit zijn de vraagstellingen die minder dan 50% scoren:

- Aandachtsgebied "Authenticatiemiddelen" (47%):
  Ik registreer mijn wachtwoorden alleen in een wachtwoordenkluis en niet op een andere wijze
- Aandachtsgebied "E-mail gebruik" (49%):
  Ik klik niet op links in e-mails ook al zijn deze van mensen die ik ken
- Aandachtsgebied "E-mail gebruik" (48%):
  Ik mag op links in e-mails klikken van mensen die ik ken
- Aandachtsgebied "Social media" (42%):
  Ik bekijk mijn social media privacy instellingen regelmatig

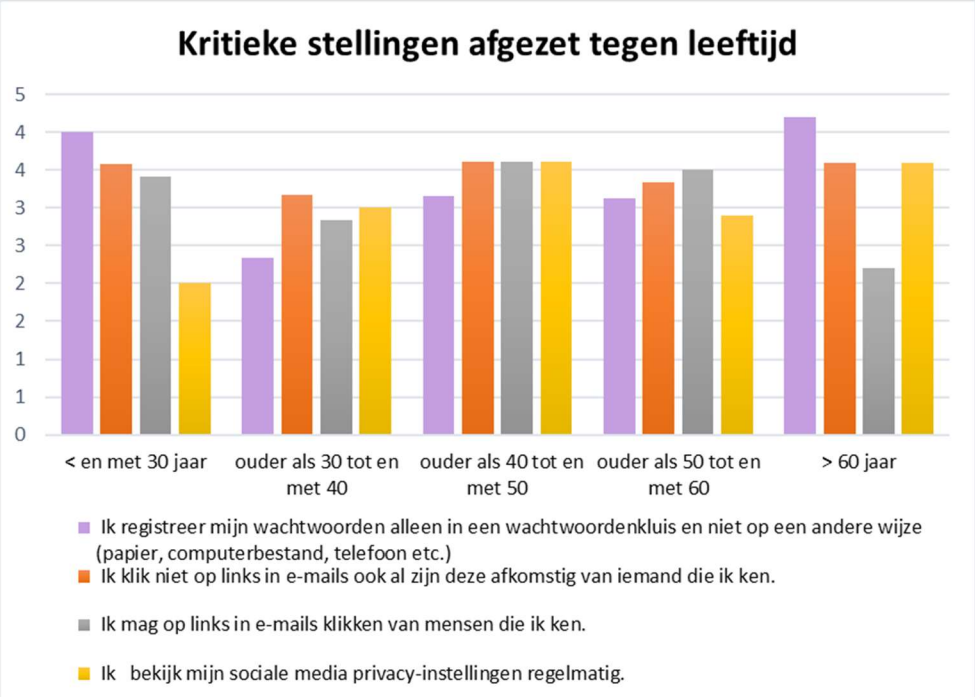
Deze vier vraagstellingen zijn in Tabel 3.3 en Tabel 3.4 in "rood" aangegeven en hebben verdere aandacht nodig.

Tabel 3.4 Resultaat 0-meting VRLN november 2022

	Aandachtsgebied	Subgebied	Stellingen	Type vraag	Score*likert *omkeer	
2	Authenticatiemiddelen	Wachtwoorden	Ik gebruik verschillende wachtwoorden voor mijn	Gedrag	304	58%
3	Authenticatiemiddelen	Wachtwoorden	Het is veilig om hetzelfde wachtwoord voor mijn privé (sociale media-accounts) en werkaccounts te	Houding	438	83%
4	Authenticatiemiddelen	Wachtwoorden	Ik mag mijn privé (social media) wachtwoord	Kennis	419	80%
5	Authenticatiemiddelen	Delen van autothenticatiemiddelen	Ik deel mijn wachtwoord (of ander	Gedrag	414	79%
6	Authenticatiemiddelen	Delen van autothenticatiemiddelen	Het is een slecht idee om mijn wachtwoorden (of andere authenticatiemiddelen zoals pasje) te	Houding	457	87%
7	Authenticatiemiddelen	Delen van autothenticatiemiddelen	Ik mag mijn wachtwoorden (of andere	Kennis	435	83%
8	Authenticatiemiddelen	Registratie wachtwoorden	Ik registreer mijn wachtwoorden alleen in een wachtwoordenkluis en niet op een andere wijze	Gedrag	246	47%
9	Authenticatiemiddelen	Registratie wachtwoorden	Ik ben van mening dat ik mijn wachtwoorden veilig kan registreren, ook zonder het gebruik van een	Houding	316	60%
10	Authenticatiemiddelen	Registratie wachtwoorden	Ik mag wachtwoorden registreren in een boekje of Excel bestand, als dit op een veilige manier kan,	Kennis	340	66%
11	E- mail gebruik	Klikken op e-mails van bekende	Ik klik niet op links in e-mails ook al zijn deze	Gedrag	257	49%
12	E- mail gebruik	Klikken op e-mails van bekende	Het is veilig om op links te klikken in e-mails van	Houding	301	57%
13	E- mail gebruik	Klikken op e-mails van bekende	Ik mag op links in e-mails klikken van mensen die	Kennis	253	48%
14	E- mail gebruik	Klikken op e-mails van onbekende	Als een e-mail van een onbekende afzender	Gedrag	428	82%
15	E- mail gebruik	Klikken op e-mails van onbekende	Er kan niets slechts gebeuren als ik op een link in	Houding	452	86%
16	E- mail gebruik	Klikken op e-mails van onbekende	Ik mag op een link in een e-mail van een	Kennis	316	60%
17	E- mail gebruik	Openen van bijlagen in e-mails van	Ik open e-mailbijlagen als de afzender mij	Gedrag	375	71%
18	E- mail gebruik	Openen van bijlagen in e-mails van	Het is riskant om een e-mailbijlage van een	Houding	452	86%
19	E- mail gebruik	Openen van bijlagen in e-mails van	Ik mag e-mailbijlagen van onbekende afzenders	Kennis	351	67%
20	Internet gebruik	Downloaden van bestanden	Ik download alleen bestanden op mijn	Gedrag	467	89%
21	Internet gebruik	Downloaden van bestanden	Het kan riskant zijn om bestanden op mijn	Houding	396	75%
22	Internet gebruik	Downloaden van bestanden	Alle soorten bestanden mag ik downloaden op	Kennis	358	68%
23	Internet gebruik	Benaderen van dubieuze websites	Als ik op het werk toegang heb tot het internet, bezoek ik elke website die ik wil bezoeken, want	Gedrag	391	74%
24	Internet gebruik	Benaderen van dubieuze websites	Ook al heb ik toegang tot een website op het werk,	Houding	444	85%
25	Internet gebruik	Benaderen van dubieuze websites	Terwijl ik aan het werk ben mag ik alle websites	Kennis	342	65%
26	Internet gebruik	Informatie online invoeren	Ik beoordeel de veiligheid van websites en het soort gevraagde informatie, alvorens deze	Gedrag	416	79%
27	Internet gebruik	Informatie online invoeren	Als het mij helpt om mijn werk te doen, maakt het	Houding	416	79%
28	Internet gebruik	Informatie online invoeren	Ik mag alle soorten informatie op een website	Kennis	396	75%
29	Social media	Social Media privacy-instellingen	Ik bekijk mijn sociale media privacy-instellingen	Gedrag	220	42%
30	Social media	Social Media privacy-instellingen	Het is goed om privacy-instellingen op social	Houding	436	83%
31	Social media	Social Media privacy-instellingen	Ik moet regelmatig de privacy-instellingen op mijn	Kennis	399	76%
32	Social media	Rekening houden met gevolgen	Ik plaats niets op sociale media wat (negatieve)	Gedrag	500	95%
33	Social media	Rekening houden met gevolgen	Op sociale media kan ik ook zaken plaatsen die ik	Houding	438	83%
34	Social media	Rekening houden met gevolgen	Ik kan niet ontslagen worden voor iets wat ik op sociale media plaats.	Kennis	427	81%
35	Social media	Plaatsen van informatie over werk	Ik plaats alles wat ik wil over mijn werk op sociale	Gedrag	484	92%
36	Social media	Plaatsen van informatie over werk	Het is riskant om bepaalde informatie over mijn	Houding	465	89%
37	Social media	Plaatsen van informatie over werk	Ik mag posten wat ik wil over mijn werk op sociale	Kennis	469	89%
38	Gebruik van mobiele	Fysieke beveiliging van mobiele	Als ik in een openbare ruimte werk, laat ik mijn	Gedrag	355	68%
39	Gebruik van mobiele apparatuur	Fysieke beveiliging van mobiele apparaten	Als ik in een openbare ruimte werk, kan ik mijn laptop en/of telefoon op tafel laten liggen terwijl ik	Houding	400	76%
40	Gebruik van mobiele apparatuur	Fysieke beveiliging van mobiele apparaten	Als ik in een openbare ruimte werk, moet ik mijn mobiele apparatuur altijd bij me houden.	Kennis	423	81%
41	Gebruik van mobiele apparatuur	Versturen van privacygevoelige informatie via wifi	Ik verstuur privacy gevoelige werkbestanden of mails via een openbaar WIFI-netwerk.	Gedrag	401	76%
42	Gebruik van mobiele apparatuur	Versturen van privacygevoelige informatie via wifi	Het is riskant om privacygevoelige werkbestanden of mails te versturen via een openbaar WIFI-	Houding	461	88%
43	Gebruik van mobiele apparatuur	Versturen van privacygevoelige informatie via wifi	Ik mag privacygevoelige werkbestanden of mails versturen via een openbaar WIFI-netwerk.	Kennis	402	77%
44	Gebruik van mobiele	Meekijken door onbevoegden.	Ik zorg dat onbevoegden niet kunnen meekijken	Gedrag	486	93%
45	Gebruik van mobiele	Meekijken door onbevoegden.	Het is riskant om gevoelige werkbestanden of	Houding	490	93%
46	Gebruik van mobiele	Meekijken door onbevoegden.	Als ik aan een gevoelig document werk, zorg ik	Kennis	492	94%
47	Informatieverwerking	Het weggooien van gevoelige afdrukken	Wanneer gevoelige afdrukken moeten worden weggegooid, zorg ik ervoor dat ze versnipperd of	Gedrag	450	86%
48	Informatieverwerking	Het weggooien van gevoelige afdrukken	Het weggooien van gevoelige afdrukken bij gewoon afval is veilig.	Houding	466	89%
49	Informatieverwerking	Het weggooien van gevoelige afdrukken	Gevoelige afdrukken mogen op dezelfde manier worden weggegooid als niet-gevoelige afdrukken.	Kennis	436	83%
50	Informatieverwerking	Achterlaten van gevoelige informatie	Ik laat afdrukken die gevoelige informatie bevatten	Gedrag	390	74%
51	Informatieverwerking	Achterlaten van gevoelige informatie	Het is riskant om afdrukken met gevoelige	Houding	419	80%
52	Informatieverwerking	Achterlaten van gevoelige informatie	Ik mag afdrukken met gevoelige informatie op mijn	Kennis	411	78%
53	Incidenten management	Melden van verdacht gedrag	Als ik iemand verdacht zie handelen op mijn	Gedrag	469	87%
54	Incidenten management	Melden van verdacht gedrag	Ik denk niet dat er iets ergs zal gebeuren als ik	Houding	377	72%
55	Incidenten management	Melden van verdacht gedrag	Als ik iemand zich verdacht zie gedragen op mijn werkplek, moet ik dat melden.	Kennis	430	82%
56	Incidenten management	Negeren van slecht veiligheidsgedrag van collega's	Als ik merk dat mijn collega de veiligheidsregels negeert, attendeer ik hem/haar daarop.	Gedrag	402	77%
57	Incidenten management	Negeren van slecht veiligheidsgedrag	Ik vind het niet mijn verantwoordelijkheid om	Houding	324	62%
58	Incidenten management	Negeren van slecht veiligheidsgedrag	Ik mag niet voorbijgaan aan verkeerd gedrag van	Kennis	398	76%
59	Incidenten management	Melden van alle Incidenten	Als ik een informatieveiligheidsincident zou	Gedrag	494	94%
60	Incidenten management	Melden van alle Incidenten	Het melden van informatieveiligheidsincidenten (incl. datalekken) helpt om de informatieveiligheid	Houding	509	97%
61	Incidenten management	Melden van alle Incidenten	Het is een keuze om informatieveiligheidsincidenten (incl. datalekken)	Kennis	375	71%
62	Incidenten management	Afdrukken van privacygevoelige informatie	Ik druk nooit privacygevoelige informatie af.	Gedrag	284	54%
63	Incidenten management	Afdrukken van privacygevoelige informatie	Voor mijn werk vind ik het gemakkelijker om privacygevoelige informatie af te drukken i.p.v.	Houding	321	61%
64	Incidenten management	Afdrukken van privacygevoelige informatie	Het is niet acceptabel om privacygevoelige informatie af te drukken als het raadplegen digitaal	Kennis	296	56%
65	Privacy	In publieke gelegenheden praten over	Als ik over klanten/cliënten en/of medewerkers	Gedrag	454	86%
66	Privacy	In publieke gelegenheden praten over cliënten en/of medewerkers.	Ik vind het geen goed idee om in een openbare ruimte over klanten/cliënten/medewerkers te	Houding	440	84%
67	Privacy	In publieke gelegenheden praten over cliënten en/of medewerkers.	Ik mag in een openbare ruimte praten over klanten/cliënten of medewerkers zolang het	Kennis	354	67%
68	Privacy	Inzien van persoonsgegevens van	Ik bekijk alleen gegevens wanneer dat nodig is om mijn	Gedrag	494	94%
69	Privacy	Inzien van persoonsgegevens van klanten/cliënten/medewerkers	Ik heb een geheimhoudingsplicht dus ik mag persoonsgegevens van iedereen raadplegen ook	Houding	454	86%
70	Privacy	Inzien van persoonsgegevens van	Ik mag alleen persoonsgegevens raadplegen als	Kennis	492	94%
			Totaal gemiddelde somscore in %			77%

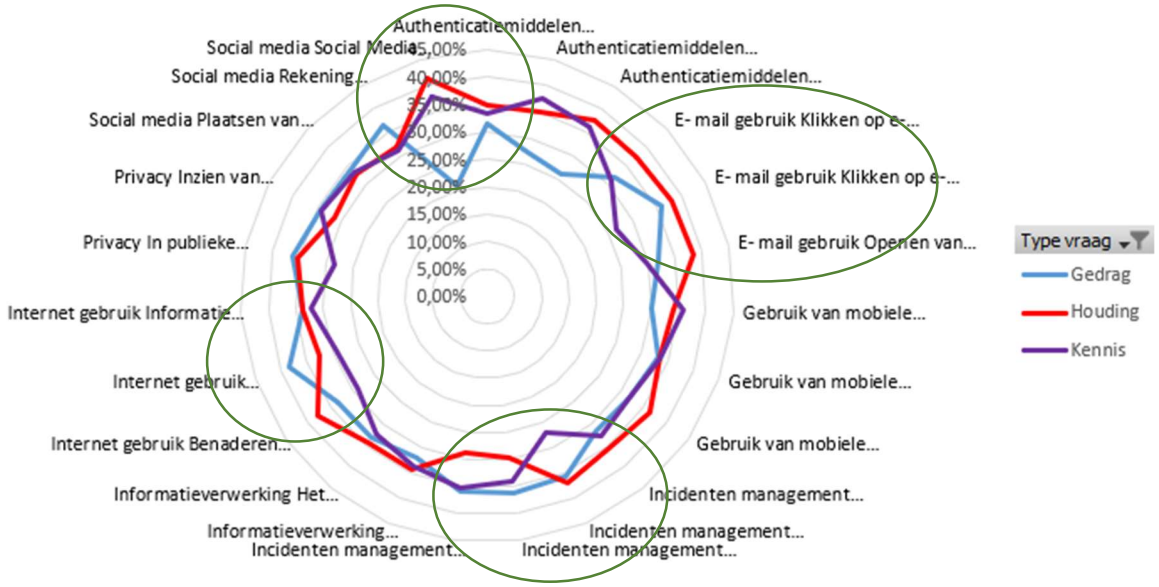
3.5 Analyse van de 0-meting met de aangepaste HAIS-Q vragenlijst

In figuur 3.2 is voor de vier in paragraaf 3.4 gevonden kritieke vraagstellingen (deze vier vraagstellingen scoorden lager dan 50%) de leeftijdsopbouw onder de respondenten nagegaan.
Drie van de kritieke vraagstellingen hebben betrekking op “Gedrag” en een vraagstelling op “Kennis”: ‘ik mag op links in e-mails klikken van mensen die ik ken’. Als we daarbij de resultaten afzetten tegen de leeftijdsgroepen zien we dat de leeftijd groep < 30 jaar de vraagstelling “Ik bekijk mijn sociale media privacy-instellingen regelmatig” duidelijk lager scoren dan de leeftijdsgroepen daar boven. Opvallend is verder dat op de vraagstelling “Ik mag op links in e-mails klikken van mensen die ik ken” duidelijk lager wordt gescoord bij de oudste leeftijdsgroep. Een mogelijke reden hiervoor zou kunnen zijn dat de oudere leeftijdsgroep onvoldoende bekend is met de veiligheidsrisico’s die hiermee samenhangen. Er blijkt dus sprake te zijn van een differentiatie tussen aandachtsgebieden en de demografie van de leeftijdsgroepen.



Figuur 3.2 Resultaat kritieke stellingen versus leeftijd opbouw

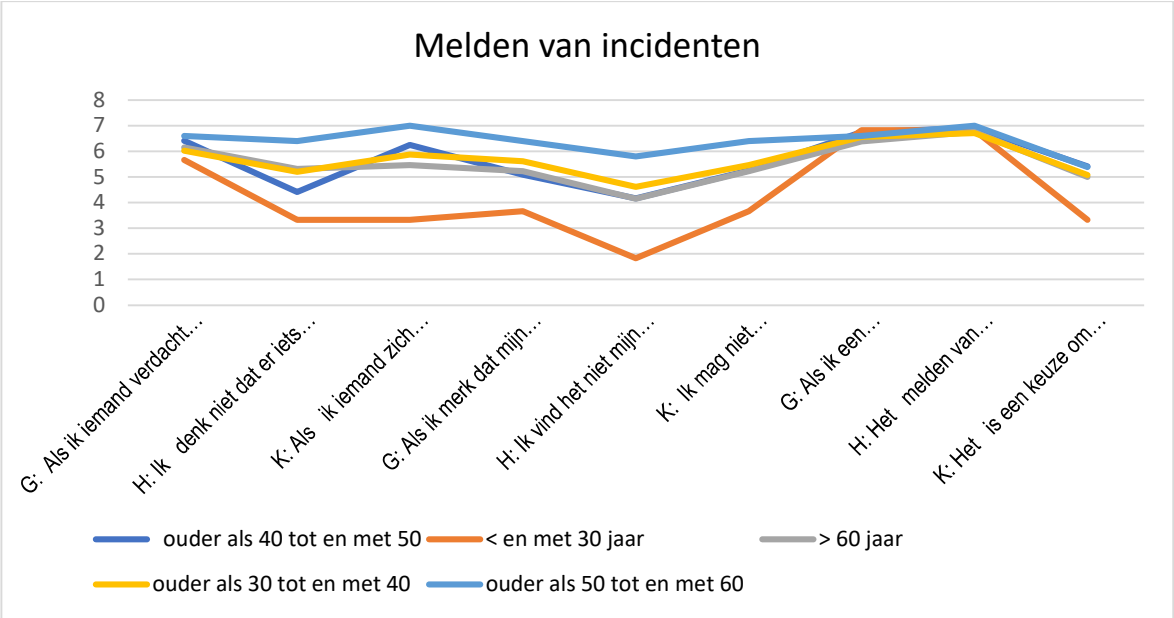
De resultaten van de HAIS-Q zijn vanuit diverse variabelen, aandachtspunten en stellingen te belichten, waardoor een "Simpson paradox"[2] ontstaat, omdat de variabelen nu afzonderlijk of gecombineerd zijn meegenomen. Het totaalresultaat geeft als resultaat dat 'er aandacht is', maar als de aandachtsgebieden afzonderlijk bekijken vanuit de COM-B variabelen is te zien dat de scores op de vraagstellingen onderling verschillen. Die differentiaties en paradox zijn onder andere vanuit de vraagstellingen zichtbaar doordat de lijnen niet alleen onderling maar ook verder uit elkaar staan voor de variabelen. Enkele verschillen aangegeven in de 'groene cirkels' (zie Figuur 3.3).



Figuur 3.3 Resultaat aandachtsgebieden en vraagstellingen

De Pearson correlatie geeft daarbij aan dat de afhankelijkheid tussen kennis en houding matig is. Een reden hiervoor kan de omgeving of de houding zijn 'Ik vind het niet mijn verantwoordelijkheid om collega's aan te spreken als zij slecht veiligheidsgedrag vertonen'. Hierbij is de "Kennis" voldoende bij alle leeftijdsgroepen, maar is de "Houding" vanuit de verschillende leeftijdsgroepen divers. Figuur 3.4 laat het verband en de Simson paradox tussen de variabalen Kennis, Houding, Gedrag en leeftijd zien vanuit het aandachtsgebied 'melden van incidenten', doordat de lijnen verder uit elkaar liggen en verschillen per leeftijd groep. De differentiatie is goed waar te nemen tussen de leeftijd groep < 30 jaar(oranje) en 'ouder als 50 tot en met 60"(lichtblauw) en de (sub)stellingen in Figuur 3.4.

[2] De paradox van Simpson is een fenomeen in de statistiek waarbij een trend waarneembaar is in verschillende groepen van data, maar verdwijnt of omkeert wanneer de groepen worden gecombineerd.



Figuur 3.4 Resultaat per leeftijdsgroep voor aandachtsgebied "Melden van incidenten"

Houding (80%)

Vanuit de HAIS-Q score voor de "Houding" is de score relatief hoog ten opzichte van het "Gedrag" en "Kennis". Dit wil zeggen dat de wil er is om het gewenste gedrag te vertonen. Bij het 'delen van wachtwoorden' en 'openen van bijlagen van onbekende afzenders' scoort deze hoog, waarbij de kennis laag scoort. Hierbij is de houding voor wat betreft de privacy laag bij het 'inzien van persoonlijke gegevens van anderen'.

Kennis (75%)

De "Kennis" van medewerkers op het gebied van informatieveiligheid is relatief laag ten opzichte van houding en gedrag. Met name de kennis over veilig omgaan met informatie is onvoldoende. Dit kan een gevolg zijn van onvoldoende governance en training door de organisatie. Een gebrek aan kennis kan leiden tot onbewust risicovol gedrag, waardoor een mogelijk hoger veiligheidsrisico ontstaat voor de organisatie.

Gedrag (76%)

Het "Gedrag" van medewerkers geeft ruimte voor verbetering. Er zijn enkele gedragingen die als laagste scoren en risicovol zijn, zoals het delen van wachtwoorden, e-mails openen van bekende en het openen van bijlagen van onbekende afzenders. Het is positief dat medewerkers zich bewust zijn van de risico's van sociale media (95%) en hierover verantwoordelijk gedrag vertonen.

De totaalscore van de HAIS-Q kan een indicatie geven van de algemene staat van het gedrag ten aanzien van informatieveiligheid in de organisatie(omgeving) en heeft daarmee een correlatie met de houding, kennis en gedrag van medewerkers.

Aandachtsgebieden

In Tabel 3.5 zijn de acht aandachtsgebieden van de HAIS-Q als werkdefinities (bijlage E) voor het inzichtelijk maken van het informatieveiligheidsgedrag met behulp van de correlatiecoëfficiënt (r) weergegeven, als indicator van de sterkte van het verband tussen de respectievelijke aandachtsgebieden.

Tabel 3.5 Resultaat correlatie tussen aandachtsgebieden

Pearsoncorrelatie tussen de aandachstgebieden

	Authenticatie middelen	*E- mail gebruik*	*Gebruik van mobiele apparatuur*	*Incidenten management*	*Informatiever werking*	*Internet gebruik*	*Privacy*	*Social media*
Authenticatiemiddelen								
E- mail gebruik	,07							
Gebruik van mobiele apparat	,97	,31						
Incidenten management	-,96	,21	-,86					
Informatieverwerking	,67	,79	,83	-,43				
Internet gebruik	-,53	,81	-,31	,74	,28			
Privacy	-,85	,46	-,70	,96	-,18	,90		
Social media	,97	,33	1,00	-,86	,84	-,29	-,69	

Hierbij is te zien dat Authenticatiemiddelen een sterk positief verband (> ,5) heeft met het gebruik van mobiele apparatuur, informatieverwerking en social media. En een sterk negatief verband (>-,5) met incidentmanagement, internet gebruik en privacy. Dit laatste betekent dat hoe minder aandacht er is voor wachtwoordbeleid, des te minder het veilig gebruik van internet en privacy en het melden en aanspreken in geval van veiligheidsincidenten. Het 'Email gebruik' lijkt geen verband te hebben. Dit zien we ook bij informatieverwerking en internetgebruik (,28) en privacy (-,18). Het gebruik van social media neemt toe bij toename van het gebruik van mobiele apparatuur (1). Hierbij geeft het gedrag bij de vraagstelling over social media privacy-instellingen 'Ik bekijk mijn sociale media privacy-instellingen regelmatig' (stelling 29) de laagste score vanuit de respondenten (42%, *heeft aandacht nodig*).

3.6 Antwoord op deelvraag 2 van het onderzoek

De voor dit hoofdstuk te beantwoorden deelvraag luidde: "*Wat zijn de resultaten van een 0-meting en analyse van het informatieveiligheidsgedrag van medewerkers werkzaam bij Veiligheidsregio Limburg-Noord?*".

De uitgevoerde 0-meting en analyse van de resultaten maakt duidelijk dat alle 69 gestelde vraagstellingen over informatieveiligheidsgedrag tezamen een somscore opleverde van 77% van de maximaal haalbare totaalscore voor informatieveiligheidsgedrag. Dit percentage geeft een beeld van het informatieveiligheidsgedrag binnen de acht, in paragraaf 2.4 onderscheiden, aandachtsgebieden

en de drie gedragsvariabelen “Houding”, “Kennis” en “Gedrag”. De score van de 0-meting is een momentopname die plaatsvond in november 2022.

Van de gestelde 69 vraagstellingen zijn er vier die als kritisch kunnen worden gelabeld omdat deze lager scoren dan 50%. Het gaat om één vraagstelling in het aandachtsgebied “Authenticatiemiddelen”: “Ik registreer mijn wachtwoorden alleen in een wachtwoordkluis en niet op andere wijze”; Twee vraagstellingen in het aandachtsgebied “E-mail gebruik”: “Ik klik niet op links in e-mails ook al zijn deze van mensen die ik ken” en “Ik mag op links in e-mails klikken van mensen die ik ken”; en tenslotte het aandachtsgebied “Social media”: de vraagstelling “Ik bekijk mijn social media privacy instellingen regelmatig”.

Uit de uitgevoerde analyse blijkt verder dat de score voor de vier kritieke vraagstellingen demografisch verschillend is voor de vijf onderscheiden leeftijdscategorieën. Zo blijkt uit de resultaten dat de leeftijdsgroep die jonger is dan 30 jaar, in onvoldoende mate de sociale media privacy instellingen te controleren en heeft de leeftijdsgroep van 60 jaar en ouder onvoldoende besef van het potentiële gevaar dat zij lopen bij het openen van een link in e-mails van bekenden. Deze demografische verschillen wijzen op de noodzaak van een gedifferentieerde aanpak bij het bevorderen van het informatieveiligheidsgedrag bij medewerkers in de organisatie. In het volgende hoofdstuk 4 een antwoord op de hoe het informatieveiligheidsgedrag is te bevorderen.

H4: Het bevorderen van het informatieveiligheidsgedrag bij de VRLN

In dit hoofdstuk wordt de derde deelvraag van het onderzoek beantwoord:

Hoe kan, gegeven de uitkomsten van de literatuurstudie en de gehouden 0-meting en analyse, het informatieveiligheidsgedrag in de organisatie worden bevorderd?

In paragraaf 2.5. en 2.6 zijn respectievelijk het door Michie et al. (2011) ontwikkelde COM-B model en de Behaviour Change Wheel (BCW) toegelicht. Het COM-B model en de Behaviour Change Wheel hebben voor Michie et al. (2016) als basis gediend voor het uitwerken van een stapsgewijze methode voor het ontwerpen van gedragsveranderingsinterventies (zie figuur 4.1). Deze methode onderscheidt drie opeenvolgende fasen:

Fase 1: Begrijpen van het gedrag;

Fase 2: Identificeren van interventieopties;

Fase 3: Identificeren van de toe te passen gedragsinterventietechnieken en implementatie opties.

Hoewel de methode door Michie et al. (2016) in lineaire termen wordt beschreven, maken zij duidelijk dat er in de praktijk sprake zal zijn van een itererend proces tussen de drie onderscheiden fasen wanneer zich tijdens de uitvoering bepaalde problemen of obstakels voordoen.

Voorafgaande aan het ontwerp van gedragsinterventies, is het van belang om de criteria te bepalen waar het ontwerp aan zal moeten voldoen. Michie et al. (2016) hebben hiertoe een zestal ontwerpcriteria benoemd die zij met het acroniem APEASE hebben afgekort. Wil een gedragsinterventie succesvol zijn, dan zal deze in ieder geval moeten voldoen aan de criteria van:

- *Acceptability (aanvaardbaarheid):* Een gedragsinterventie is aanvaardbaar voor de medewerkers en andere stakeholders en stelt geen onredelijke eisen.
- *Practicability (uitvoerbaarheid):* Een gedragsinterventie is uitvoerbaar voor zover deze kan worden gerealiseerd met de beschikbare middelen.
- *Effectiveness (effectiviteit):* Een gedragsinterventie is effectief wanneer de vooraf beoogde doelstellingen van de interventie worden bereikt.
- *Affordability (betaalbaarheid):* Een gedragsinterventie is betaalbaar wanneer deze past binnen het budget.
- *Side-effects/ safety (veiligheid):* Een gedragsinterventie is veilig wanneer de toepassing ervan niet leidt tot ongewenste en onbedoelde neveneffecten.
- *Ethical (ethiek):* Een gedragsinterventie moet ethisch verantwoord zijn en niet in strijd zijn met de waarden en normen van de organisatie en de maatschappij.

In dit afstudeeronderzoek wordt uitgegaan van de door Michie et al. (2016) voorgestelde methode voor het ontwerpen van gedragsinterventies. De te volgen stappen in deze methode worden in paragraaf 4.1. tot en met 4.3. nader toegelicht en ingevuld voor het aandachtsgebied “E-mail gebruik”. Dit hoofdstuk sluit af met een antwoord op de gestelde derde deelvraag van dit onderzoek.

Figuur 4.1 Stappenplan voor het ontwerpen van gedragsinterventies

4.1 Fase 1: Begrijpen van het veiligheidsgedrag

In de eerste fase van de aanpak, is het belangrijk om het gedrag te begrijpen. Dit kan bereikt worden door middel van drie stappen:

Stap 1) Definieer het te veranderen gedrag. Om een probleem aan te pakken, moet men zo specifiek mogelijk vaststellen: a) het gedrag dat veranderd moet worden om het (veiligheids)probleem op te lossen; b) waar en wanneer het gedrag zich voordoet; en c) het individu of de specifieke groep die betrokken is bij het gedrag dat veranderd moet worden.

Stap 2) Analyseer de context waarbinnen het gedrag zich voordoet. Waar wordt het gedrag door beïnvloed? Gedragingen bestaan niet in een vacuüm, maar vinden plaats binnen de context van ander gedrag van dezelfde of andere individuen en werken als een systeem op elkaar. Wanneer men een specifiek type gedrag wil veranderen, is het daarom van belang om tijdens het interventie-ontwerp ook het gedrag mee te nemen dat het specifieke type gedrag beïnvloedt.

Stap 3) Specificeer wat er exact veranderd moet worden aan het gedrag. Stel een beschrijving op van wie het gedrag moet vertonen; Wat de persoon of de groep anders moet gaan doen om het gewenste gedrag te vertonen; Wanneer, waar, hoe vaak, en met wie zal het individu of de groep dit doen?

In tabel 4.1 zijn bovenstaande drie stappen voor het beoogde gedrag ten aanzien van het e-mail gebruik binnen de VRLN uitgewerkt.

Een voorbeeld van bovenstaande drie stappen is uitgewerkt voor het aandachtsgebied 'E-mail gebruik' bij VRLN.

Tabel 4.1 Identificatie gedragsverandering voor E-mail gebruik bij VRLN

Wat is het doelgedrag?	Het niet zondermeer openen van bijlagen of 'linkjes' in een E-mail.
Welke bedreigingen zijn er en voor wie?	Onrechtmatig toegang tot gegevens zonder toestemming Onrechtmatig toegang tot inloggegevens of bestanden Continuïteit organisatie Schade claims externe Boete
Wie moet het gedrag uitvoeren?	Alle medewerkers van de VRLN
Wat is het zichtbare resultaat voor het gewenste gedrag?	Controleer de afzender. Gebruik voor het versturen van bestanden, gegevens het technische programma (te denken is 'Zivver) Minder (bijna) informatieveiligheidsincidenten
Wanneer uitvoeren?	Tijdens het werk.
Waar gebruiken/Doen?	Overal waar je werkt.
Hoe vaak?	Bij het ontvangen van een E-mail Bij het openen van E-mail. Bij het versturen van een E-mail.
Met wie?	Alleen als eigen verantwoordelijke
Waarde in doel voor de organisatie als tijdsgebonden?	Risicotolerantie: 75 % van de medewerkers vanaf december 2023.

Stap 4) Inventariseren van wat er moet veranderen. Identificeer wat er moet veranderen in persoon en/of omgeving om het gewenst gedrag te bereiken. Interventieontwerpers moeten hiertoe een gedragsanalyse uitvoeren. Deze analyse kan worden uitgevoerd met behulp van het in hoofdstuk 2 besproken COM-B-model en het ondersteunend gebruik van focusgroepen, vragenlijsten, observaties en/of document analyses. Doel van stap 4 is om te bepalen welke COM-B-componenten moeten veranderen om het beoogde gedrag te laten plaatsvinden.

Een voorbeeld van de invulling van stap 4 is uitgewerkt voor het aandachtsgebied 'E-mail gebruik' bij VRLN.

Tabel 4.2 Identificatie van de beoogde gedragsverandering van het E-mail gedrag bij VRLN

Doelgedrag: medewerkers van de VRLN controleren bijlagen en 'links' in E-mails van (on)bekenden voordat ze die openen.		
Com -B componenten	Wat moet er gebeuren om het doelgedrag te laten optreden?	Is er verandering nodig?
Fysieke mogelijkheden	De fysieke vaardigheden om bijlagen in een E-mail te beoordelen	Geen verandering nodig omdat deze voor handen zijn
Psychologisch vermogen	Kennis hebben van den werkwijze voor het beoordelingen en weten waar die informatie te vinden is.	Kennis nodig over hoe dit te doen.
Kansen fysiek/sociaal	Zorg voor een informatie om te controleren. Constateer dat 'ouderen medewerkers' dit gedrag ook doen.	Verandering nodig om dat niet duidelijk is wat de gevolgen zijn of hoe dit te realiseren is.
Motivatie	Overtuigen/ motiveren dat vaker toepassen van controles de incidenten terugdringt. Zorg dat de routine een automatisme is.	Verandering nodig om de motivatie te bevorderen.
Gedragdiagnose/ com-b component	Psychologische/Technische vermogen	Capaciteit en motivatie motiveren.

4.2 Fase 2: Het identificeren van interventie opties. Beleid en strategie.

Stap 5a) Inventariseren van interventieopties. Het COM-B-model identificeert wat er moet veranderen om het gewenste gedrag te bereiken. Het BCW identificeert interventiefuncties en ondersteunend beleid dat waarschijnlijk effectief zal zijn om de beoogde verandering teweeg te brengen. Door deze twee modellen te combineren ontstaat een interventiestrategie.

In tabel 4.3 zijn op basis van de BCW van Michie et al. (2016) de interventiefuncties en acties uitgewerkt voor het Email gedrag bij VRLN.

Tabel 4.3 Interventie functies en acties t.b.v. beoogde verandering Email gedrag bij VRLN

Interventie functie (rode rand BCW)	Interventie actie
Onderwijs	Leren door kennis en begrip laten toenemen. Te denken is aan het aanbieden van 'verplichte' E-learning, technische inrichting van bijscholing, ervaringen delen.
Overtuiging	Positieve en negatieve intrinsieke motivatie(gevoelens) activeren om tot actie te komen. Te denken is aan het stimuleren door communicatie technieken te gebruiken.
Training/Opleiding	Vaardigheden doceren en bijbrengen. Te denken is aan handelingsperspectieven voor veilige athenticatiemiddelen.
Beperking	Beleid en procedures aanpassen om de gelegenenheid te beperken van het ongewenste gedrag. Te denken is aan het technisch inregelen dat van authentificaitie (zoals mininmaal acht karakters, dubbele toegangscontrole)
Herstructurering/ Omgeving	Het aanpassen van de van de bestaande of sociale perspectief. Te denken is aan het verstrekken van informatie op het scherm bij nieuwe of aanpassingen wachtwoord (verplichte handelingen).
Dwang	Verwachtingen en beloningen creeren. Te denken is door geen toegang geven tot mobiele apparatuur bij verkeerd gebruik of juist 'handige' apps ontvangen.
Modellering	Medewerkers een laten zien wat te doen of te gaan doen. Te denken is aan hoe effectief een wachtwoordkluis is en op welke manier je dit kunt inrichten.
Enablement/ in staat stellen	Gewenst gedrag instaat stellen door mogelijkheden te geven en barrieres weg te nemen. Te denken is het aanbieden van een wachtwoordklus of afgeschermde toegang.
Stimuleren	Complimenten geven bij goed gedrag en dit delen. Te denken is om kleinen successen te 'vieren'. Kleinen stapje naar grote doelen is vooruitgang.

Stap 5b) Toetsing van interventiefuncties en interventieacties. Voor een selectie uit de interventieopties worden deze getoetst aan de APEASE-criteria (Michie et al. 2014). Dit om opties te selecteren met de grootste slagingskans. In tabel 4.4 zijn de mogelijke interventieopties voor "Het niet openen van bijlagen of links in e-mails" getoetst aan de APEASE-criteria.

Tabel 4.4 Toetsing van mogelijke interventiefuncties voor "Het niet openen van bijlagen of links in e-mails"

Mogelijke Interventie functie (rode rand BCW)	Voldoet de interventie aan de APEASE-criteria
Onderwijs	Praktisch omdat het vergroten van kennis het gedrag bevorder over hoe te handelen bij het vermoeden van een bijlage of link dit niet betrouwbaar is. Niet praktische gezien de werkdruk en verloop van medewerkers. Wel als een awarenss programma cyclisch meerdere keren per jaar.
Overtuiging	Het is onwaarschijnlijk dat dit effect heeft, omdat de houding er is, maar de kennis onlvoldoende.
Training/Opleiding	Ja, Praktisch omdat dit kleinschallig en specifiek op te zetten is. Echter zal rekening gehouden moeten worden met de tijdsbesteding. Stelling 14 'Ik mag op links in e-mails klikken van mensen die ik ken. (48%) Te denken is aan handelingsperspectieven voor veilige gebruik gegevens.
Beperking	Niet praktisch omdat beleid en procedures in deze context beperkt is gezien de diversiteit aan werkzaamheden en afhangkelijkheid van informatie.
Herstructurering/ Omgeving	Praktisch en wordt al gedaan bij gevoelige informatie, maar het is slecht meetbaar of dit toegepast wordt.
Dwang	Niet acceptabel voor het personeel.
Modellering	Niet praktisch gezien de beperkte monitoring op inhoud.
Enablement/ in staat stellen	ja
Stimuleren	ja

Stap 6) Identificeer beleidscategorieën. Aan de hand van de 'grijze' 2e omliggende ring van het BCW-model (zie ook Figuur 2.4 in hoofdstuk 2) kunnen op basis van zeven beleidscategorieën, beleidscategorieën worden geïdentificeerd die de slagingskans van gekozen interventiefuncties en acties kunnen ondersteunen. Te denken valt hierbij aan de Wetgeving door de overheid voor het vergroten van veilig informatiegedrag. Of aan de adoptie van kwaliteitsnormen zoals NEN 7510 en BIO door de directie van een organisatie. Het niveau van een behaalde certificering kan worden beschouwd als een redelijk betrouwbare voorspeller van de te verwachten prestaties.

In tabel 4.5. is voor elke BCW-beleidscategorie een voorbeeld gegeven hoe een specifieke beleidscategorie de beoogde verandering van e-mail gedrag bij VRLN kan ondersteunen.

Tabel 4.5 BCW- beleidscategorieën van Michie et al. (2016) van beoogde verandering veilig E-mail gedrag bij VRLN

Beleidscategorie	Definitie	Voorbeeld
Communicatieplan	Het gebruik van gedrukte, elektronische, telefonische of uitgezonden (social) media	Organisatiebrede campagne opstellen. Waarbij de interne als de extreme stakeholders zoals de samenwerkingspartners meegenomen zijn. Hoe om te gaan met informatie in E-mails.
Richtlijnen	Documenten maken die de praktijk aanbevelen of mandateren. Dit omvat alle wijzigingen in de dienstverlening	Opstellen en verspreiden van processen en handelsprotocollen afgeleid van NEN7510/BIO. Incl. mogelijke uitzondering die gemotiveerd variatie toelaten.
Fiscale maatregelen	Budgetten genereren/aanpassen om generieken informatieveiligheidsbewustzijn kosten te verhogen of plaasten op de afdelinge	Budgetten centraliseren voor informatieveiligheidsbewustzijn. De privacy en informatieveiligheid voor E-mail informatie hierin geprioriteerd is.
Verordening	Het vaststellen van regels of principes van gedrag of praktijk in warme(inzet) en koude organisatie.	Samenwerkingsafspraken met partners om het informatieveiligheidsbewustzijn binnen Midden-Noord Limburg tijdens een (cyber/informatieveiligheid) crisis te borgen.
Wetgeving	Wetten en governance opstellen/aanpassen	Verbieden van social mediaberichten plaatsen tijdens een incident of gebruik maken van de mobiel voor opnames en dit verspreiden via E-mail
Milieu/sociale planning	Ontwerpen en/of controleren van de fysieke of sociale omgeving. Waarbij preventie boven duurzaam staat. Rekening houdend met effecten als gevolg van een IFV.	Informatieveiligheidsprofessionals inschakelen als samenwerkingsketen voor informatieveiligheid regionaal.
Dienstverlening	Een dienst leveren	Het opzetten van ondersteunende diensten op werkplekken zoals Key-user bij Teams. Die opgeleid zijn om de basis ondersteuning te geven.

Om de *Capaciteit/Kennis* te bevorderen voor het eigen gedrag is te denken aan het ontwikkelen van vaardigheden of kennis. Hierbij laat het onderzoek van Bullée et al. (2016) zien dat beleid en educatie op het gebied van communicatie met klanten, de social engineering door cybercriminelen via telefoon tegen gaat en al effectief is op korte termijn. Om het zelfregelende *gedrag* te bevorderen is het geven van dienstverlening of het aanpassen van de werkomgeving effectief (Het Hoff-de Goede et al., 2019). Om de *motivatie* te bevorderen voor het gewenste gedrag is te denken aan het stimuleren en motiveren voor risico-eigenaarschap van het eigen gedrag van medewerkers.

4.2.1 De medewerker als risicoleider voor het bevorderen van informatieveilig gedrag

Om het informatiegedrag te bevorderen is het belangrijk om de medewerker bewust te maken van het bestaan van informatieveiligheidsrisico's. Het bewust maken van het bestaan en de preventie mogelijkheden van het risico begint bij de medewerker(Bullée,2017; Hart, 2017)). Volgens Van Staveren (2018) kan iedereen als risicoleider fungeren als rolmodel voor anderen. De medewerker als risicoleider durft om te gaan met de onzekerheden op een doelgerichte manier in de VUCA-wereld (van Staveren, 2018). Het als beleidsmaatregel bevorderen van risicoleiderschap in een organisatie kan bijdragen aan de informatieveiligheid in een organisatie. Om inzicht te krijgen welke vaardigheden hiertoe binnen de VRLN verder dienen te worden ontwikkeld, zijn tijdens het afstudeeronderzoek interviews met leidinggevenden en professionals gehouden en is een enquête (Van Staveren, 2018) afgenomen waarin gevraagd is om vaardigheden te prioriteren die van belang zijn voor de rol van een risicoleider binnen VRLN. Uit deze enquête kwamen vier vaardigheden naar voren die prioriteit verdienen (stelling 6, 8, 18 en 20), namelijk het ontwikkelen van: Risicoeigenaarschap; Positief gedrag en vertrouwen; Vroegtijdig signaleren van afwijkingen en fouten en het stellen van vragen (zie ook Figuur 4.2.) en bijlage F met een verdere toelichting.

Voor de inzetbaarheid van deze vier vaardigheden als risico-leiderschap is sturing nodig vanuit management om terug naar de essentie van het risico te gaan. Voor de effectiviteit zijn deze in te delen vanuit risicosturing in 4D's clusters (Van Staveren 2018, 2020):

De risicoleider werkt *D*oelgericht. Dit kunnen meerdere doelen of tegenstrijdige doelen zijn. Door het maken van keuzes, het prioteren van doelen en risico's te monitoren.

De risicoleider accepteert *D*iversiteit door het toelaten en accepteren van variatie, het stellen van vragen en motiveren van anderen.

De risicoleider *D*urft en heeft lef om eigenaarschap vanuit positief gedrag en vertrouwen de onzekerheden te accepteren. Verkwisting toelaten om grotere (gevolg) risico's te verkleinen.

De risicoleider gaat het ook *D*oen. Het ontwikkelen van een dynamiek om interacties of afwijkingen vroegtijdig te signaleren vanuit lineaire en cyclische risico-stappen.

Voor het case-voorbeeld bij de VRLN van informatieveiligheidsgedrag wil dit zeggen dat de medewerker de houding heeft om eerst de informatieveiligheid van een E-mail met bijlage van een bekende te onderzoeken. Dit door deze niet te openen, ondanks dat deze belangrijk lijkt. Eerst te

controleren door bijvoorbeeld contact op te nemen met de afzender. Het (gevolg)-risico accepteren dat de gewenste actie of antwoord te laat is.

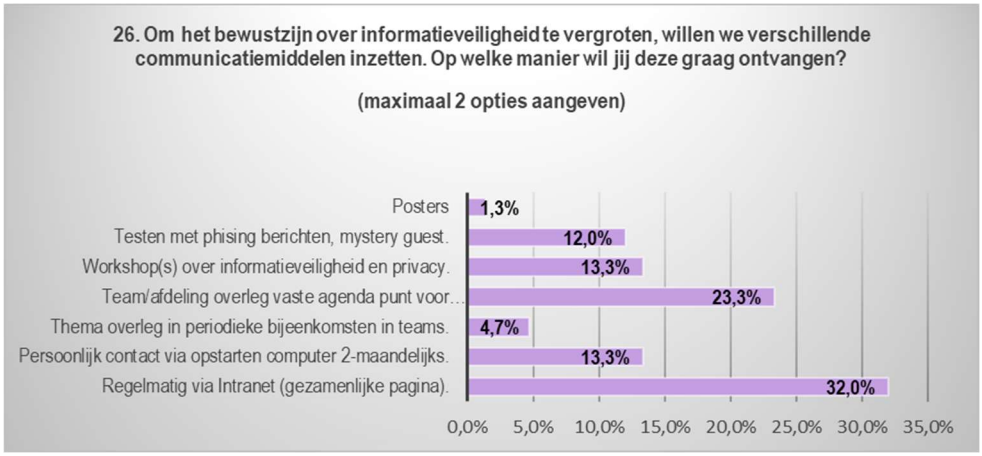
Figuur 4.2 Resultaat enquête over vaardigheden risico-eigenaarschap (Van Staveren, 2018)

4.3 Fase 3: Wat en hoe: Het identificeren van inhoud- en implementatieopties

Stap 7) Identificeer technieken voor gedragsverandering. Het identificeren van specifieke gedragsveranderingstechnieken is een actief onderdeel van een interventie die is ontworpen om gedrag te veranderen. Gedragsveranderingstechnieken kunnen verschillende interventiefuncties hebben en elke interventiefunctie kan worden geleverd door een verscheidenheid aan gedragsveranderingstechnieken. Michie et al. (2016) geven richtlijnen voor het koppelen van gedragsveranderingstechnieken aan interventiefuncties. Met behulp van de APEASE-criteria kan een selectie plaatsvinden van de technieken die het meest waarschijnlijk geschikt zijn voor een bepaalde situatie.

Bij het bevorderen van het veilig gebruik van E-mail bij de VRLN valt bijvoorbeeld te denken aan de implementatie van het 'vier ogen' principe, waarbij een collega controleert, door het uitvoeren van onafhankelijke audits, door het uitdragen van een handelingsprotocol voor E-mail en bijscholing in kleine groepen of individueel om het gewenste gedrag mogelijk maken. Bij het naleven van het gewenste gedrag is bijvoorbeeld de toekenning van een certificaat of positieve feedback bij de jaarlijkse beoordeling een stimulans.

Stap 8) Communicatie/rapportage. Deze stap is gericht op communicatie en rapportage en omvat het opstellen van een plan voor beide. Het communicatieplan omvat ook de selectie van de meest geschikte rapportage- of leveringsmethode. Het verdient aanbeveling om jaarlijks de HAIS-Q enquête te gebruiken om vorderingen ten aanzien van informatieveilig gedrag in kaart te brengen en in het bijzonder verbetering van het gedrag ten aanzien van eerdere als kritiek beoordeelde vraagstellingen. Voor het onderwerp "bewustwording" is in de uitgevoerde enquête stelling 26 opgenomen. De resultaten toonden aan dat het interne intranet het meest effectieve communicatiemiddel is (zie Figuur 4.3). Dit biedt de mogelijkheid om kleine successen te vieren, zoals het voorkomen van een cyberincident of het volgen van een training. Hierdoor wordt de bewustwording en betrokkenheid onder de medewerkers ten aanzien van informatieveiligheid verder verhoogd.



Figuur 4.3 HAIS-Q enquête vraag 26

4.4 Antwoord op deelvraag 3 van het onderzoek

De voor dit hoofdstuk te beantwoorden deelvraag luidde: "*Hoe kan, gegeven de uitkomsten van de literatuurstudie en de gehouden 0-meting en analyse, het informatieveiligheidsgedrag in de organisatie worden bevorderd?*".

Voor Veiligheidsregio Limburg-Noord kan het door Michie et al. (2016) ontwikkelde stappenplan voor het ontwerpen van gedragsveranderingsinterventies worden toegepast. In dit hoofdstuk is dit stappenplan nader toegelicht en ter illustratie ook concreet toegepast voor de bevordering van het veilig gebruik van E-mails bij Veiligheidsregio Limburg-Noord.

Maar is dit zo? Deze discussie en de beperkingen van dit onderzoek zijn toegelicht in het vijfde hoofdstuk.

H5 Discussie, beperking en vooruitzicht

Het verhogen van het informatieveiligheidsgedrag van medewerkers werkzaam bij Veiligheidsregio Limburg-Noord is leidend geweest als doelstelling in dit afstudeeronderzoek. Dit doel werd tijdens het onderzoek geëffectueerd door:

- Het uitvoeren van een 0-meting van het informatieveiligheidsgedrag van medewerkers van Veiligheidsregio Limburg-Noord en
- Effectieve interventies voor te stellen voor het bevorderen van informatieveiligheidsgedrag van medewerkers.

Bovenstaande doelstelling resulteerde in de volgende hoofdvraag voor het afstudeeronderzoek:

> Op welke wijze is het informatieveiligheidsgedrag van medewerkers bij de VRLN op structurele wijze te bevorderen?

Deze hoofdvraag is beantwoord door eerst een drietal deelvragen te onderzoeken en beantwoorden. Paragraaf 5.1 gaat in op de drie gestelde deelvragen en beantwoordt vervolgens de hoofdvraag van het afstudeeronderzoek. In paragraaf 5.2. vindt een discussie plaats over de wetenschappelijke en maatschappelijke bijdrage van dit onderzoek. Paragraaf 5.3 geeft de conclusie. Tenslotte worden in paragraaf 5.4 een aantal beperkingen van het onderzoek toegelicht en aanbevelingen gemaakt voor vervolgonderzoek.

5.1 Een antwoord op de deelvragen en hoofdvraag van dit onderzoek

Deelvraag 1: Welke variabelen zijn te gebruiken voor het beoordelen van de effectiviteit van het informatieveiligheidsgedrag?

Zoals toegelicht in het eerste hoofdstuk is het onderzoek gestart met een vooronderzoek naar het informatieveiligheidsgedrag bij de VRLN een heeft er vervolgens een uitgebreid literatuuronderzoek plaatsgevonden naar variabelen die te gebruiken zijn voor het beoordelen van de effectiviteit van het informatieveiligheidsgedag van medewerkers in organisaties. De in hoofdstuk 2 besproken literatuur maakte dat duidelijk dat de 'Human Aspects of Information Security Questionnaire' (HAIS-Q) de relevante variabelen bevat om het informatieveiligheidsgedrag van medewerkers in een organisatie te meten en te classificeren: Kennis, Houding en Gedrag.

Deelvraag 2: Wat zijn de resultaten van een 0-meting en analyse van het informatieveiligheidsgedrag van medewerkers werkzaam bij de VRLN?

Op basis van een zevental semigestructureerde interviews met medewerkers bij de VRLN, met als doel de validiteit en betrouwbaarheid van de HAIS-Q voor de situatie bij de VRLN te verifiëren, is de HAIS-Q vragenlijst op een beperkt aantal onderdelen aangepast, uitgebreid en vervolgens als meetinstrument toegepast bij de VRLN. De uitgevoerde 0-meting en analyse van het informatieveiligheidsgedrag maakt duidelijk dat van de 69 gestelde vraagstellingen, er vier als kritisch kunnen worden gelabeld en duidelijk verbetering behoeven. Uit de analyse blijkt verder dat de score voor de vier kritieke vraagstellingen verschilt per leeftijdsgroep. Zo blijkt uit de resultaten dat de leeftijdsgroep die jonger is dan 30 jaar, in onvoldoende mate de sociale media privacy instellingen controleren en dat de leeftijdsgroep van 60 jaar en ouder onvoldoende besef heeft van het potentiële gevaar dat zij lopen bij het openen van links in e-mails van bekenden. Deze demografische verschillen wijzen op de noodzaak van een gedifferentieerde aanpak bij het bevorderen van het informatieveiligheidsgedrag bij medewerkers bij de VRLN.

Deelvraag 3: Hoe kan, gegeven de uitkomsten van de literatuurstudie en de gehouden 0-meting en analyse, het informatieveiligheidsgedrag in de organisatie verder worden bevorderd?

Een belangrijke opbrengst van de uitgevoerde literatuurstudie is de door Michie et al. (2016) op basis van het COM-B model en BCW-model (Michie et al., 2011) ontwikkelde methode voor het succesvol ontwerpen van gedragsveranderingsinterventies. In hoofdstuk 4 is deze methode toegepast om mogelijke interventies af te leiden om het informatieveiligheidsgedrag bij E-mail gebruik bij de VRLN te bevorderen. Met het oog op het bevorderen van het informatieveiligheidsgedrag bij de VRLN is daarnaast met behulp van een door Van Staveren (2018) ontwikkelde vragenlijst nagegaan, welke risicovaardigheden er binnen de organisatie verder ontwikkeld dienen te worden.

Hoofdvraag: Op welke wijze is het informatieveiligheidsgedrag van medewerkers bij de VRLN op structurele wijze te bevorderen?

Op basis van de inzichten verworven bij de beantwoording van de drie deelvragen, kan worden gesteld dat het informatieveiligheidsgedrag van medewerkers bij de VRLN op structurele wijze kan worden bevorderd door:

- De op basis van de specifieke VRLN-context aangepaste HAIS-Q vragenlijst, periodiek opnieuw uit te zetten in de organisatie. Op basis hiervan kan niet alleen worden vastgesteld welke vorderingen er zijn gemaakt op het gebied van het informatieveiligheidsgedrag bij medewerkers bij de VRLN, maar ook wat de volgende te nemen prioriteiten zijn ten aanzien van het bevorderen van de informatieveiligheid.

- Het toepassen van de door Michie et al. (2016) ontwikkelde methode voor het succesvol ontwerpen en implementeren van gedragsveranderingsinterventies. Dit op korte termijn voor de bij de 0-meting afgeleide vier kritieke vraagstellingen. Een eerste aanzet hiertoe is uitgewerkt in hoofdstuk 4 voor het bevorderen van het informatieveiligheidsgedrag bij E-mail gebruik.
- Het op continue wijze bevorderen van het informatieveiligheidsgedrag in de organisatie door het implementeren van een cyclisch Plan-Do-Check-Act leerproces voor de te implementeren en de al geïmplementeerde interventies ter bevordering van het informatieveiligheidsgedrag bij medewerkers van de VRLN (Deming, 1952).

5.2 Discussie: de wetenschappelijke en maatschappelijke bijdrage

De belangrijkste wetenschappelijke bijdrage van dit afstudeeronderzoek is het bijeenbrengen van de relevante wetenschappelijke literatuur op het gebied van het bevorderen van het informatieveiligheidsgedag van medewerkers. De uitgevoerde literatuurstudie heeft duidelijk gemaakt welke variabelen te gebruiken zijn voor het beoordelen van de effectiviteit van het informatieveiligheidsgedag van medewerkers. Daarnaast is in kaart gebracht op welke wijze op een wetenschappelijk verantwoorde wijze, gedragsinterventies gericht op het bevorderen van het informatieveiligheidsgedrag kunnen worden ontworpen en geïmplementeerd. Dit leidt tot een synthese waarbij op een wetenschappelijk onderbouwde wijze de probleemdiagnose, het ontwerp en de implementatie van interventies gericht op het bevorderen van het veiligheidsgedrag van medewerkers in een organisatie kunnen worden uitgevoerd.

Het afstudeeronderzoek is ook maatschappelijk relevant. In het eerste hoofdstuk is toegelicht dat de verwachting is, dat met de voortgaande digitalisering van onze samenleving, organisaties vroeg of laat te maken krijgen met cyberaanvallen. En dat het gedrag van medewerkers in de organisatie in dit kader een belangrijke rol speelt. In het meest recente onderzoek door een extern bedrijf naar informatieveiligheid is het onvoldoende systematisch monitoren van het informatieveiligheidsgedrag van medewerkers als één van de belangrijkste aandachtspunten aangedragen (M&I/Partners, 2019; Securesult, 2021).

Dit afstudeeronderzoek kan worden gezien als een belangrijke bijdrage tot het systematisch monitoren en bevorderen van het informatieveiligheidsgedrag van de medewerkers bij de VRLN. Bovendien kan de voorgestelde aanpak ook dienen als voorbeeld voor het bevorderen van het veiligheidsgedrag van medewerkers die werkzaam zijn in andere veiligheidsregio's in Nederland.

5.3 Conclusie

De conclusie is dat uit de kwalitatieve en kwantitatieve resultaten inzicht is gegeven in de 0-meting (IST-situatie) informatieveiligheidsgedrag eind 2022 van de VRLN met behulp van de HAIS-Q en BCW. Hierbij is op basis van de uitgevoerde deelonderzoeken een interventie cyclus uitgewerkt met behulp van Michie et al (2016) in hoofdstuk vier om de wendbaarheid, weerbaarheid en veerkracht te bevorderen. Vanuit maatschappelijk perspectief is een interventie met behulp van een praktijkvoorbeeld het aandachtsgebied 'E-mail gedrag' uitgewerkt voor de VRLN.

Concluderen is dat vanuit wetenschappelijk- en maatschappelijk perspectief het informatieveiligheidsgedrag van medewerkers op structurele wijze is te bevorderen. Nieuwe theorievorming is ontstaan voor informatieveiligheidsgedrag.

5.4 Beperkingen en aanbevelingen

Zoals bij elk onderzoek, zijn er ook voor dit afstudeeronderzoek de nodige beperkingen vast te stellen. Bij de afbakening van het onderzoek in paragraaf 1.4 werd al vermeld dat het onderzoek zich zou beperken tot het veiligheidsgedrag van medewerkers en dat de focus van het onderzoek zou liggen bij de medewerkers van de VRLN. Bijgevolg zijn de resultaten moeilijk generaliseerbaar naar andere organisaties. Een andere beperking betreft de relatief lage respons van 11,8% op de in de organisatie uitgezette HAIS-Q vragenlijst. Deze respons is evenwel niet uniek. Een respons van minder dan 10% blijkt niet ongewoon te zijn bij een online-enquête (Couper et al., 2007). Een volgende beperking is het feit dat de 0-meting een momentopname betreft. Het is zeer wel mogelijk dat het informatieveiligheidsgedrag van medewerkers sinds het moment dat de enquête werd uitgevoerd is gewijzigd. Dit pleit voor het periodiek herhalen van de meting. Fertig en Schültz (2020) concluderen in een recent uitgevoerd systematisch literatuuronderzoek, dat het meten van het bewustzijn van informatieveiligheid bij medewerkers, doorgaans via enquêtes plaatsvindt waar bij respondenten sociaal-wenselijke antwoorden kunnen geven. Daarom wordt aanbevolen om naast enquêtes ook observaties en audits uit te voeren.

Op basis van het uitgevoerde onderzoek worden de navolgende aanbevelingen gedaan.

Zoals in paragraaf 5.1. gesteld, is het belangrijk om de HAIS-Q vragenlijst periodiek uit te zetten in de organisatie. Wel zal dan steeds moeten worden nagegaan in hoeverre de vragenlijst nog up-to-date is voor wat betreft ontwikkelingen op het gebied van informatieveiligheid. Verhagen en Hermus (2023) wijzen er bijvoorbeeld op dat het inloggen met wachtwoorden, als het aan google ligt, binnenkort verleden tijd is.

En tweede aanbeveling is het verder uitwerken en toepassen van de in hoofdstuk 4 voorgestelde aanpak voor het ontwerpen en implementeren van interventies waarmee het veiligheidsgedrag van medewerkers kan worden bevorderd.

Tenslotte wordt aanbevolen om in een vervolgonderzoek na te gaan op welke wijze een cyclisch leerproces kan worden ontwikkeld en geïmplementeerd dat niet alleen rekening met het continu verbeteren van het veiligheidsgedrag van medewerkers op basis van geconstateerde tekortkomingen, maar waarbij ook rekening gehouden wordt met externe veranderingen op het gebied van cybersecurity die ook weer van invloed kunnen zijn op het veiligheidsgedrag van medewerkers.

Literatuur

Abraham, C., & Sheeran, P. (2015). The Health Belief Model. *ResearchGate*. https://www.researchgate.net/publication/290193215_The_Health_Belief_Model

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50(2)*, 179-211. http://doi:10.1016/0749-5978(91)90020-T

Ajzen, I. (2002). Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior1. *Journal of Applied Social Psychology*, 32(4), 665–683. https://doi.org/10.1111/j.1559-1816.2002.tb00236.x

Binder, Dijker, Otte &CO (BDO) (2022). security- en privacy-awareness in onderwijs en onderzoek 2022. BDO. https://www.bdo.nl/nl-nl/perspectieven/security-en-privacy-awarenessmeting-in-onderwijs-en-onderzoek-maak-awareness-minder-vrijblijvend

Bio-overheid. (2020). *BIO versie 1*. https://bio-overheid.nl/media/1572/bio-versie-104zv_def.pdf

Bullée, JW.H., Hartel, P., M., Junger, M., Montaya (2015). *The persuasion and security awareness experiment: reducing the success of social engineering attacks.* Journal of Experimental Criminology, 11(1), 97–115. https://doi.org/10.1007/s11292-014-9222-7

Bullee, J., Montoya, L., Pieters, W., Hartel, P. H., & Hartel, P. H. (2018). On the anatomy of social engineering attacks-A literature-based dissection of successful attacks. *Journal of Investigative Psychology and Offender Profiling*, 15(1), 20–45. https://doi.org/10.1002/jip.1482

Bullee, J., & Hartel, P. H. (2020). How effective are social engineering interventions? A meta-analysis. *Information & computer security*, 28(5), 801–830. https://doi.org/10.1108/ics-07-2019-0078

Cohen, J. (2013). *Statistical power analysis for the behavioral sciences*. Routledge

Conner, M., & Norman, P. (2017). Health behaviour: Current issues and challenges. *Psychology & Health*, 32(8), 895–906. https://doi.org/10.1080/08870446.2017.1336240

Conner, M., & Norman, P. (2022). Understanding the intention-behavior gap: The role of intention strength. Frontiers in Psychology, 13. https://doi.org/10.3389/fpsyg.2022.923464

Couper, M. P., Kapteyn, A., Schonlau, M., & Winter, J. (2007). Noncoverage and nonresponse in an Internet survey. Social Science Research, 36(1), 131–148. https://doi.org/10.1016/j.ssresearch.2005.10.002

Clarke, N., & Furnell, S. (2020). Human Aspects of Information Security and Assurance. *In IFIP advances in information and communication technology*. Springer Science+Business Media. https://doi.org/10.1007/978-3-030-57404-8

Clarke, N., & Furnell, S. (2022). Human Aspects of Information Security and Assurance: 16th IFIP WG 11.12 International Symposium, HAsISA 2022, Mytilene, Lesbos, Greece, July 6–8, 2022, Proceedings. Springer Nature.

Deming, W.E. (1952). *Elementary Principles of the Statistical Control of Quality*. Uitgeverij Nippon Kagaku

Dhakal, R. (2018). *Measuring the effectiveness of an information security training and awareness program*. https://www.semanticscholar.org/paper/Measuring-the-effectiveness-of-an-information-and-Dhakal/29fdb0b62c6bf92748edd8147ddea084259cc05e

Digitale Overheid. (2022, 6 mei). *Wet- en regelgeving Cybersecurity - Digitale Overheid*. https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/informatieveiligheid/wet-en-regelgeving

Dodel, M., & Mesch, G. S. (2017). Cyber-victimization preventive behavior: A health belief model approach. *Computers in Human Behavior*, 68, 359–367. https://doi.org/10.1016/j.chb.2016.11.044

Fertig, T., Schültz (2020). *About the Measuring of Information Security Awareness: A Systematic Literature Review*. https://scholarspace.manoa.hawaii.edu/handle/10125/64540

Global Risks Report 2023 | World Economic Forum. (z.d.). World Economic forum. https://www.weforum.org/reports/global-risks-report-2023

Halman, J.I.M., & Huisman, H.M. (2021) Evaluation of Covid-19 crisis management at the University of Twente: The first phase of covid-19 crisis https://doi.org/10.3990/1.9789036551595

Hart, W. (2017). Anders vasthouden: 9 sleutels voor het werken vanuit de bedoeling. Vakmedianet management b.v.

Häussinger, F. (2015). Studies on Employees' Information Security Awareness. https://doi.org/10.53846/goediss-5137

Het Hoff-de Goede, S., Van der Kleij, R., s, van der Weijer, & Leukfeldt, R. (2019). Hoe veilig gedragen wij ons online. onderzoek NSCR.Ministerie van justitie en Veiligheid. https://open.overheid.nl/documenten/ronl-8271d4ec-e54c-4568-b00d-7cc161ef7066/pdf

Home NL - *bio-overheid*. (z.d.). Geraadpleegd op 19 oktober 2022, van https://www.bio-overheid.nl/

Kasperson, R. E., Renn, O., Slovic, P., Brown, H. S., Emel, J., Goble, R., Kasperson, J. X., & Ratick, S. (1988). The social amplification of risk: A conceptual framework. *Risk Analysis, 8*(2), 177–187. https://doi.org/10.1111/j.1539-6924.1988.tb01168.x

Kotter, J. P., (2007). *Leading change: Why transformation efforts fail*, university Twente (IEEE Engineering Management Review) http://DOI:10.1109/EMR.2009.5235501

Leukfeldt, E. R. (2017). Research agenda. The human factor in cybercrime and cybersecurity. ResearchGate. https://www.researchgate.net/publication/317191029_Research_agenda_The_human_factor_in_cybercrime_and_cybersecurity/link/592c11b6458515e3d46fabff/download

Maddux, J. E., & Rogers, R. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

McCormac, A., Calic, D., Parsons, K., Zwaans, T., Parsons, M., & Pattison, M. (2016). Test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q). corpus ID:1992671.

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

M&I/Partners. 2019, integrale toets veiligheidsregio's. Vertrouwelijk rapport

Michie, S., Van Stralen, M. M., & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science, 6*(1). https://doi.org/10.1186/1748-5908-6-42

Michie, S., Atkins, L., & Gainforth, H. L. (2016). Changing Behaviour to Improve Clinical Practice and Policy. In Novos Desafios, Novas Competências: *Contributos Atuais da Psicologia* (pp. 41–60). https://doi.org/10.17990/axi/2016_9789726972679_041

Ministerie van Justitie en Veiligheid. (2021, 7 december). *Evaluatie Wet veiligheidsregio's naar toekomstbestendige crisisbeheersing en brandweerzorg.* Rapport | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/rapporten/2020/12/04/tk-bijlage-evaluatie-wet-veiligheidsregio-s

Mukhtar, S. (2020). Mental health and emotional impact of COVID-19: Applying Health Belief Model for medical staff to public of Pakistan. *Brain Behavior and Immunity*, 87, 28–29. https://doi.org/10.1016/j.bbi.2020.04.012

NEderlandse Norm (NEN) (2015). *Verzekeren kan altijd nog. Risicomanagement en bedrijfscontinuiteitsmanagement*. Geraadpleegd 16 Februari 2023, van https://www.nen.nl/verzekerenkanaltijdnog

NEderlandse Norm (NEN) (2019). *Informatiebeveiliging in de zorg - register NEN 7510*. Geraadpleegd op 19 oktober 2022, van https://www.nen.nl/certificatie-en-keurmerken-nen-7510

Onderzoekgroep Cybersafety(2021) D*e werking van de basisscan cyberweerbaarheid*, Een kwalitatief onderzoek naar het gedrag van ondernemers , Geraadpleegd 12 oktober 2022, van https://www.researchgate.net/publication/355146282_De_werking_van_de_Basisscan_Cyberweerbaarheid_Een_kwalitatief_onderzoek_naar_het_gedrag_van_ondernemers

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

Parsons, K., McCormac, A., Parsons, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 173–174. https://doi.org/10.1016/j.cose.2013.12.003

Rogers, R. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology,* 91(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Stel, M., Ketelaar, D., Gutteling, J. M., Giebels, E., Egtbers, M., & Kerstholt, J. (2019). *Vulnerable Groups in Emergencies: When and Why are They at Risk?* University of Twente.

Securesult. 2021, Analyse BIO en NEN7510 2e helft 2021, vertrouwelijk rapport

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

Slovic, en Weber(2002). Perception of Risk Posed by Extreme Events. In Risk Management strategies in an Uncertain World. *ResearcheGate* https://www.researchgate.net/publication/209805350_Perception_of_Risk_Posed_by_Extreme_Events

Taleb, N. N. (2008). *De Zwarte Zwaan(2e)*. Uitgeverij Nieuwezijds.

Van Aken, J.,van & Berends, H.(2018). *Problem solving in Organizations. A Methodological Handbook for Business and Management Students* (3e druk). Uitgeverij Cambridge University Press

Van Der Kleij, R., & Leukfeldt, R. (2019). *Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security. In Advances in intelligent systems and computing*. Springer Nature. https://doi.org/10.1007/978-3-030-20488-4_2

Van Heijst, L. (2021, 27 oktober). *Cronbach's alpha in SPSS: Berekenen en interpreteren*. Scribbr. https://www.scribbr.nl/statistiek/cronbachs-alpha.

Van Staveren, M.T.(2009). Risk, Innovation and Change: Design Propositions for Implementing Risk Management in Organizations. Dissertation University of Twente.

Van Staveren, M.T. (2015). *Risicogestuurd werken in de praktijk* (3e editie). Vakmedianet.

Van Staveren, M.T. (2018). *Risicoleiderschap: doelgericht omgaan met onzekerheden*. Vakmedianet

Van Staveren, M.T. (2020). *Iedereen risicoleider(3e)*. Boom

Van Der Steen, M., & Van Twist, M. (2014). Weerbaar of wendbaar zijn? Strategische opties in de voorbereiding op de drie decentralisaties. B En M, 41(1), 58–64. https://doi.org/10.5553/benm/138900692014041001010

Verbeek (2021). De Human Aspects of Information Security Questionnaire (HAIS-Q). (z.d.). *Open Universiteit research portal*. https://research.ou.nl/en/studentTheses/de-human-aspects-of-information-security-questionnaire-hais-q

Verhagen, L. & Hermus, S. (2023) Inloggen met wachtwoord verleden tijd? Als het aan google ligt wel. *Volkskrant*, 4 mei 2023. https://www.volkskrant.nl/economie/inloggen-met-wachtwoord-binnenkort-verleden-tijd-als-het-aan-google-ligt-wel~b758d8b3/

Verschuren, P., & Doorewaard, H. (2021). *Het ontwerpen van een onderzoek,* (6e druk), Boom uitgeverij.

VRLN beleidsplan 2020-2023 - Cover. (2019), geraadpleegd december 2022. https://publicaties.vrln.nl/vrln-beleidsplan2020-2023

Wetten.nl - Regeling - *Wet veiligheidsregio's* - BWBR0027466. (2010, 1 oktober). https://wetten.overheid.nl/BWBR0027466/2010-10-01/1

Lijst met afkortingen

Afkorting	Omschrijving
BIO	Baseline Informatiebeveiliging Overheid
BCW	Behaviour Change Wheel
CISO	Chief Information Security Officer
COM-B	Cability-Opportunity-Motivation-Behaviour model
DPG	Directeuren Publieke Gezondheid
GGD	Gemeenschappelijk gezondheidsdienst
GRIP	Gecoördineerde Regionale Incidentbestrijdingsprocedure
HAIS-Q	Human Aspect of information Security Questionnaire.
Enquête	De HAIS-Q vragenlijst aangevuld met de demografische gegevens en interventievragen
Informatieveiligheidsgedrag	Informatieveiligheidsgedrag. In het Engels information safety awareness (ISA)
IBP	Informatieveiligheidsplan
ISO	International Organization for Standardization
NEN	Nederlandse normering van richtlijnen
NIPV	Nederlands instituut publieke veiligheid
PvA	Plan van aanpak
PDCA	Plan Do Check Act circle (Deming, 1952)
RCDV	Raad Commandanten en Directeuren Veiligheidsregio's
SIEM	Security information & event management
VR	Veiligheidsregio met een GGD
VRLN	Veiligheidsregio Limburg- Noord
VUCA	Volantiel, Onzekerheid, Complexiteit en Ambiguïteit (- wereld)
VWS	Ministerie van volksgezondheid, Welzijn en sport

Figuren en tabellen

Gebruikte figuren **Pagina**

Gebruikte tabellen

Bijlage A: HAIS-Q toelichting

Toelichting aandachtsebieden

Een toelichting op de aandachtsgebieden informatieveiligheid en aangepaste subgebieden vanuit Parsons et a.l (2014) en (Clarke & Furnell, 2020)vanuit drie variabelen gedrag, houding en kennis:

1) *Authentificatiemiddelen/Wachtwoordmanagement*
   Informatiebronnen beschermen. Het is een beveiligingstechniek tegen cybercriminaliteit en is een vorm van digitaaal bewijs van de identiteit. Het inregelen en managenen van wachtworoden door te varieren, regelmatig wijzigen en kiezen van sterke wachtwoorden. Dit betekent het gedrag, kennis en houding hoe informatiesysteembronnen te beschermen. Deze zijn vaak technisch ondersteund(afgedwongen). Hierbij gaat het om het gebruik van verschillende wachtwoorden bij diverse systemen. Het delen van wachtwoorden of 'pasjes' met andere (bekenden).
2) *Emailgebruik*
   Dit betekent gedrag van veilig gebruik van Email. Hierbij is een onderverdeling in downloaden van onveilige bijlagen of klikken op links van bekende of onbekende afzenders.
   Hierbij is het 'vissen' of 'hengelen' meestal via een Email om informatie te ontfutselen 'phising' genoemd. Bij het onveilige bijlage kan er sprake zijn van 'Spyware'. Dit is software die ongegemerkt informatie verzameld en doorstuurd, waarbij te denken is aan inlogggegevens, mailadresssen of persoonlijke informatie. 'online fingerprint' het actief ophalen van unieke gegevens van de computer (zoals Email adresssen, wachtwoorden) via een een kwaadaardige software die geactiveerd is na het het openen van een bericht (site politie.nl).
3) *Internetgebruik*
   Het gedrag bij het veilig gebruiken van intranet. Het downloaden van bestanden, Het opzoeken van dubieuze websites en het online invoeren van informatie.
4) *Incidentenmanagement*
   Dit betekent gedrag van hoe incidenten beperkt en gemeld kunnen worden. Hierbij is een onderverdeling in het zelf handelen en collega's aanspreken, tot het melden van een incident aan bod komen.
5) *Gebruik van sociale media*
   Dit betekent gedrag van sociale media gebruik, waarbij het gaat om de eigen
   privacy-instellingen, nettiquette (rekening houden met de gevolgen van het plaatsen van informatie(berichten) en doen van handelingen.
6) *Gebruik van (mobiele) apparaten*
   Het fysiek omgaan met mobiele aparaten (in openbare ruime). Het fysiek beveiligen, het verzenden van gevoelige informatie via openbare wifi en het beschermen tegen schoudersurfen (meekijken) door onbevoegden.
7) *Informatieverwerking*
   Dit betekent hoe met gevoelige informatie om te gaan, waarbij het gaat om het weggooien, het opslaan op de computer of op een extern apparaat als USB (wat in de organisatie technisch niet mogelijk is) en gebruiken op de werkplek.
8) *Privacy*
   Omgang met privacygevoelige informatie, waarbij het gaat om het niet openbaar maken, de rechtmatigheid van verwerken en het verzamelen volgens de privacyrichtlijnen wet en regelgeving en goverance van de organisatie.

Onderstaand het orgineel HAIS-Q Parson et al (2013)

	Knowledge	Attitude	Behaviour
Focus area: Password management			
Using the same password	It's acceptable to use my social media passwords on my work accounts. ^	It's safe to use the same password for social media and work accounts. ^	I use a different password for my social media and work accounts.
Sharing passwords	I am allowed to share my work passwords with colleagues. ^	It's a bad idea to share my work passwords, even if a colleague asks for it.	I share my work passwords with colleagues. ^
Using a strong password	A mixture of letters, numbers and symbols is necessary for work passwords.	It's safe to have a work password with just letters. ^	I use a combination of letters, numbers and symbols in my work passwords.
Focus area: Email use			
Clicking on links in emails from known senders	I am allowed to click on any links in emails from people I know. ^	It's always safe to click on links in emails from people I know. ^	I don't always click on links in emails just because they come from someone I know.
Clicking on links in emails from unknown senders	I am not permitted to click on a link in an email from an unknown sender.	Nothing bad can happen if I click on a link in an email from an unknown sender. ^	If an email from an unknown sender looks interesting, I click on a link within it. ^
Opening attachments in emails from unknown senders	I am allowed to open email attachments from unknown senders. ^	It's risky to open an email attachment from an unknown sender.	I don't open email attachments if the sender is unknown to me.
Focus area: Internet use			
Downloading files	I am allowed to download any files onto my work computer if they help me to do my job. ^	It can be risky to download files on my work computer.	I download any files onto my work computer that will help me get the job done. ^
Accessing dubious websites	While I am at work, I shouldn't access certain websites.	Just because I can access a website at work, doesn't mean that it's safe.	When accessing the Internet at work, I visit any website that I want to. ^
Entering information online	I am allowed to enter any information on any website if it helps me do my job. ^	If it helps me to do my job, it doesn't matter what information I put on a website. ^	I assess the safety of websites before entering information.
Focus area: Social media use			
SM privacy settings	I must periodically review the privacy settings on my social media accounts.	It's a good idea to regularly review my social media privacy settings.	I don't regularly review my social media privacy settings. ^
Considering consequences	I can't be fired for something I post on social media. ^	It doesn't matter if I post things on social media that I wouldn't normally say in public. ^	I don't post anything on social media before considering any negative consequences.
Posting about work	I can post what I want about work on social media. ^	It's risky to post certain information about my work on social media.	I post whatever I want about my work on social media. ^
Focus area: Mobile devices			
Physically securing mobile devices	When working in a public place, I have to keep my laptop with me at all times.	When working in a café, it's safe to leave my laptop unattended for a minute. ^	When working in a public place, I leave my laptop unattended. ^
Sending sensitive information via Wi-Fi	I am allowed to send sensitive work files via a public Wi-Fi network. ^	It's risky to send sensitive work files using a public Wi-Fi network.	I send sensitive work files using a public Wi-Fi network. ^
Shoulder surfing	When working on a sensitive document, I must ensure that strangers can't see my laptop screen.	It's risky to access sensitive work files on a laptop if strangers can see my screen.	I check that strangers can't see my laptop screen if I'm working on a sensitive document.
Focus area: Information handling			
Disposing of sensitive print-outs	Sensitive print-outs can be disposed of in the same way as non-sensitive ones.^	Disposing of sensitive print-outs by putting them in the rubbish bin is safe. ^	When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed.
Inserting removable media	If I find a USB stick in a public place, I shouldn't plug it into my work computer.	If I find a USB stick in a public place, nothing bad can happen if I plug it into my work computer. ^	I wouldn't plug a USB stick found in a public place into my work computer.
Leaving sensitive material	I am allowed to leave print-outs containing sensitive information on my desk overnight. ^	It's risky to leave print-outs that contain sensitive information on my desk overnight.	I leave print-outs that contain sensitive information on my desk when I'm not there. ^
Focus area: Incident reporting			
Reporting suspicious behaviour	If I see someone acting suspiciously in my workplace, I should report it.	If I ignore someone acting suspiciously in my workplace, nothing bad can happen. ^	If I saw someone acting suspiciously in my workplace, I would do something about it.
Ignoring poor security behaviour by colleagues	I must not ignore poor security behaviour by my colleagues.	Nothing bad can happen if I ignore poor security behaviour by a colleague. ^	If I noticed my colleague ignoring security rules, I wouldn't take any action. ^
Reporting all incidents	It's optional to report security incidents. ^	It's risky to ignore security incidents, even if I think they're not significant.	If I noticed a security incident, I would report it.

Bijlage B: Enquete HAIS-Q en aanvullende vragen (IST-situatie) (deelvraag 2 en 3)

Vragenlijst op interne digitale pagina voor medewerkers VRLN geplaats

- *De enquête publiceren op de interne informatiepagina intranet om toegankelijkheid te bevorderen.*
- *De enquête is anoniem en bedoeld om kwantitatieve en kwalitatieve informatie over informatieveiligheidsgedrag te ontvangen.*
- *De enquête vindt plaats op vrijwillige basis en de respondent weet dat het voor het afstuderen en probleem van de organisatie is.*
- *De enquête is een afgeleide van de HAIS-Q-enquête en aangevuld met algemene vragen voor diepteanalyse en voor organisatie-inzicht met betrekking tot het onderwerp. vraag 1, 25 t/m 31*
  De vraagstelling van de HAIS-Q zijn in afwijking van eerder onderzoeken bondiger opgesteld om een betere leesbaarheid te krijgen. Dit gevalideerd op construct door interview vooraf met een professional.
  Groen : tekstuele aanpassing en ~~Rood:~~ tekst weggehaald
- *Hierbij is een keuze vanuit een likert schaal van zeven*
- *De enquête is samengesteld met behulp van het programma Microsoft Forms.*
- *Zie bijlage H voor de vragen lijst.*
- *De Ethische code van universiteit van Twente en de privacyrichtlijnen van de VRLN zijn van toepassing*
- *Dit onderzoek is beoordeeld en goedgekeurd door de ethische commissie van de faculteit BMS.*
- *In het kort bestaat de enquête uit acht aandachtsgebieden en hierin drie onderwerpen met een likert-schaal van zeven*
- *Naast de acht aandachtsgebieden vanuit de HAIS-Q zijn nog algemene vragen gesteld .*

Veerkrachtige informatieveiligheid

veiligheidsregio limburg-noord

Beste collega's

Zoals jullie wellicht weten zitten we in een traject om informatieveiligheid binnen de VRLN op orde te krijgen. Hiervoor loopt voor de GGD een certificeringstraject NEN 7510 en voor Brandweerzorg en Crisisbeheersing een BIO (Baseline Informatieveiligheid Overheid) traject. Een belangrijk element hierin is de awareness meting. Met andere woorden, waar staan we nu op het gebied van ons handelen en doen als het aankomt op informatieveiligheid. Deze meting zal door Desiré Jetten uitgevoerd worden en is ook haar afsluitend onderzoek in het kader van de studie master risicomanagement. Deze meting geeft ons zicht op de situatie waar we nu staan.

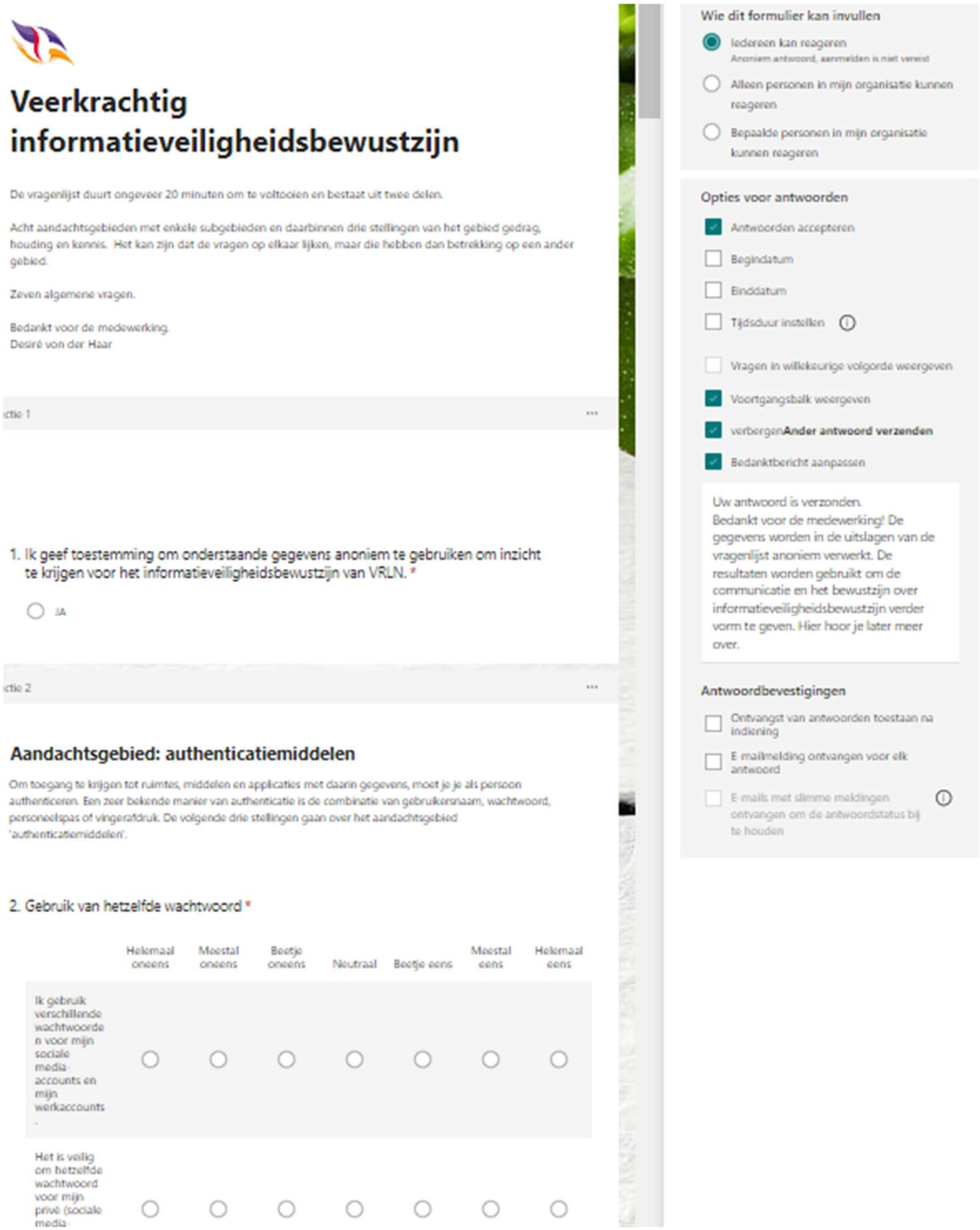
Het gaat om een vragenlijst over het informatieveiligheidsbewustzijn van de VRLN. Eerdere personen hadden hiervoor 10 á 15 minuten van hun tijd nodig. Er is geen goed of fout antwoord en de antwoorden worden anoniem verwerkt.

De vragenlijst bestaat uit twee delen:

- Stellingen over informatieveiligheid binnen acht aandachtsgebieden en enkele subgebieden. Hierbij kunnen zeven keuzes gemaakt worden.
- Vijf algemene vragen die anoniem verwerkt worden voor mogelijke analyse.

Heb je opmerkingen, wil je die dan onderaan de vragenlijst voor me opschrijven? Daar is ruimte voor. Bij prangende vragen kun je mij een mail sturen en dan beantwoord ik die.

Met vriendelijke groet,
Desiré Jetten-von der Haar



Veerkrachtig informatieveiligheidsbewustzijn

De vragenlijst duurt ongeveer 20 minuten om te voltooien en bestaat uit twee delen.

Acht aandachtsgebieden met enkele subgebieden en daarbinnen drie stellingen van het gebied gedrag, houding en kennis. Het kan zijn dat de vragen op elkaar lijken, maar die hebben dan betrekking op een ander gebied.

Zeven algemene vragen.

Bedankt voor de medewerking.
Desiré von der Haar

ctie 1

1. Ik geef toestemming om onderstaande gegevens anoniem te gebruiken om inzicht te krijgen voor het informatieveiligheidsbewustzijn van VRLN. *

JA

ctie 2

Aandachtsgebied: authenticatiemiddelen

Om toegang te krijgen tot ruimtes, middelen en applicaties met daarin gegevens, moet je je als persoon authenticeren. Een zeer bekende manier van authenticatie is de combinatie van gebruikersnaam, wachtwoord, personeelspas of vingerafdruk. De volgende drie stellingen gaan over het aandachtsgebied 'authenticatiemiddelen'.

2. Gebruik van hetzelfde wachtwoord *

	Helemaal oneens	Meestal oneens	Beetje oneens	Neutraal	Beetje eens	Meestal eens	Helemaal eens
Ik gebruik verschillende wachtwoorden voor mijn sociale media accounts en mijn werkaccounts.							
Het is veilig om hetzelfde wachtwoord voor mijn privé (sociale media							

Wie dit formulier kan invullen

- Iedereen kan reageren
  Anoniem antwoord, aanmelden is niet vereist
- Alleen personen in mijn organisatie kunnen reageren
- Bepaalde personen in mijn organisatie kunnen reageren

Opties voor antwoorden

- Antwoorden accepteren
- Begindatum
- Einddatum
- Tijdsduur instellen
- Vragen in willekeurige volgorde weergeven
- Voortgangsbalk weergeven
- verbergen**Ander antwoord verzenden**
- Bedanktbericht aanpassen

Uw antwoord is verzonden.
Bedankt voor de medewerking! De gegevens worden in de uitslagen van de vragenlijst anoniem verwerkt. De resultaten worden gebruikt om de communicatie en het bewustzijn over informatieveiligheidsbewustzijn verder vorm te geven. Hier hoor je later meer over.

Antwoordbevestigingen

- Ontvangst van antwoorden toestaan na indiening
- E-mailmelding ontvangen voor elk antwoord
- E-mails met slimme meldingen ontvangen om de antwoordstatus bij te houden

Tabel 0.1 HAIS-Q aangepast lijst

Aandachts-gebied	Subgebieden	Stellingen	Variabelen
Authenticatie-middelen	Wachtwoorden	Ik gebruik verschillende wachtwoorden voor mijn sociale media-accounts en mijn werkaccounts.	Gedrag
		Het is veilig om hetzelfde wachtwoord voor mijn privé (sociale media-accounts) en werkaccounts te gebruiken.	Houding
		Ik mag mijn privé (social media) wachtwoord gebruiken voor mijn werkaccount.	Kennis
	Delen van authenticatie-middelen	Ik deel mijn wachtwoord (of ander authenticatiemiddel zoals een pasje, druppel) met collega s.	Gedrag
		Het is een slecht idee om mijn wachtwoorden (of andere authenticatiemiddelen zoals pasje) te delen met een collega.	Houding
		Ik mag mijn wachtwoorden (of andere authenticatiemiddelen zoals pasje) delen met mijn collega s.	Kennis
	Registratie wachtwoorden	Ik registreer mijn wachtwoorden alleen in een wachtwoordenkluis en niet op een andere wijze (papier, computerbestand, telefoon etc.)	Gedrag
		Ik ben van mening dat ik mijn wachtwoorden veilig kan registreren, ook zonder het gebruik van een wachtwoordenkluis.	Houding
		Ik mag wachtwoorden registreren in een boekje of Excel bestand, als dit op een veilige manier kan, zoals in een wachtwoordenkluis.	Kennis
E- mail gebruik	Klikken op Emails van bekende afzenders	Ik klik niet op links in Emails ook al zijn deze afkomstig van iemand die ik ken.	Gedrag
		Het is veilig om op links te klikken in Emails van mensen die ik ken.	Houding
		Ik mag op links in Emails klikken van mensen die ik ken.	Kennis
	Klikken op Emails van onbekende afzenders	Als een Email van een onbekende afzender interessant lijkt, klik ik op de link in de Email.	Gedrag
		Er kan niets slechts gebeuren als ik op een link in een Email van een onbekende afzender klik.	Houding
		Ik mag op een link in een Email van een onbekende afzender klikken.	Kennis
	Openen van bijlagen in Emails van onbekende afzenders	Ik open Emailbijlagen als de afzender mij onbekend is.	Gedrag
		Het is riskant om een Emailbijlage van een onbekende afzender te openen.	Houding
		Ik mag Emailbijlagen van onbekende afzenders openen.	Kennis
Internet gebruik	Downloaden van bestanden	Ik download alleen bestanden op mijn werkcomputer die ik nodig heb en vertrouw.	Gedrag
		Het kan riskant zijn om bestanden op mijn werkcomputer te downloaden.	Houding
		Alle soorten bestanden mag ik downloaden op mijn werkcomputer voor mijn werk.	Kennis
	Benaderen van dubieuze websites	Als ik op het werk toegang heb tot het internet, bezoek ik elke website die ik wil bezoeken, want het is veilig.	Gedrag
		Ook al heb ik toegang tot een website op het werk, betekent dat niet dat het een veilige website is.	Houding
		Terwijl ik aan het werk ben mag ik alle websites benaderen.	Kennis

	Informatie online invoeren	Ik beoordeel de veiligheid van websites en het soort gevraagde informatie, alvorens deze informatie in te voeren.	Gedrag
		Als het mij helpt om mijn werk te doen, maakt het niet uit welke informatie ik op een website zet.	Houding
		Ik mag alle soorten informatie op een website invoeren als dat mij helpt bij het uitvoeren van mijn werk.	Kennis
Social media	Social Media privacy-instellingen	Ik bekijk mijn sociale media privacy-instellingen regelmatig.	Gedrag
		Het is goed om privacy-instellingen op social media regelmatig te herzien.	Houding
		Ik moet regelmatig de privacy-instellingen op mijn sociale media-accounts controleren.	Kennis
	Rekening houden met gevolgen	Ik plaats niets op sociale media wat (negatieve) gevolgen voor mijzelf en anderen kan hebben.	Gedrag
		Op sociale media kan ik ook zaken plaatsen die ik normaal gesproken niet in het openbaar zou zeggen.	Houding
		Ik kan niet ontslagen worden voor iets wat ik op sociale media plaats.	Kennis
	Plaatsen van informatie over werk	Ik plaats alles wat ik wil over mijn werk op sociale media.	Gedrag
		Het is riskant om bepaalde informatie over mijn werk op sociale media te plaatsen.	Houding
		Ik mag posten wat ik wil over mijn werk op sociale media.	Kennis
Gebruik van mobiele apparatuur	Fysieke beveiliging van mobiele apparaten	Als ik in een openbare ruimte werk, laat ik mijn laptop onbeheerd achter.	Gedrag
		Als ik in een openbare ruimte werk, kan ik mijn laptop en/of telefoon op tafel laten liggen terwijl ik een drankje ga halen.	Houding
		Als ik in een openbare ruimte werk, moet ik mijn mobiele apparatuur altijd bij me houden.	Kennis
	Versturen van privacygevoelige informatie via wifi	Ik verstuur privacygevoelige werkbestanden of mails via een openbaar WiFi-netwerk.	Gedrag
		Het is riskant om privacygevoelige werkbestanden of mails te versturen via een openbaar WiFi-netwerk.	Houding
		Ik mag privacygevoelige werkbestanden of mails versturen via een openbaar WiFi-netwerk.	Kennis
	Meekijken door onbevoegden.	Ik zorg dat onbevoegden niet kunnen meekijken als ik aan een gevoelig document werk.	Gedrag
		Het is riskant om gevoelige werkbestanden of mails te openen als onbevoegden meekijken.	Houding
		Als ik aan een gevoelig document werk, zorg ik dat onbevoegden niet kunnen meekijken.	Kennis
Informatie-verwerking	Het weggooien van gevoelige afdrukken	Wanneer gevoelige afdrukken moeten worden weggegooid, zorg ik ervoor dat ze versnipperd of vernietigd worden.	Gedrag
		Het weggooien van gevoelige afdrukken bij gewoon afval is veilig.	Houding
		Gevoelige afdrukken mogen op dezelfde manier worden weggegooid als niet-gevoelige afdrukken.	Kennis
	Achterlaten van gevoelige informatie	Ik laat afdrukken die gevoelige informatie bevatten op mijn bureau liggen als ik er niet ben.	Gedrag
		Het is riskant om afdrukken met gevoelige informatie op mijn bureau te laten liggen.	Houding

		Ik mag afdrukken met gevoelige informatie op mijn bureau laten liggen.	Kennis
~~Het plaatsen van verwijderbare media.~~ Is technische ingeregeld bij de VRLN		~~Ik zou een USB stick die ik op een openbare plaats heb gevonden niet in mijn privé of werkcomputer steken.~~	Vervallen
		~~Als ik een USB stick op een openbare plaats vind, kan er niets ergs gebeuren als ik hem op mijn privé of werkcomputer aansluit.~~	Vervallen
		~~Als ik een USB stick op een openbare plaats vind, moet ik hem niet op mijn privé of werkcomputer aansluiten~~	Vervallen
Incidenten management	Melden van verdacht gedrag	Als ik iemand verdacht zie handelen op mijn werkplek, zou ik er iets aan doen (melden of aanspreken).	Gedrag
		Ik denk niet dat er iets ergs zal gebeuren als ik iemand negeer die verdacht handelt op mijn werk.	Houding
		Als ik iemand zich verdacht zie gedragen op mijn werkplek, moet ik dat melden.	Kennis
	Negeren van slecht veiligheidsgedrag van Collega's	Als ik merk dat mijn collega de veiligheidsregels negeert, attendeer ik hem/haar daarop.	Gedrag
		Ik vind het niet mijn verantwoordelijkheid om collega s aan te spreken als zij slecht veiligheidsgedrag vertonen.	Houding
		Ik mag niet voorbijgaan aan verkeerd gedrag van mijn collega s.	Kennis
	Melden van alle incidenten	Als ik een informatieveiligheidsincident zou opmerken, zou ik het melden.	Gedrag
		Het melden van informatieveiligheidsincidenten (incl. datalekken) helpt om de informatieveiligheid te verhogen.	Houding
		Het is een keuze om informatieveiligheidsincidenten (incl. datalekken) te melden.	Kennis
	Afdrukken van privacygevoelige informatie	Ik druk nooit privacygevoelige informatie af.	Gedrag
		Voor mijn werk vind ik het gemakkelijker om privacygevoelige informatie af te drukken i.p.v. gebruik te maken van de computer.	Houding
		Het is niet acceptabel om privacygevoelige informatie af te drukken als het raadplegen digitaal kan.	Kennis
Privacy	In publieke gelegenheden praten over cliënten en/of medewerkers.	Als ik over klanten/cliënten en/of medewerkers praat, let ik op waar ik ben en doe het altijd anoniem.	Gedrag
		Ik vind het geen goed idee om in een openbare ruimte over klanten/cliënten/medewerkers te praten, ook niet als dat anoniem is.	Houding
		Ik mag in een openbare ruimte praten over klanten/cliënten of medewerkers zolang het anoniem gebeurt.	Kennis
	Inzien van persoonsgegevens van klanten/cliënten/medewerkers	Ik bekijk alleen gegevens wanneer dat nodig is om mijn werk te kunnen doen.	Gedrag
		Ik heb een geheimhoudingsplicht dus ik mag persoonsgegevens van iedereen raadplegen ook al is dat niet nodig voor mijn werk.	Houding
		Ik mag alleen persoonsgegevens raadplegen als dat voor mijn werk noodzakelijk is.	Kennis

Privacygevoelige gegevensverzamelingen buiten de applicaties Weggelaten overlapt aandachtsgebied informatieverwerking i.o.m. met projectleider NEN7510(1e interview) dubbel	~~Voor mijn studie/werk/onderzoek haal ik soms privacygevoelige gegevens uit een applicatie en sla deze op buiten den applicatie of op mijn privé computer.~~	Vervallen
	~~Het kan geen kwaad om een privacygevoelige gegevensverzameling voor mijn werk/studie/onderzoek aan te leggen op ene locatie buiten de applicatie of op mijn privé computer.~~	Vervallen
	~~Voordat ik een eigen privacygevoelige gegevensverzameling voor studie/werk/onderzoek aanleg, moet ik dit laten toetsen door de privacy officer.~~	vervallen

25. Over welke onderwerpen van informatieveiligheid wil je meer weten?
    Maximaal 2 keuzes *(interventievraag)*
    - Basiskennis informatieveiligheid (inclusief privacy)
    - Het gebruik van authenticatiemiddelen als wachtwoorden, pasjes(druppel), tweeweg verificatie
    - Welke informatie mag ik onder welke voorwaarden verzamelen, opslaan en delen?
    - Hoe kan ik social media veilig gebruiken voor het werk?
    - Wat te doen bij (het vermoeden van) een informatieveiligheid of datalek incident?
    - Hoe kan ik phishing en ransomware herkennen.

26. Om het bewustzijn over informatieveiligheid te vergroten, willen we verschillende communicatiemiddelen inzetten. Op welke manier wil jij deze graag ontvangen?
    (maximaal 2 opties aangeven) *(interventievraag)*
    - Regelmatig via Intranet (gezamenlijke pagina).
    - Persoonlijk contact via opstarten computer 2-maandelijks.
    - Thema overleg in periodieke bijeenkomsten in teams.
    - Team/afdeling overleg vaste agenda punt voor informatieveiligheid.
    - Workshop(s) over informatieveiligheid en privacy.
    - Testen met phising berichten, mystery guest.
    - Posters

27. Betrokkenheid van de afdeling bij informatieveiligheid. *(interventievraag)*
    - Mijn afdeling vindt informatiebeveiliging noodzakelijk, maar besteedt er binnen de afdeling weinig aan of stelt zich neutraal op.
    - Mijn afdeling stimuleert informatieveiligheid door het als een vast terugkomend agendapunt te bespreken.
    - Mijn afdeling vindt informatieveiligheid noodzakelijk, maar laat het vooral door de medewerkers zelf onderling oppakken.
    - Mijn afdeling wil het informatieveiligheid stimuleren, maar vindt het een lastig onderwerp.

28. Bij welke afdeling ben je werkzaam? *(optie)*
    - Brandweerzorg
    - GGD
    - Crisisbeheersing
    - Bedrijfsvoering, concern

29. Tot welke leeftijd-groep behoor je? *(discussie*)
    - < en met 30 jaar
    - ouder als 30 tot en met 40
    - ouder als 40 tot en met 50
    - ouder als 50 tot en met 60
    - 60 jaar
30. Hoelang bent u werkzaam voor de Veiligheidsregio Limburg-Noord?*(optie en discussie)*
    Graag afronden naar beneden. Iemand die 11 maanden werkzaam is, heeft dan 0 werkjaren.
31. Heb je naar aanleiding van deze enquête vragen, opmerkingen of suggesties? *(optie en discussie*

Bijlage C: Interview ontwikkeling enquête (60 minuten)

Interview met een direct strategisch leidinggevend voor validatie enquête (HAIS-Q) en/of Quiz.
Dit interview is semi-gestuurd om inzicht te krijgen in de verwachtingen van het onderzoek en mogelijke aanpassingen.

- *Het interview afnemen bij één deelnemer van de projectgroep informatieveiligheid.*
- *Het interview uitvoeren door de onderzoeker op kantoor. Als dit door omstandigheden (Covid) niet mogelijk is dan via Microsoft Teams realiseren.*
- *Het is een semi-gestuurd interview waardoor er de mogelijkheid is om verdiepingsvragen te stellen om het doel van het onderzoek te bereiken.*
- *Het interview vindt plaats op vrijwillige basis en de geïnterviewde weet dat het voor het afstuderen en probleem van de organisatie is.*
- *Het interview is anoniem, de naam en functie worden niet gepubliceerd.*
- *Het interview wordt opgenomen en getranscribeerd voor kwalitatieve analyse.*
- *De geïnterviewde krijgt vooraf de enquête voor de meting van het informatieveiligheidsgedrag om deze te classificeren; Van belang, Nuttig maar niet van belang, Niet noodzakelijk*
- *Het interview duurt maximaal 1,5 uur.*
- *De Ethische code van universiteit van Twente en de privacyrichtlijnen van de VRLN zijn van toepassing*

<u>Vragen:</u>

1) Inleiding
   - Bedanken voor deelname,
   - Vragengelegenheid
   - Doornemen van interviewopzet (vrijwillig, voor studiedoeleinden en organisatie)
   - Toestemming voor het opnemen
2) Wie is de geïnterviewde(professional als stakeholder)
   - Wat is uw functie en relatie met informatieveiligheid (gedrag)?
3) Kennis over informatieveiligheid (IST situatie)
   - Bent u bekend met de governance van informatieveiligheid van de VRLN en haar methodiek?
   - Op welk niveau staat de VRLN, kijkend naar de factor mens (informatiegedrag)
     i) 1 Geïnformeerd: reactief-
     ii) 2 Beheerd: processen worden uitgevoerd
     iii) 3 Vastgesteld: organisatiebreed vastgesteld
     iv) 4 Voorspelbaar: vastgesteld en vergeleken met de branche.
4) Oorzaken van informatieveiligheidsincidenten. (Resultaat deelvraag 2)
   - Wat zijn volgens u (de top 3) oorzaken van informatieveiligheidsincidenten?
   - Weet u in hoe de medewerkers/gebruikers in de preventie op dit moment zijn meegenomen?
5) De enquête uitleggen (20 min); 8 aandachtsgebieden met 3 onderwerpen, stellingen over kennis, houding en gedrag met 7 keuzemogelijkheden. Algemene vragen over preventiemogelijkheden, betrokkenheid organisatie en medewerkers. (Resultaat deelvraag 2)
6) Zijn de 8 aandachtsgebieden relevant volgens u voor het meten van het informatieveiligheidsgedrag? (Validatie en betrouwbaarheid HAIS-Q)
   - Welke aandachtsgebieden zijn van mindere relevantie?
   - Missen er naar uw mening aandachtsgebieden?
   - Welk aandachtsgebied is volgens u van het grootste belang?
7) Verwachting bruikbaarheid enquête (10 minuten) (Validatie en betrouwbaarheid HAIS-Q)
   - Hoe denkt u dat bereidheid is om de enquête in te vullen?
   - Hoe denkt u dat de enquête oprecht en eerlijk ingevuld wordt?
   - Levert de enquête naar uw mening bruikbare informatie op voor de organisatie?
   - Wat vindt u van de algemene vragen die gesteld worden?
8). Afronding
   - Dank u voor de bereidheid voor deelname aan het interview.
   - Wat vond u van het interview?
   - Graag wil ik u uitnodigen, als afsluiting van dit gesprek, voor een afspraak voor een tweede interview (Akkoord, datum/tijdstip inplannen en Email sturen met link) na het uitzetten van de enquête.

Bijlage D: 2e Enquete. Interventie enquête
2e interviewronde na 1e enquête (45 minuten)

Dit is een semie-gestuurd-interview met als doel evaluatie enquête en inzicht in vaardigheden voor risico-leiderschap als leider van eigen informatieveilig gedrag

- *Dit interview is bestemd voor een respondent expaire met kennis van informatieveiligheid en een respondent van bedrijfsvoering die betrokken bij het verwerken van informatie.*
- *Het interview uitvoeren door de onderzoeker op kantoor. Als dit door omstandigheden niet mogelijk is via Microsoft Teams.*
- *Het is een semi-gestuurd interview waardoor de mogelijkheid bestaat verdiepingsvragen te stellen om het doel van het onderzoek te bereiken.*
- *Het interview vindt plaats op vrijwillige basis en de geïnterviewde is geïnformeerd over de doelstellingen van het onderzoek.*
- *De Ethische code van universiteit van Twente en de privacyrichtlijnen van de VRLN zijn van toepassing.*
- *Het interview is anoniem, de naam en functie worden niet gepubliceerd.*
- *Het interview wordt opgenomen en getranscribeerd voor kwalitatieve analyse.*
- *Het interview duurt maximaal een uur.*

<u>Vragen:</u>

1. Inleiding
   - Bedanken voor deelname.
   - Bedankt voor uw medewerking aan dit onderzoek naar veerkrachtig informatieveiligheid.
   - U heeft deelgenomen aan de enquête over het informatieveiligheidsgedrag. Dit interview heeft als doel evaluatie enquête en inzicht in vaardigheden voor risico-leiderschap als leider van eigen informatieveilig gedrag. Met de resultaten, en dus ook uw feedback, kijken we naar de relevantie van de enquête over gedrag.
   - Daarnaast heeft u het verzoek om de digitale enquête over vaardigheden risicoleider in te vullen.
   - Het geheel is op vrijwillige basis en bedoeld voor de studieopdracht en probleem in de organisatie.
   - Vindt u het goed dat ik het opneem om het verder te kunnen uitwerken. U krijgt de uitwerking te zien.
2. Wie is de geïnterviewde
   a. Wat is uw functie en relatie met informatieveiligheid(gedrag) (professional)
   a. Ben u bekend met de governance van informatieveiligheid van de VRLN en haar methodiek?
3. Oorzaken van informatieveiligheidsincidenten. (deelvraag 2)
   a. Wat zijn op dit moment volgens u (de top 3) oorzaken van informatieveiligheidsincidenten?
   b. Hoe zijn de medewerkers/gebruikers in de preventie meegenomen?
   c. Op welke manier is het informatiebeleid binnen de VRLN geregeld en waar is het te vinden?
4. Enquête informatieveiligheidsgedrag? (deelvraag 2 en 3)

   De enquête bestond uit 8 aandachtsgebieden met gedrag, houding en kennis vragen.
   - Authenticatiemiddel
   - Email gebruik
   - Internetgebruik
   - Social media gebruiken
   - Mobiele apparaten
   - Informatieverwerking
   - Melden van incidenten
   - Omgang privacy

   d. Zijn de 8 aandachtsgebieden volgens u relevant voor het meten van het informatieveiligheidsgedrag?
      I. Welk aandachtsgebied is volgens u van het grootste belang? Inkleuren bolletje
      II. Welk aandachtsgebied is volgens u van het minste belang? Kruis door het bolletje
   e. Zijn de vragen duidelijk verwoord in de context van de organisatie (VRLN, Gezondheidszorg en brandweer)?

5. De volgende vragen gaan over de zeven algemene vragen over preventiemogelijkheden, betrokkenheid organisatie en medewerkers zijn gesteld: (deelvraag 2 en preventie)

   a. Welke preventiemogelijkheden zou het meest relevant vinden voor de VRLN?
   b. Hoe kan volgens u de organisatie de betrokkenheid motiveren? (deelvraag 3)
6. Hoe realistische en relevant is deze meetmethode ? (deelvraag 2 en discussie)
   a. Is de enquête voor informatieveiligheidsgedrag naar uw mening compleet?
   b. Is de enquête voor informatieveiligheidsgedrag betrouwbaar en waarom?
7. Risico-leiderschap: tweede enquête (deelvraag 3 en discussie)
   Risico eigenaarschap door risicoleiderschap van medewerkers voorinformatieveiligheid. 20 vaardigheden.
   a. Hoe ziet u het eigenaarshap (zelf verantwoordelijk zijn) van medewerkers?
   b. Welke vaardigheden zijn nodig van de organisatie voor de medewerker.
   c. Welke vaardigheid/actie vindt u het belangrijkste om op te pakken?
8. Afronding
   a. Heeft u nog vragen
   b. Dank u voor de deelnamen?
   c. Verloop van het verder onderzoek aangeven?

Bijlage E: Analyse nulmeting aandachtsgebieden

Niet openbaar

Bijlage F: Vaardigheden van risicogestuurd leiderschap informatieveiligheidsgedrag

Onderstaand vaardigheden die nodig zijn voor iedereen risicoleider die zijn overgenomen van het boek iedereen risicoleider (van Staveren, 2018, P341-346,2020) en op enkele punten aangepast voor het informatieveiligheidsgedrag als risicoleider.

1. Maakt doelen leidend: doelverantwoordelijk.
    1) Bekijk doelen in de volle breedte.
    2) Onderscheidt doelen van wensen.
    3) Formuleert doelen aantrekkelijk en realistisch.
    4) Maakt onderscheidt tussen doelen in verschillende organisatieniveaus, inclusief de bijbehorend risico's.

2. Kan omgaan met meerdere en mogelijk conflicterende doelen.
    1) Erkent de realiteit van meerdere doelen.
    2) Erkent de realiteit van conflicterende doelen.
    3) Maakt expliciete afwegingen voor maatregelen, vanuit doelen en gevolgen.
    4) Gebruikt risicosturing om problemen of aandachtspunten met doelen op te lossen.
    5) Gebruikt de risicosturing als middel als doel.

3. Waarde dominantie bepalen: Relatie leggen tussen kosten en (subjectieve) waarde in relatie tot de risico's.
    1) Kent het verschil tussen kosten en waarden in relatie tot het risico's.
    2) Neemt risico's met gevolgen die niet eenduidig in geld zijn uit te drukken wel serieus.
    3) Waarde voor iedereen in het risico.
    4) Kan omgaan met subjectiviteit van de waarde in het risico.
    5) Beseft de waarde en rol van tijd bij het omgaan met risico's.

4. Positief benaderen en gebruiken van veerkracht in variatie als standaard.
    1) Beseft dat effectief omgaan met risico's flexibiliteit en wendbaarheid vereist.
    2) Hanteert in principe maatwerk voor omgaan met risico's.
    3) Zoekt het optimum tussen standaardisatie en variatie.
    4) Houdt accreditaties en certificeringen beperkt en werkbaar.

5. Een risicoleider gebruikt variatie als vertrouwen van informatieveiligheidsgedrag.
    1) Gebruikt bewust de verschillen en veranderingen.
    2) Benut de kracht van variatie.
    3) Betrekt betrokkenen bij het omgaan met risico's
    4) Is kritisch positief.
    5) Stelt groepsdenken aan de orde en past teamleren toe-> Samen

6. Is een risico-eigenaar als risicoleider. High trust-Low tolerance leren.
    1) Risico-leiderschap vanuit doelverantwoordelijkheid.
    2) Risicosturing opgenomen in functieprofielen en – gesprekken.
    3) Houdt zich aan risicoafspraken en wijkt ervan af als de situatie erom vraagt.
    4) Is zelf risico-leiderschap en neemt verantwoordelijkheid.

7. Taakgericht vanuit de functie-omvang voor effectief omgaan met risico's.
    1) Stemt de inspanning voor risicosturing af op de omvang van de organisatie.
    2) Gebruikt risicosturing.
    3) Bespreekt de relevante risico's en maatregelingen in bestaande overleggen.
    4) Rapporteert en beoordeeld.

8. Gaat vanuit positief gedrag en vertrouwen om met risico's.
    1) Heeft en positieve houding voor informatieveilig te werken in de werkomgeving.
    2) Organiseert de combinatie van intentie en vakmanschap. (houding en kennis)
    3) Staat afwijkingen van regels toe mits noodzakelijk en achteraf gemotiveerd.
    4) Spreekt mensen aan op en grijpt (als vertrouwen wordt geschonden)

9. Keuze voor risicogestuurd werken vanuit de kracht van overtuiging als kans. Van oplossingen naar het oplossend vermogen.
    1) Benut de kracht van overtuigingen.
    2) Overtuigt met de combinatie ratio en emotie
    3) Gebruikt de juiste techniek voor benaderen (bv storytelling)
    4) Heeft kennis en werkt op een risicogestuurde wijze.
    5) Geeft zelf het goede voorbeeld, door zelf risicosturing toe te passen.

10. Onzekerheden toelaten door veerkrachtig om te gaan met risico's.
    1) (H)erkent de belangrijkste onzekerheden
    2) Beseft de illusie dat een risicodossier niet volledig is.
    3) Doorbreekt de objectieve illusie van risicoanalyse.

4) Beseft dat een volledige risicobeheersing een illusie is.
5) Organiseert mede resilience(veerkracht) om optredende risico's te incasseren.

11. Is moedig door risico's als kansen te zien en keuzes durven te maken..
    1) Weet wat de visie en missie betekend.
    2) Werkt met kaders vanuit principe en waarden.
    3) Maakt een krachtig risicobereidheid.
    4) Ontwikkeld de moed.

12. Een risicoleider geeft beperkingen aan van of voor het (risico)onderzoek.
    1) Ontleden van een risico.
    2) Kan het verschil van wanneer een wel of niet te verkleinen van een onzekerheid.
    3) Stelt vast wat aannames, feiten en interpretaties zijn.
    4) Is alert op de betrouwbaarheid van (risico-)informatie.
    5) Doet geen of beperkt onderzoek naar een risico.

13. Risicosturing in een cyclisch proces toepassen
    1) Is bekend met de zes stappen voor risicosturing
    2) Weet dat de zes risicostappen effectief zijn.
    3) Is zelf al begonnen met het toepassen van den zes stappen.
    4) Kan de zes risicostappen integreren in de bestaande processen en PDCA.

14. Leren van kansen door te doen.
    1) Weet dat de standaardmethode voor omgaan met risico's niet bestaat.
    2) Doet(start) en betrekt anderen.
    3) Experimenteert met risicosturing.
    4) Leert van risicosturing, vanuit overtuigingen
    5) Benut de kracht van actie.

15. Ontwikkelen vanuit dynamiek.
    1) Erkent de risicodynamiek
    2) Beschouwt de risicoclassificaties als momentopnames.
    3) Benut het principe als houvast.
    4) Evalueert risicosturing in een ritme.
    5) Organiseert een bepaalde flexibiliteit: risk agility

16. Ziet de interactie in een risicobeoordeling: oorzaak x gevolg-> risico's.
    1) Weet wat wilde en tamme vraagstukken zijn met de bijbehorende risico's.
    2) Doorziet interacties tussen oorzaak, gevolg van risico's.
    3) Ziet de doelen, de oorzaken en gevolgen met de bijbehorende interacties.
    4) Ziet de interacties tussen de verschillende risico's.

17. Kansen voor veerkracht door kleine verspilling toe te laten (op korte en lange termijn voor risico's).
    1) Kent en ziet het verschil tussen efficiëntie en effectiviteit.
    2) Let op met lean en verbindt lean met risicosturing.
    3) Overziet hoe kleine besparingen tot groet verspillingen mogelijk leiden en visa versa.
    4) Doorziet de relatie tussen risicosturing op korte en lange termijn.
    5) Benut kleine verspillingen voor veerkracht en weerbaarheid.

18. Het zien en opmerken van kleine afwijkingen en relativeren om te leren. Beperkingen accepteren
    1) Herkent afwijkingen en relativeert fouten in de dagelijkse praktijk.
    2) Kijkt en luistert met aandacht.
    3) Toetst systeem: 1) denken met systeem en 2) denkers.
    4) Neemt tijdig een time-out. Relativeert
    5) Ontwikkeld mentale fitheid.

19. Effectrisico's intern en extern omgeving reduceren.
    1) Begrijpt het onderscheidt tussen kansreductie en gevolgreductie. Crisismanagement
    2) Doorziet de prijs van effectrisico's en kanseffecten.
    3) Beschouwt gevolgreductie als kans.
    4) Noodzaak van effectrisico's beoordelen.
    5) Benut technologie en omgeving voor gevolg- en kansreductie.

20. Onzekerheden als continue krachtbron voor kansen en vragen stellen (Vragen stellen boven antwoorden).
    1) Stelt verschillende soorten vragen in een sociaal veilige omgeving.
    2) Kan de socratische dialoog toepassen.
    3) Beseft dat domme vragen en antwoorden niet bestaan.
    4) Behoedt zich voor het overschatten van de eigen competenties.
    5) Benut het niet zekerweten.
    6) Als continue krachtbron