THE HUMAN FIREWALL OF BEHAVIORAL INFORMATION SECURITY

Radboud Universiteit Nijmegen
Master Thesis Informatiekunde
November 2008

Auteurs:	Michiel Dam en Kevin Wessels
Afstudeernummers:	83 IK en 84 IK
Eerste begeleider:	Prof. dr. B.P.F. Jacobs
Tweede begeleider:	Drs. G.P.A. Bergers
Eerste Referent:	Dr. P.J. van Rossum
Tweede Referent:	Prof. dr. E. Barendsen

VOORWOORD

Zoals de Engelse titel kan doen vermoeden gaat dit onderzoek in op het onderwerp informatiebeveiliging en het gedrag dat mensen vertonen ten aanzien hiervan. Hierbij staat het gedrag van de mens ten aanzien van informatiebeveiliging centraal. Kan de mens met betrekking tot informatiebeveiliging een "human firewall" zijn of is hij zo lek als een mandje? Verder is het gedrag van mensen verder toegespitst op personen die actief zijn binnen de arbeidsorganisatie. Het betreft hier arbeidsgedrag van individuen die onderworpen zijn aan beleid, richtlijnen, voorschriften en procedures vanuit de organisatie. Hierdoor vormt het gedrag van deze individuen de doorslaggevende factor voor het succes of het falen van de informatiebeveiliging. Dit samen met de interesse voor de onderzoeksgebieden arbeids- en organisatiepsychologie en informatiebeveiliging die wij[1] hebben, heeft ertoe geleid dat dit onderzoek tot stand is gekomen. Een stuk van het resultaat is hier in de vorm van een scriptie verwoord. Op deze manier hebben wij een zelfstandige wetenschappelijke bijdrage willen leveren.

Met het afronden van de laatste zinnen voor deze scriptie komt er niet alleen een einde aan een bevlogen afstudeeronderzoek van bijna een jaar, maar ook aan het schrijfproces, de studie Informatiekunde aan de Radboud Universiteit Nijmegen, de samenwerking tussen ons, de dagenlange Skype gesprekken over van alles en niets en een avontuurlijke ontdekkingsreis zoals wij het hebben ervaren.

Ons avontuur begon in november 2007 bij een bezoek aan het Nobiles Careerevent in Utrecht. Met de planning van een afstudeeronderzoek voor ogen en de interesse voor de onderzoeksgebieden arbeids- en organisatiepsychologie en informatiebeveiliging, gingen we op zoek naar organisaties die ons zouden kunnen helpen bij een surveyonderzoek. De zoektocht in Utrecht leverde vier potentiële kandidaten op: Laurens Simonse Groep, NS, Corus en Capgemini. Onze eerste twee bedrijfsbezoeken vonden plaats bij de Laurens Simonse Groep en de NS. Hier kwamen we al snel tot de conclusie dat een eventuele samenwerking met één van beide organisaties voor ons niet tot de gewenste resultaten zou leiden. Vervolgens kregen we begin januari 2008 bericht van Corus met daarin een enthousiast verhaal over het bewustzijn en gedrag van medewerkers ten aanzien van informatiebeveiliging. Het schrijfproces was vanaf dat moment begonnen. Snel na het bericht van Corus hadden we ons eerste bedrijfsbezoek in IJmuiden. Tegelijkertijd gingen we op zoek naar een begeleider voor het onderzoek. Onze eerste gedachte ging uit naar Erik Proper, aangezien hij ons ook had begeleid bij het onderzoek naar business rules ten aanzien van informatiebeveiliging. Al snel kwamen we bij de Digital Security onderzoeksgroep van Bart Jacobs uit. In eerste instantie had Bart niet veel tijd om het onderzoek te begeleiden. Gaandeweg groeide zijn belangstelling en vertrouwen in het onderzoek. De gesprekken in Nijmegen en IJmuiden liepen op dat moment dwars door elkaar heen. 's-Ochtends een afspraak bij Corus en 's-middags een afspraak op de Radboud Universiteit was geen uitzondering. Tijdens het eerste bedrijfsbezoek bij Corus hadden we een positief gesprek met Peter van Boxtel over een mogelijke samenwerking. Al snel waren we het eens over het onderzoeksdoel en moesten we op korte termijn een appartement zoeken in de omgeving van IJmuiden. Midden februari begon het avontuur in IJmuiden met op de eerste dag een veiligheidstoets en een rondleiding over het terrein van Corus. Na een aantal dagen begonnen we echter te twijfelen aan de mogelijkheden en eventuele resultaten bij Corus. Na overleg met alle betrokken partijen hebben we gezamenlijk besloten om ons onderzoek voort te zetten in Nijmegen. Via Bart Jacobs kwamen we in contact met de politie regio Gelderland-Zuid. Daarnaast kregen we uit onverwachte hoek ook bericht van Capgemini. Aan beide partijen hebben we onze onderzoeksplannen

[1] Wanneer er gesproken wordt over we, wij, ons, onze, onderzoekers of auteurs wordt er gerefereerd aan de auteurs van deze scriptie, te weten Michiel Dam en Kevin Wessels.

voorgelegd. Binnen no-time reageerde Capgemini met een uitnodiging om te komen praten met Alina Stan van de afdeling TTU binnen Capgemini. Tijdens het gesprek werd snel duidelijk dat wij alle vrijheid zouden krijgen ten aanzien van het uit te voeren onderzoek. Helaas liet de reactie van de politie regio Gelderland-Zuid langer op zich wachten, waarop wij na overleg met Bart Jacobs besloten in zee te gaan met Capgemini. Vanuit Capgemini was Marco Plas onze gesprekspartner en aanspreekpunt voor zaken die betrekking hadden op het uitzetten van de vragenlijst. Naarmate het onderzoek steeds meer vorm kreeg kwamen we tot de conclusie dat niet alle benodigde kennis voorhanden was binnen de Digital Security onderzoeksgroep. Om toch de benodigde kennis en begeleiding te vinden, is binnen de Radboud Universiteit Nijmegen de samenwerking gezocht met de sociale wetenschappen. Zo kwamen we bij Gerard Bergers terecht. Hij was ons aanspreekpunt voor alles wat met sociaalwetenschappelijke aspecten te maken had. Naast alle organisatorische aspecten van dit onderzoek is er ook veel energie gestoken in het operationele vlak. Zo is het uitzetten van de vragenlijst en het benaderen van honderden mensen binnen het bedrijfsleven een complexe lobby en tijdsintensieve bezigheid gebleken. Voor de faciliteiten ten aanzien van de vragenlijst was de samenwerking gezocht met Computer & Communicatiezaken (CNCZ). Hierbij ging het tijdens de pilot-vragenlijst niet altijd even vlekkeloos, maar bij de hoofdvragenlijst ging de uitzet zonder problemen.

Het vormgeven van het onderwerp en onderzoek ging niet zonder slag of stoot. We hebben bij dit afstudeeronderzoek veel gezien, gelezen, gehoord en gesproken over de onderzoeksgebieden informatiebeveiliging en gedragswetenschappen. Het ontwikkelen van een meetinstrument vanuit de sociale wetenschappen en het uitzetten en analyseren hiervan hebben we als de grootste uitdaging gezien. Dit komt vooral doordat het onderwerp zich voor ons op een onbekend terrein bevond, waarin nog veel onzekerheden en risico's aanwezig waren. De verdeling van de kennisgebieden was 80% gamma-wetenschappen en 20% bèta-wetenschappen. Maar ondanks deze verdeling hebben wij hier toch mee weten om te gaan. Hierbij is er zonder vooroordeel en met een kritische blik gekeken naar de beschikbare theoretische concepten en empirische voorhanden zijnde conclusies. De termen gedrag, bewustzijn en informatiebeveiliging zijn onafhankelijk van elkaar relatief simpel uit te leggen, maar zodra deze gecombineerd worden, ontstaat er iets dat vreemd en onverklaarbaar aandoet. Wij hebben getracht enige duidelijkheid te verschaffen in dit onderzoeksterrein, wat voor ons als *behavioral information security* bekend staat. Middels veldonderzoek hebben we laten zien wat de invloed is van termen zoals attitude of kennis op het gedrag ten aanzien van informatiebeveiliging. Deze termen die vanuit het vakgebeid informatiebeveiliging worden onderkend, zijn vanuit dit vakgebied nooit onderzocht.

Dit onderzoek was uiteraard niet mogelijk geweest zonder de medewerking van tal van mensen. Via deze weg willen wij graag een aantal mensen persoonlijk bedanken voor hun inzet, belangstelling en enthousiasme. Het eerste dankwoord gaat uit naar prof. dr. Bart Jacobs, die het onderzoek vanaf het eerste moment letterlijk en figuurlijk heeft zien groeien. Zijn mening en kritische blik op het onderzoek was waardevol, alsook zijn toenemende belangstelling en vertrouwen in ons. Helaas was de begeleiding op dit vrij onontgonnen gebied vakinhoudelijk wat summier. Desondanks waren er altijd goede kritische gesprekken waarbij gelukkig ook altijd iets was om over te lachen. Daarnaast willen we dr. Peter van Rossum en prof. dr. Erik Barendsen bedanken voor hun rol als referent bij dit onderzoek en voor een luisterend oor op de wandelgangen. Het dankwoord voor de ondersteuning en begeleiding voor de sociaalwetenschappelijke aspecten is voor drs. Gerard Bergers en drs. Rinske de Graaff Stoffers, aangezien het grootste deel van het onderzoek zich afspeelde op het terrein van de gamma-wetenschappen. Voor de faciliteiten vanuit Capgemini Nederland B.V. willen we drs. Marco Plas bedanken. Voor de samenwerking vanuit CNCZ willen we drs. Remco Aalbers bedanken. Verder willen we iedereen danken die de vragenlijst mede hebben uitgezet binnen zijn of haar netwerk. We willen elkaar bedanken voor de uitzonderlijke samenwerking middels moderne communicatie, zoals MediaWiki en Skype, om dit onderzoek mogelijk te maken. Hierbij waren vele verhitte discussies over hoe bepaalde concepten en theorieën er uit zouden moeten zien, maar ook

vele momenten van overeenstemming. Voor het aanhoren van de dagelijkse beslommeringen willen we Ankie Clement, Sarah-Jane Maytum en onze ouders bedanken. Een laatste dankwoord gaat uit naar Hans Clement, die tijdens het schrijfproces urenlang tal van teksten heeft gecontroleerd. Een ondankbare en tijdsintensieve taak die niet onbeloond voorbij kan gaan. Bedankt voor het scherpe taalinzicht.

Als laatste willen wij dit onderzoek opdragen ter nagedachtenis aan Anne-Marie Clement-Venrooij en Herman Junier die beiden dit jaar overleden zijn aan de gevolgen van kanker. Anne-Marie is de moeder van Ankie Clement, de vriendin van Michiel Dam. Herman Junier is de peetoom van Kevin Wessels.

Michiel Dam en Kevin Wessels

Sint-Oedenrode / Wijchen, 2008

SAMENVATTING

In dit onderzoek is het gedrag van een medewerker beschouwd als de centrale factor die de kwaliteit van de informatiebeveiliging binnen een organisatie bepaalt. Het uitgangspunt hierbij is de aard en de oorsprong van gedrag, die de basis vormt voor behavioral information security. De term behavioral information security wordt gebruikt om het gedrag aan te duiden dat medewerkers in organisaties (kunnen) vertonen ten aanzien van informatiebeveiliging. Middels een verkennend onderzoek van het vakgebied "informatiebeveiliging" kwam er een beeld naar boven, waarbij gedrag ten aanzien van informatiebeveiliging samengevat kan worden in drie aspecten: attitude, kennis en gedrag, die samen het informatiebeveiligingsbewustzijn vormen. Hierbij spelen informatiebeveiligingstrainingen en bewustwordingscampagnes een rol van betekenis, omdat die mogelijk het gedrag ten aanzien van informatiebeveiliging kunnen veranderen. Een inventarisatie van mogelijk wetenschappelijke empirische ondersteuning voor deze bevindingen was er niet. Zowel vanuit de gamma- als de bètawetenschappen is er zover wij hebben kunnen nagaan geen systematisch onderzoek verricht naar het gedrag ten aanzien van informatiebeveiliging.

Vanuit de sociale wetenschappen is er theorievorming waarmee mogelijk gedrag voorspeld en verklaard kan worden. Volgens de theorie van gepland gedrag die ontwikkeld is door Ajzen, wordt het menselijke gedrag geleid door drie determinanten: attitude toward the behavior (houding), subjective norm (norm vanuit de sociale omgeving) en perceived behavioral control (capaciteit en controle), die samen de intentie tot gedrag bepalen. Als algemene regel geldt dat, hoe positiever de drie determinanten samenhangen, hoe sterker de intentie van de persoon zal zijn, om het gedrag in kwestie uit te voeren. Als laatste wordt verwacht dat een persoon zijn intentie tot gedrag zal omzetten tot werkelijk gedrag, als de situatie zich voordoet en als er voldoende werkelijke controle is over het gedrag [AJZE91].

In dit onderzoek is er gekeken vanuit de theorie van gepland gedrag, om een verklarende en voorspellende uitspraak te kunnen doen over de gedragsintentie van medewerkers binnen organisaties in Nederland bij het beveiligen van en veilig omgaan met de informatievoorziening van zijn of haar organisatie. Hierbij is uitgegaan van de drie determinanten attitude toward the behavior, subjective norm en perceived behavioral control die individueel en samen de gedragsintentie beïnvloeden.

Middels een vragenlijst zijn data verzameld in de maanden augustus en september 2008. Deze data zijn verzameld middels de online vragenlijst applicatie: LimeSurvey. Hierbij is gebruik gemaakt van het HTTPS-protocol, gehost op een server van het CNCZ. De vragenlijst is uiteindelijk uitgezet onder tientallen organisaties. Hierbij varieerde het aantal medewerkers per organisatie van minimaal 2 tot meer dan 10.000. Per organisatie varieerde het aantal respondenten van 1 tot maximaal 40. Eerst zijn sponsoren binnen verschillende branches (hightech industrie, overige industrie, kennisintensieve dienstverlening en overige dienstverlening) gezocht. Dit zoeken naar sponsoren is geschied middels sociale netwerken, vakgroeporganisaties en alumni groepen. Er waren uiteindelijk 224 respondenten, waarvan er na data interpretatie 8 respondenten zijn verwijderd, omdat zij buiten de steekproef vielen. Dit gaf een betrouwbaarheidsniveau van 92% en een foutmarge van 6%. Het was onmogelijk om een response rate te bepalen, aangezien niet binnen elke organisatie de medewerking gelijkwaardig was. Er zijn 403 medewerkers die geklikt hebben op de link om de vragenlijst in te vullen, uiteindelijk hebben 224 respondenten ook daadwerkelijk de vragenlijst afgerond. Dit geeft een response van 55,6%. De werkelijke non-respons is echter niet te bepalen aangezien onbekend is hoe vaak de vragenlijst is uitgezet. De online vragenlijst was gebaseerd op de "theorie van gepland gedrag" toegespitst op gedrag ten aanzien van informatiebeveiliging. Hierbij zijn 177 items gebruikt die ontwikkeld zijn aan de hand van een meta-analyse vanuit de gamma- en bètawetenschappen. De focus van de items lag namelijk op de onderwerpen ***B***(eschikbaarheid) ***I***(ntegriteit) en

V(ertrouwelijkheid) van bedrijfsgegevens, back-up en wachtwoordgebruik. De items maken gebruik van een 5-punts Likert schaal, met schaalscores van 1 tot en met 5 en van -2 tot en met 2. De items gaan in op de volgende 4 constructen: de attitude toward the behavior, de subjective norm, de perceived behavioral control en de gedragsintentie ten aanzien van informatiebeveiliging.

Vervolgens zijn voor de drie hoofdonderwerpen bedrijfsgegevens, back-up en wachtwoordgebruik multipele regressieanalyses uitgevoerd. Uit de resultaten wordt geconcludeerd met betrekking tot de attitude toward the behavior dat een positieve of negatieve houding van een medewerker ten opzichte van de gedragsintentie om bedrijfsgegevens te beschermen, bedrijfsgegevens zeker te stellen en veilig om te gaan met wachtwoordgebruik de sterkst verklarende voorspeller is van de drie determinanten (attitude toward the behavior, subjective norm en perceived behavioral control). Hierbij zijn de volgende relaties gevonden. Naarmate een medewerker het verstandiger, nuttiger voor zichzelf en nuttiger voor anderen vindt om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoordgebruik, zullen ook de intenties om dit te doen toenemen. Naarmate een medewerker het prettiger vindt om zijn bedrijfsgegevens te beschermen, zal ook de intentie om dit te doen toenemen. Daarentegen heeft de moeilijkheidsgraad voor een medewerker om zijn bedrijfsgegevens te beschermen geen invloed op de intentie om dit te doen. Als laatste hebben de pleziergraad en de moeilijkheidsgraad voor een medewerker om zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoord ook geen invloed op de intenties om dit te doen. De bovenstaande relaties zijn in onderstaande tabel samengevat weergegeven.

Tabel 1
Samenvatting relaties attitude

	Beschermen bedrijfsgegevens	Zekerstellen bedrijfsgegevens	Veilig omgaan wachtwoordgebruik
Wijsheidsgraad	+	+	+
Pleziergraad	+		
Nuttigheidsgraad voor zichzelf	+	+	+
Moeilijkheidsgraad			
Nuttigheidsgraad voor anderen	+	+	+

Geconcludeerd wordt met betrekking tot de subjective norm dat de volgende relaties bestaan. Naarmate de invloed van wat belangrijke mensen[2] van een medewerker vinden dat hij moet doen en wat er van een medewerker verwacht wordt toeneemt om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoordgebruik, zullen ook de intenties om dit te doen toenemen. Naarmate de invloed van wat naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen toeneemt om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoordgebruik, zullen ook de intenties om dit te doen groter zijn dan de invloed van wat een direct leidinggevende van een medewerker vindt dat hij moet doen. Naarmate de invloed van wat naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen toeneemt om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoordgebruik, zullen ook de intenties om dit te doen groter zijn dan de invloed van wat naaste collega's, die belangrijk voor een medewerker zijn, zelf doen. Naarmate de invloed van wat belangrijke mensen van een medewerker zelf doen toeneemt om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoordgebruik, zullen de intenties om dit te doen

[2] Dit zijn referentiepersonen uit de omgeving van de medewerker, die voor hem of haar belangrijk zijn.

minimaal toenemen. Naarmate de invloed van wat belangrijke mensen van een medewerker vinden dat hij moet doen en wat er van een medewerker verwacht wordt toeneemt om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoordgebruik, zullen ook de intenties om dit te doen groter zijn dan de invloed van wat direct leidinggevende en naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen. Naarmate de invloed van wat naaste collega's, die belangrijk voor een medewerker zijn, zelf doen toeneemt om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoordgebruik, zullen ook de intenties om dit te doen groter zijn dan de invloed van wat belangrijke mensen van een medewerker zelf doen. De bovenstaande relaties zijn in onderstaande tabel samengevat weergegeven.

Tabel 2
Samenvatting relaties subjective norm

	Beschermen bedrijfsgegevens	Zekerstellen bedrijfsgegevens	Veilig omgaan wachtwoordgebruik
Wat belangrijke mensen van een medewerker vinden dat hij moet doen	+++	+++	+++
Wat er van een medewerker verwacht wordt	+++	+++	+++
Wat belangrijke mensen van een medewerker zelf doen			
Wat een direct leidinggevende van een medewerker vindt dat hij moet doen	+	+	+
Wat naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen	++	++	++
Wat naaste collega's, die belangrijk voor een medewerker zijn, zelf doen	+	+	++

Geconcludeerd wordt met betrekking tot de perceived behavioral control dat de volgende relaties bestaan. Naarmate een medewerker zelf meer kan ten aanzien van het beschermen van zijn bedrijfsgegevens, het zekerstellen van zijn bedrijfsgegevens en het veilig omgaan met zijn wachtwoord, zullen ook de intenties om dit te doen toenemen. Naarmate een medewerker zelf meer kan ten aanzien van het beschermen van zijn bedrijfsgegevens, het zekerstellen van zijn bedrijfsgegevens en het veilig omgaan met zijn wachtwoord, zullen ook de intenties om dit te doen groter zijn dan wat een medewerker denkt zelf te kunnen. Naarmate een medewerker denkt zelf meer te kunnen ten aanzien van het beschermen van zijn bedrijfsgegevens en het veilig omgaan met zijn wachtwoord, zullen de intenties om dit te doen *minimaal* toenemen. De bovenstaande relaties zijn in onderstaande tabel samengevat weergegeven.

Tabel 3
Samenvatting relaties perceived behavioral control

	Beschermen bedrijfsgegevens	Zekerstellen bedrijfsgegevens	Veilig omgaan wachtwoordgebruik
Wat een medewerker zelf meer kan	++	++	++
Wat een medewerker denkt zelf te kunnen	+	+	+

Geconcludeerd kan worden met betrekking tot de relatie tussen de attitude toward the behavior, subjective norm en perceived behavioral control ten aanzien van de drie gedragsintenties, dat met name de houding van een medewerker ten aanzien van de drie gedragsintenties de sterkst verklarende voorspeller van de drie determinanten (attitude toward the behavior, subjective norm en perceived behavioral control) is. Dit wil zeggen dat de houding van een medewerker de meeste invloed heeft op de intentie om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoord. Daarnaast zijn attitude toward the behavior en subjective norm de sterkst verklarende voorspellers voor de intentie van een medewerker om zijn bedrijfsgegevens te beschermen en veilig om te gaan met zijn wachtwoord. Dit wil zeggen dat de houding en de norm vanuit de sociale omgeving van een medewerker de meeste invloed hebben op de intentie om zijn bedrijfsgegevens te beschermen en veilig om te gaan met zijn wachtwoord. Als laatste zijn de attitude toward the behavior, subjective norm en perceived behavioral control alle drie sterke verklarende voorspellers voor de intentie van een medewerker om zijn bedrijfsgegevens zeker te stellen. Dit wil zeggen dat de houding, de norm vanuit de sociale omgeving, de capaciteit en de controle van een medewerker de meeste invloed hebben op de intentie om zijn bedrijfsgegevens zeker te stellen. De bovenstaande relaties zijn in onderstaande tabel samengevat weergegeven.

Tabel 4
Samenvatting relaties tussen attitude, subjective norm en perceived behavioral control

	Beschermen bedrijfsgegevens	Zekerstellen bedrijfsgegevens	Veilig omgaan wachtwoordgebruik
Attitude	+++	++	+++
Subjective norm	++	++	++
Perceived behavioral control	+	++	+

Ajzen stelt dat de *behavioral beliefs* gemedieerd worden middels de *attitude toward the behavior*, de *normative beliefs* gemedieerd worden middels de *subjective norm* en de *control beliefs* gemedieerd worden middels de *perceived behavioral control*. Uit de resultaten van dit onderzoek kan geconcludeerd worden dat er voor de drie determinanten: *attitude toward the behavior, subjective norm en perceived behavioral control* een gedeeltelijk of volledig mediatoreffect bestaat. Dit wil zeggen dat de theoretische relaties worden bevestigd door de empirische gegevens uit dit onderzoek.

Tot slot kan vanuit "training and awareness" en "organisatorische verplichting" geconcludeerd worden, dat deze een lage voorspellende waarde hebben voor de gedragsintenties van een medewerker om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoord.

ABSTRACT

In this research the behavior of an employee has been considered as the central factor which determines the quality of the information security within an organization. The starting point here is the nature and origin of behavior, which forms the basis for behavioral information security. The term behavioral information security is used to indicate behavior that employees might show with respect to information security. By means of exploratory research in the specialist field of "information security" a picture was formed where behavior with respect to information security can be summarized in three aspects: attitude, knowledge and behavior. Together these form information security awareness. Information security trainings and awareness campaign play an important role here, because these might change the behavior in relation to information security. There was no inventory of possible scientific empirical support for these findings. Both from the gamma- as the beta science there hasn't, as far as we know, been any systematic research done in behavior with respect to information security.

Within the social sciences there is a theory which says that possible behavior can be predicted and explained. According to the theory of planned behavior developed by Ajzen, human behavior is conducted by three determinants: attitude toward the behavior (attitude), subjective norm (norm from the social environment) and perceived behavioral control (capacity and control), that together determine the intention to behavior. As a general rule, the more positive the three determinants are connected to each other, the stronger the intention of the person will be to perform the behavior in question should the situation arise, and if there is sufficient real control over the behavior [AJZE91].

In this research with the theory of planned behavior in mind, we have looked to give an explanatory and prediction statement on the behavioral intention of employees within organizations in the Netherlands with respect to the protection and safe use of the information supply of its organization. The assumption is made regarding the three determinants; attitude toward the behavior, subjective norm en perceived behavioral control that have individual and combined influences on the behavioral intention.

By means of a questionnaire data was collected in the months August and September 2008. This data was collected by means of the online questionnaire application: LimeSurvey. Here, the HTTPS-protocol was used, hosted on a server of the CNCZ. The questionnaire was eventually distributed to a number of organizations. The number of employees in each organization varied from a minimum of 2 to more than 10,000. Per organization the number of respondents varied from 1 to a maximum of 40. First we searched for sponsors in different lines of business (hightech industry, other industry, knowledge intensive service and other service) by means of social networks, trade union organizations and alumni groups. There were eventually 224 respondents, of which 8 were removed following data interpretation, because they fell outside the random sample survey. This gave a reliability level of 92% and error margin of 6%. It was impossible to determine a response rate, since the level of collaboration within each organization differed. There were 403 employees who clicked on the link to fill in the questionnaire, and eventually 224 employees actually completed it, a response of 55.6%. However, it is not possible to stipulate the real non-response since it is unknown how many times the questionnaire was set out. The online questionnaire was based on the theory of planned behavior focused on behavior with respect to information security. Here, 177 items were used which were developed by means of an meta-analyze from the gamma- and the beta science. The focus of the items was on the subjects ***C***(onfidentiality) ***I***(ntegrity) ***A***(vailability) of company data, back-up and password use. The items make use of 5-punts Likert scale, with scale scores of 1 up to and including 5 and of -2 up to and including 2. The items look at the following 4 constructs: the attitude toward the behavior, the subjective norm, the perceived behavioral control and the behavioral intention with respect to information security.

Further, for the three main subjects; company data, back-up and password use, multiple regression analyses were implemented. From the results we have concluded, with regards to the attitude towards the behavior that a positive or negative attitude of an employee with respect to the behavioral intention to protect company data, to back-up company data and safe use of the password that the strongest explanatory predictor is of the three determinants (attitude toward the behavior, subjective norm and perceived behavioral control). Here, the following relationships were found. As an employee finds it more reasonable, more useful for himself and more useful for others to protect his company data, to back-up his company data and to use his password safely, the intentions to do this will also increase. As an employee finds it more pleasant to protect his company data, the intention to do this will also increase. On the other hand, the level of difficulty for an employee to protect his company data has no influence on the intention to do this. Finally, the pleasure level and the level of difficulty for an employee to back-up his company data and safely use his password, have no influence on the intentions do this. The above relations are summarized described in the table below.

Table 5
Summary relations attitude

	Protect company data	Back-up company data	Safe use of the password
Level of wisdom	+	+	+
Level of pleasure degree	+		
Level of usefullness for himself	+	+	+
Level of difficulty			
Level of usefulness for others	+	+	+

We conclude in relation to the subjective norm that the following relationships exist. With the increasing influence of what important people[3] think that an employee must do and what of an employee is expected to do with respect to the protection of his company data, to back-up his company data and the safe use of his password, the intentions to do this will also increase. As the influence of what close colleagues who are important for an employee think that he must do increases to protect his company data, to back-up his company data and safely to go with his password use, the intentions to do this will also be larger than the influence of what the direct management of an employee thinks that he must do. As the influence of what close colleagues who are important for an employee think that he must do increases to protect his company data, to back-up his company data and to safely use his password, the intentions to do this will also be larger than the influence of what close colleagues, who are important for an employee, himself does. As the influence of what important people of an employee themselves do increases to protect his company data, to back-up his company data and to safely use his password, the intentions to do this will have a *minimal* increase. As the influence of what important people of an employee think that he must do and what of an employee is expected to do increases to protect his company data, to back-up his company data and safely to go with his password use, the intentions to do this will also be larger than the influence of what the direct management and close colleagues, who are important for an employee, finds that he has to do. As the influence of what close colleagues, who are important for an employee, do increases to protect his company data, to back-up his company data and use safely his password, the intentions to do this will also be larger than the influence of what important people of an employee does himself. The above relations are summarized described in the table below.

[3] These people are reference points from the environment of the employee, that are for him or her important.

Table 6
Summary relations subjective norm

	Protect company data	Back-up company data	Safe use of the password
What important people think that an employee must do	+++	+++	+++
What of an employee is expected to do	+++	+++	+++
What important people of an employee themselves do			
What the direct management of an employee thinks that he must do	+	+	+
What close colleagues who are important for an employee think that he must do	++	++	++
What close colleagues, who are important for an employee, himself does	+	+	++

It is concluded in relation to the perceived behavioral control that the following relationship exists. As an employee himself can do more with regards to the protection of his company data, the back-up of company data and to use his password safely, also the intentions to do this will increase. As an employee himself can do more with respect to the protection of his company data, to back-up his company data and to use his password safely, also the intentions to do this will be larger than the influence of what an employee thinks he can do himself. As an employee thinks he can do more himself with respect to protecting his company data and to use his password safely, the intentions to do this will increase *minimally*. The above relations are summarized described in the table below.

Table 7
Summary relations perceived behavioral control

	Protect company data	Back-up company data	Safe use of the password
What an employee himself can do more	++	++	++
What an employee thinks he can do himself	+	+	+

It can be concluded with respect to the relationship between the attitude towards the behavior, subjective norm and perceived behavioral control and with respect to the three behavioral intentions, that particularly the attitude of an employee in relation to the three behavioral intentions is the strongest explanatory predictor of the three determinants (attitude toward the behavior, subjective norm and perceived behavioral control). That is to say that the attitude of an employee has the most influence on the intention to protect his company data, to back-up his company data and to use safely his password. Further, attitude toward the behavior and subjective norm are the strongest explanatory predictors for the intention of an employee to protect his company data and to safely use his password. That is to say that the attitude and the norm from the social environment of an employee have the most influence on the intention to protect his company data and to safely use his password. Finally, the attitude toward the behavior, subjective norm and perceived behavioral control are all strong explanatory predictors for the intention of an employee to back-up his company data. This is to say that the attitude, the norm from the social environment, the capacity and the control of an employee have the most influence on the intention to back-up his company data. The above relations are summarized described in the table below.

Table 8

Summary relations between attitude, subjective norm en perceived behavioral control

	Protect company data	Back-up company data	Safe use of the password
Attitude	+++	++	+++
Subjective norm	++	++	++
Perceived behavioral control	+	++	+

Ajzen suggests that the *behavioral beliefs* are mediated by means of the *attitude toward the behavior*, the *normative beliefs* are mediated by means of the *subjective norm* and the *control beliefs* are mediated by means of the *perceived behavioral control*. From the results of this research we can conclude that for the three determinants: *attitude toward the behavior, subjective norm en perceived behavioral control* a partial or complete mediator effect exists. This is to say that the theoretical relations are confirmed by the empirical data from this research.

Finally, it can be concluded from "training and awareness" and "organizational commitment" that these have a low prediction value for the behavioral intentions of an employee to protect his company data, to back-up his company data and to safely use his password.

INHOUDSOPGAVE

1. PROBLEEMSTELLING

1.1 Aanleiding

In dit onderzoek naar informatiebeveiliging staat het individuele gedrag van medewerkers[4] in organisaties centraal. Hierbij wordt informatiebeveiliging opgevat als een vorm van gedrag. Bepaalde gedachtengangen of redeneringen spelen een rol in beslissingen van medewerkers om wel of niet veilig en beveiligd met bedrijfsgegevens om te gaan. Welke dit zijn, zal onderzocht worden in dit onderzoek.

Stanton e.a. noemen de term *behavioral information security* voor het eerst in [STAN03b]. Deze term omvat: *Work Motivation + Personnel Psychology + Focus on Security*. Hierin wordt een koppeling gelegd tussen gedrag en informatiebeveiliging. De uiteindelijke omschrijving van behavioral information security is als volgt:

In exploring behavioral information security we are trying to understand the nature and origins as a basis for providing practical and principled approaches for increasing information security while respecting employee rights and preferences. [STAN06]

Vanuit deze benadering kan het gedrag van een medewerker gezien worden als de centrale factor die de kwaliteit van de informatiebeveiliging binnen een organisatie bepaalt. Het uitgangspunt hierbij is de aard en de oorsprong van gedrag, die de basis vormt voor behavioral information security. In dit onderzoek wordt de term behavioral information security gebruikt om het gedrag aan te duiden wat medewerkers in organisaties (kunnen) vertonen ten aanzien van informatiebeveiliging.

La Société Générale, de op een na grootste bank van Frankrijk, die het slachtoffer is geworden van de grootste bankfraude aller tijden, zal gebruikt worden als startpunt binnen dit onderzoek. Dit om duidelijk te maken hoe behavioral information security binnen dit onderzoek gepositioneerd is. De fraude die de Franse bank begin dit jaar 4,9 miljard euro kostte, was mogelijk doordat de Franse effectenhandelaar Jerome Kerviel applicatiecontroles en controleprocedures omzeilde en onklaar maakte. Hierdoor kon dit "informatiebeveiligingsincident" deze omvang krijgen[5]. De informatiebeveiliging van La Société Générale heeft hier gefaald. Er waren namelijk onvoldoende maatregelen genomen om de betrouwbaarheid van de informatievoorziening te waarborgen. Hierdoor kon Kerviel met behulp van een constructie met fictieve transacties zijn posities verbergen[6]. Met als gevolg dat Kerviel ongeautoriseerde transacties in de informatievoorziening kon verwerken en zo ongeoorloofde speculaties op de future markt kon verwezenlijken.

Dit is één van de vele voorbeelden, waarbij bepaalde handelingen van individueel gedrag hebben geleid tot (een) informatiebeveiligingsincident(en), waardoor er veel schade is ontstaan. De mogelijke intentie van Kerviel's handelen was om zoveel mogelijk winst te verkrijgen voor La Société Générale. Dit deed Kerviel door applicatiecontroles te omzeilen en onklaar te maken. Zo wilde Kerviel uiteindelijk laten zien dat hij een goede handelaar was en een riante bonus te krijgen. Helaas pakte dit voor hem, maar vooral voor La Société Générale, verkeerd uit en werd grote winst omgezet in groot verlies en status werd omgezet in minachting en beschuldiging. Als men kijkt naar het handelen van

[4] Hierbij worden die medewerkers bedoeld waarbij spraken is dat zij tot de eindgebruikers behoren binnen een organisatie.

[5] http://www.nu.nl/news/1409535/32/rss/%27Kerviel_gokte_met_50_miljard_euro%27.html

[6] http://www.demorgen.be/dm/nl/990/Home/article/detail/145429/2008/01/24/Grootste-bankfraude-aller-tijden-ontdekt-in-Frankrijk.dhtml

Kerviel, dan vormde hij een 'insider threat'. Volgens Jacobs is het een feit dat veel informatiebeveiligingsincidenten veroorzaakt worden door insiders[7] [JACO07]. Bijna zeventig procent van alle incidenten op het gebied van informatiebeveiliging kunnen geheel of gedeeltelijk aan menselijk falen worden toegeschreven [BIBE07]. Mitnick geeft aan dat hij meer gegevens heeft verkregen door menselijk falen dan middels technische inbraken [MITN02].

Uit het bovenstaande concluderen de auteurs van dit onderzoek, dat het gedrag van Kerviel ten aanzien van informatiebeveiliging een relevant en niet opzichzelfstaand probleem is binnen organisaties. Maar waardoor ontstaat dit soort gedrag? Wat is de aard en de oorsprong van het gedrag zoals Kerviel dat vertoonde? Om een mogelijk antwoord hierop te geven, kan gekeken worden in de literatuur van het vakgebied van de informatiebeveiliging. Jentjes en de Graaf spreken over het "gewenste" en "werkende" niveau van informatiebeveiliging, dat te bereiken is door medewerkers zich bewust te laten zijn van hun rol binnen informatiebeveiliging. Dit bewustzijnsniveau kan volgens Jentjes en de Graaf worden bereikt door de kennis, de houding en het gedrag van de medewerkers te veranderen, middels leren als instrument [JENT04]. Maar betekent dit in het geval van Kerviel dat hij te weinig had geleerd, een negatieve houding had ten opzichte van La Société Générale en zijn gedrag onwenselijk was om het "gewenste" en "werkende" niveau van informatiebeveiliging te bereiken of was het toch iets anders? Kerviel had redelijk wat kennis vergaard over de controleprocedures. Daarnaast is er geen duidelijke aanleiding om aan te nemen dat zijn houding tegenover La Société Générale en haar informatiebeveiliging negatief was. Dat het gedrag van Kerviel niet wenselijk was, is duidelijk, maar het gaat juist om gedrag. Dus om nu te stellen dat het bewustzijnsniveau bereikt kan worden door gedrag, is nogal triviaal. Maar houdt het "gewenste" en "werkende" niveau van informatiebeveiliging niet per definitie in dat medewerkers niet meer kunnen falen? En wanneer is het "gewenste" en "werkende" niveau van informatiebeveiliging bereikt? Is dat wanneer er geen informatiebeveiligingsincidenten meer plaats vinden? Hierop geven de schrijvers naar de mening van de auteurs van dit onderzoek geen concrete antwoorden.

Naast kennis, houding en gedrag voegt Basten daar nog de beïnvloeding vanuit de omgeving aan toe [BAST03]. De omgeving is echter alles, waardoor het volledig onduidelijk wordt wat er nu precies wordt bedoeld. Kruger en Kearney meten op basis van de aspecten attitude, kennis en gedrag het informatiebeveiligingsbewustzijn [KRUG06]. Maar kan het bewustzijn[8] ten aanzien van informatiebeveiliging wel meten aan de hand van de aspecten attitude, kennis en gedrag? Praat geeft aan dat het management en de beveiligingsfunctionarissen zodanige omstandigheden moeten creëren dat medewerkers zorgvuldig omgaan met informatiebeveiliging. Het belangrijkste hierbij is het stimuleren van het informatiebeveiligingsbewustzijn bij de medewerkers zelf. Het gaat er voornamelijk om dat de medewerkers gewezen worden op de risico's die het gevolg kunnen zijn van onzorgvuldig omgaan met informatie [PRAA02]. Heeft in het geval van Kerviel het management en de beveiligingsfunctionaris gefaald om omstandigheden te creëren die bijdragen aan het zorgvuldig omgaan met informatie en is er niet voldoende gewezen op de risico's die het gevolg kunnen zijn van onzorgvuldig omgaan met informatie?

---

[7] Spee stelt dat men gemakkelijk de begrippen 'insider' en 'insider threat' gebruikt zonder daarvan een definitie te geven. Het is niet zonder reden om dat te doen, organisaties bestaan immers niet (meer) zwart-wit uit insiders en outsiders. Daarom zal in dit onderzoek de werkdefinitie van Spee deels worden aanhouden: *Een insider is iemand met wie een organisatie een formele werkrelatie heeft, waarbij sprake is van overeengekomen rolverwachtingen, een bewust gekozen functietoekenning en die een daarvan afgeleide toegang heeft tot delen van de technische en logische infrastructuur en van wie verwacht wordt dat hij zich aan de geschreven en algemeen aanvaarde ongeschreven regels van de organisatie houdt* [SPEE04]. In dit onderzoek is er sprake van een insider threat als de insider regels bewust of onbewust overtreedt en daarmee de organisatie met of zonder opzet schaadt.

[8] Bewustzijn is het momentane besef van externe of interne stimuli, wat voorwerpen in de omgeving kunnen zijn (externe stimuli) en lichaamsgewaarwordingen, herinneringen, gevoelens of gedachten (interne stimuli). [ROED98]

Killmeyer stelt dat een informatiebeveiligingsbewustwordingscampagne het meest significante element is bij het inrichten van een informatiebeveiligingsproces [KILL06]. Waarom dit zo is en waarom er niets anders mogelijk is, wordt echter niet duidelijk. Het Information Security Forum en de National Institute of Standards and Technology hebben een reeks van publicaties uitgegeven waarin bewustwordingscampagnes, trainingen voor informatiebeveiliging en het meten van informatiebeveiligingsbewustzijn worden beschreven [INFO91], [INFO93], [INFO00], [INFO02], [NIST98], [NIST03]. De nadruk ligt hier vooral op richtlijnen en raamwerken omtrent trainings- en bewustwordingscampagnes voor informatiebeveiliging en het meten van het niveau en de effectiviteit van het informatiebeveiligingsbewustzijn. Er wordt niet duidelijk en overtuigend uitgelegd waarom nu juist deze zaken van belang zijn. De ISO standaard 27002 geeft aan dat het hebben van een gepast bewustzijnsniveau en het geven van training en opleiding aan medewerkers een kritieke succes factor is voor het wel of niet slagen van informatiebeveiliging [INTE05]. In deze internationale norm voor informatiebeveiliging wordt niet concreet ingegaan op wat nu eigenlijk een gewenst niveau van beveiliging en veiligheid is en wat de relatie is met informatiebeveiligingsbewustzijn. In het geval van La Société Générale was Kerviel niet genoeg getraind en opgeleid, waardoor hij niet het gewenste informatiebeveiligingsbewustzijnsniveau had. Kerviel had dus "bewust" gemaakt moeten worden van de mogelijke risico's en het belang van informatiebeveiliging. Maar waar men moet beginnen, is niet duidelijk; laat staan hoe het wetenschappelijk onderbouwd is.

Hierboven zijn een aantal punten beschreven uit de standaard literatuur op het gebied van informatiebeveiliging. Daarnaast kan men kijken naar de grijze literatuur op dit terrein en dan komt men ongeveer dezelfde trend tegen zoals hierboven beschreven staat. Hofland gaat in zijn onderzoek in op een model waarmee organisaties op strategisch niveau het informatiebeveiligingsbewustzijn in kaart kunnen brengen. Via een quickscan wordt de huidige positie van een organisatie in een matrix met vier kwadranten in kaart gebracht. Daarna kan de organisatie bewust een verbetertraject voor de toekomst kiezen [HOFL05]. Maar is het wel mogelijk om het niveau van informatiebeveiligingsbewustzijn bij een organisatie in kaart te brengen? Kan zoiets als het bewustzijn wel gepositioneerd worden?

In het onderzoek van Mathisen wordt via een kwalitatieve methode antwoord gezocht op de vraag hoe informatiebeveiligingsbewustzijn gemeten kan worden [MATH04]. Hierin worden een negental matrices beschreven die als uitgangspunten kunnen dienen om het informatiebeveiligingsbewustzijn te meten. Deze matrices zijn nog niet getoetst in de praktijk en Mathisen geeft dan ook aan dat dit een logisch vervolgonderzoek is. Mathisen gaat echter te snel over op het meten van het bewustzijn zonder rekening te houden met cruciale gedragsvariabelen zoals attitude, motivatie, enz… . Het onderzoek van Thangarajan is een eerste kwantitatieve benadering van het onderwerp informatiebeveiligingsbewustzijn, waarbij 105 medewerkers van Indiase IT bedrijven zijn ondervraagd over hun informatiebeveiligingsbewustzijn [THAN06].

Ook Shaikh heeft kwantitatief onderzoek gedaan binnen 20 bedrijven onder 98 medewerkers. Hierbij is er op organisatieniveau gekeken naar het effect van trainings- en bewustwordingscampagnes voor informatiebeveiliging [SHAI06]. Zowel Thangarajan als Shaikh concluderen dat trainings- en bewustwordingscampagnes belangrijk zijn voor het informatiebeveiligingsbewustzijn, maar waarom dit dan belangrijk zou kunnen zijn vanuit gedrag gezien wordt niet duidelijk.

Neys concludeert in haar onderzoek dat door de combinatie van het gedragsmodel van Clarke en een methode van risicobeheersing door incidentanalyse zoals de PRISMA-methode, het mogelijk is om inzicht te verkrijgen in de oorsprong van onveilig gedrag bij medewerkers. Door meer begrip te hebben voor de situatie van medewerkers en de keuzes die ze moeten maken, wordt dit gedrag begrijpelijker. Als de echte oorzaak van het gedrag bekend is, kunnen tegenmaatregelen geïmplementeerd worden. Dit moet uiteindelijk leiden tot het minder schenden van de

beveiligingsnormen en tot vermindering van het risico van incidenten veroorzaakt door een onvoldoende niveau van het beveiligingsbewustzijn. De volgende stap is het evalueren van de tegenmaatregelen, waardoor volgens Neys deze methode kan leiden tot voortdurende verbetering van het beveiligingsbewustzijn. Neys wijst er nog wel op dat de casestudie die ze gedaan heeft als doel had te beoordelen of de gevolgde methode toepasbaar zou zijn binnen haar organisatie. Ook de geringe omvang van de geanalyseerde data rechtvaardigt terughoudendheid ten opzichte van de getrokken conclusies [NEYS04]. Met deze laatste zin worden alle constateringen omtrent het nemen van tegenmaatregelen en het verhogen van het informatiebeveiligingsbewustzijn ontkracht. Het enige dat overblijft is dat de PRISMA-methode mogelijk toepasbaar is om inzicht te krijgen in de oorsprong van onveilig gedrag bij medewerkers. Neys komt met haar gedragsmodel van Clarke al in een richting, waarbij gedrag verklaard kan worden. Helaas kijkt ze alleen naar incidenten om het gedrag te verklaren, terwijl niet al het ongewenste gedrag leidt tot incidenten. In het geval van Kerviel had het ook anders kunnen zijn. La Société Générale had ook 4,9 miljard euro aan winst kunnen opstrijken en Kerviel had zijn fictieve ongeautoriseerde transacties kunnen blijven verwerken. Dit geeft aan dat als men alleen maar naar incidenten kijkt, men slechts een beperkt aantal gedragingen ziet.

Bij de bovengenoemde literatuur, bekeken vanuit het vakgebeid van de informatiebeveiliging, komt bij de auteurs een beeld naar voren waarbij gedrag ten aanzien van informatiebeveiliging samengevat kunnen worden in drie aspecten: attitude, kennis en gedrag [JENT04], [BAST03], [KRUG06], die samen het informatiebeveiligingsbewustzijn vormen. Hierbij spelen informatiebeveiligingstrainingen en bewustwordingscampagnes blijkbaar een rol van betekenis, omdat die mogelijk het gedrag ten aanzien van informatiebeveiliging kunnen veranderen [KILL06], [NIST98], [NIST03], [INFO91], [INFO93], [INTE05]. Echter of trainingen met betrekking tot informatiebeveiliging leiden tot vaardigheden en kennis, waarmee medewerkers bijvoorbeeld veilig kunnen omgaan met wachtwoorden (door bijvoorbeeld periodiek het wachtwoord te wijzigen, complexere wachtwoorden te kiezen, het wachtwoord niet te delen met anderen en het wachtwoord niet op te schrijven), veilig gebruik kunnen maken van e-mail of internet (door bijvoorbeeld geen virussen en / of spyware binnen laten), veilig gebruik kunnen maken van automatiseringsmiddelen, adequaat kunnen reageren op mogelijke beveiligingsincidenten (door bijvoorbeeld een bedreiging op tijd te signaleren en de verantwoordelijken in te lichten) en het maken van back-ups, is onduidelijk. Daarnaast is onduidelijk of bewustwordingscampagnes leiden tot het bewustzijn dat er voor zorgt dat medewerkers bijvoorbeeld het belang van informatiebeveiliging inzien en er ook naar handelen. Het is niet duidelijk welke factoren van het menselijke handelen belangrijk zijn om te zorgen dat medewerkers het wenselijke gedrag met betrekking tot informatiebeveiliging vertonen. Dus welke eigenschappen van de mens verklaren waarom bepaald gedrag wel of niet vertoond wordt en middels welke eigenschappen het gedrag ten aanzien van informatiebeveiliging beïnvloed kan worden is niet duidelijk.

De werkwijze binnen het vakgebeid van de informatiebeveiliging rond informatiebeveiligingstrainingen en bewustwordingscampagnes is een "best practice" benadering die vergelijkbaar is met de code voor informatiebeveiliging. Men doet het zo, omdat dit tot nu toe het beste werkt, maar door welke factoren het gedrag van bijvoorbeeld Kerviel werd beïnvloed is niet duidelijk. Er wordt gekeken vanuit de effectiviteit van informatiebeveiliging, terwijl zoals Schneier opmerkt het geen nut heeft om beveiliging te bekijken in termen van effectiviteit. Schneier geeft aan dat beveiliging een trade-off is en dat er niet zoiets is als een volmaakte beveiliging. Een voorbeeld hiervan is dat een kogelvrijvest in Nederland niet echt nuttig is, terwijl het in andere delen van de wereld van levensbelang kan zijn. Daarnaast is beveiliging zowel een gevoel als werkelijkheid en die twee verschillen nogal van elkaar [SCHN08]. Dit wil niet zeggen dat de genoemde termen trainings- en bewustwordingscampagnes en informatiebeveiligingsbewustzijn onzinnig en niet relevant zijn. De termen gaan echter voorbij aan de oorzaak en proberen direct in te gaan op het probleem zoals dat van Kerviel, om een oplossing te bieden. Het zou eerst duidelijk moeten worden, welke factoren van

het menselijk handelen invloed hebben op het individuele gedrag van medewerkers in organisaties op de mate van informatiebeveiliging van die organisatie. Hierna kan dan gericht een interventie plaatsvinden om het individuele gedrag van medewerkers in organisaties bij te sturen. Wat betreft informatiebeveiligingsbewustzijn stelt Spruit dat een organisatiebrede informatiebeveiligingsbewustwordingscampagne gebaseerd op voorlichting, geen rol van betekenis heeft om de risico's van het menselijke falen te beperken. Spruit stelt dat deze campagnes alleen nuttig zijn om plotselinge risico- of organisatieveranderingen onder de aandacht te brengen [SPRU04]. Overbeek, Lindgreen en Spruit geven aan dat mensen hun eigen persoonlijke belangen hebben. Slechts voor een deel vallen deze belangen samen met de bedrijfsbelangen. Hun mening is dat het geven van een goede algemene voorlichting of instructie een ondankbare taak is. Zij wijzen er op dat voorlichtingscampagnes, bewustwordingscampagnes, instructiefolders, cursussen en dergelijke dan ook neigen te mislukken en slechts een marginale verbetering met zich meebrengen. In hun optiek is het beter om de voorlichting en instructie te individualiseren of op functieniveau toe te passen. Het is nauwelijks te doen om een zodanige argumentatie te geven dat individuele belangen voldoende terug te vinden zijn, terwijl ook het bedrijfsbelang niet uit het oog verloren wordt [OVER05].

Hiermee zijn we terug bij af en lijkt er geen duidelijke verklaring voor de wijze waarop Kerviel handelde. Maar er is vanuit de sociale wetenschappen theorie waarmee mogelijk gedrag voorspeld en verklaard kan worden. Volgens de *theorie van gepland gedrag* (TpB) die ontwikkeld is door Ajzen, wordt het menselijke gedrag geleid door drie determinanten (attitude toward the behavior, subjective norm en perceived behavioral control) die samen de intentie tot gedrag bepalen [AJZE91]. Als algemene regel geldt dat, hoe positiever de drie determinanten samenhangen, hoe sterker de intentie van de persoon zal zijn, om het gedrag in kwestie uit te voeren. Als laatste wordt verwacht dat een persoon zijn intentie tot gedrag zal omzetten tot werkelijk gedrag, als de situatie zich voordoet en als er voldoende werkelijke controle is over het gedrag [AJZE02].

Stanton e.a. hebben al onderzoek gedaan waarbij de theorie van gepland gedrag voor een klein deel gebruikt is. Daarnaast is er een taxonomie met 6 categorieën ontworpen voor gedragingen ten aanzien van informatiebeveiliging [STAN05a]. Op basis van brainstormsessies en interviews zijn er 93 gedragingen geïnventariseerd. Vervolgens zijn de gedragingen gecategoriseerd, waarbij de 93 gedragingen verdeeld zijn over de zes gedragscategorieën [STAN06]. Helaas is er een vragenlijst gebruikt bestaande uit slechts tien items[9]. Daarnaast is er niet gekeken naar individueel gedrag, maar naar het collectieve gedrag per businessunit. Ondanks dat de werkwijze van Stanton e.a. niet aansluit op de theorie van gepland gedrag en dat het een opzichzelfstaand onderzoek is, zijn de resultaten toch waardevol voor vervolgonderzoek, omdat deze een handreiking geven in welke richting er mogelijk gezocht moet worden.

Middels dit onderzoek is op basis van de theorie van gepland gedrag inzicht verkregen in de aard en oorsprong van de gedragsintentie van medewerkers binnen organisaties bij het beveiligen van en veilig omgaan met de informatievoorziening van een organisatie. Teruggekoppeld naar het gedrag van Kerviel zou dit inzicht moeten verklaren, waarom hij zou kunnen komen tot het misbruik van vertrouwen, het vervalsen van documenten en het onbevoegd gebruik maken van computers. Ervanuitgaande dat Kerviel een vragenlijst invult. Hierbij is de gedragsintentie ingevuld aan de hand van de 93 gedragingen en de 6 gedragscategorieën van Stanton e.a. [STAN05a], [STAN06]. De drie determinanten uit de theorie van gepland gedrag zijn ingevuld aan de hand van een definitie van betrouwbaarheid van informatiebeveiliging [OVER05], van informatiebeveiligingsbewustzijn [INFO02], een clustering van de 93 gedragingen van Stanton e.a. over de informatievoorziening [STAN06] en twee andere vragenlijsten met betrekking tot wachtwoordmanagement [STAN04].

[9] De twee termen *items* en *vragen* zullen vaak door elkaar worden gebruikt, maar beiden termen hebben de zelfde betekenis.

1.2 Onderzoeksvraag

De volgende onderzoeksvraag zal in dit onderzoek behandeld worden:

Wat zijn de mogelijke voorspellende verklaringen voor de gedragsintenties van medewerkers binnen organisaties in Nederland ten aanzien van informatiebeveiliging, gezien vanuit de attitude toward the behavior, subjective norm en perceived behavioral control beschreven in de theorie van gepland gedrag?

1.3 Deelvragen

De onderzoeksvraag wordt beantwoord met behulp van de volgende deelvragen:

- Wat is de voorspellende waarde van attitude toward the behavior ten opzichte van de gedragsintentie ten aanzien van informatiebeveiliging?
- Wat is de voorspellende waarde van subjective norm ten opzichte van de gedragsintentie ten aanzien van informatiebeveiliging?
- Wat is de voorspellende waarde van perceived behavioral control ten opzichte van de gedragsintentie ten aanzien van informatiebeveiliging?
- In hoeverre leveren attitude toward the behavior, subjective norm en perceived behavioral control een unieke bijdrage aan het voorspellen van de gedragsintentie ten aanzien van informatiebeveiliging?

2. VERANTWOORDING

2.1 Domein

Het domein van dit onderzoek zijn medewerkers binnen organisaties in Nederland. Deze medewerkers worden beschouwd als eindgebruikers van de informatievoorziening binnen de organisatie waarin ze werkzaam zijn. Hierbij is onderscheid gemaakt tussen drie verschillende rollen die medewerkers binnen de organisaties kunnen vervullen, te weten: managers, IT- specialisten en overige medewerkers (bij overige medewerkers moet gedacht worden aan HRM-medewerkers, administratiemedewerkers, secretariaatmedewerkers, enz...). De betreffende organisaties die binnen de onderzochte doelgroep vallen zijn actief binnen één van de volgende bedrijfstakken[10]:

- Hightech industrie: onder andere chemische industrie, vervaardiging van machines, elektrische en optische apparaten, transportmiddelen.
- Overige industrie: onder andere voedings- en genotmiddelen, textiel, houtindustrie, papierindustrie, vervaardiging van rubber, kunststof, glas, aardewerk, metaalproducten en meubels, scheepsbouw en -reparatie.
- Kennisintensieve dienstverlening: onder andere telecommunicatie, informatietechnologie, onderzoeksbureaus, rechtskundige dienstverlening, accountants, architecten, ingenieurs, technische adviesbureaus en reclamebureaus.
- Overige dienstverlening: onder andere (semi-)overheidsinstanties, productie en distributie van elektriciteit, aardgas en water, bouwnijverheid, handel en reparatie, horeca, vervoer, opslag en communicatie, verhuur van en handel in roerende en onroerende goederen, uitzendbureaus, beveiliging, reiniging en fotografie.

2.2 Relevantie

Binnen een groot aantal organisaties krijgt informatiebeveiliging een steeds belangrijkere rol. Beveiligingsstandaarden als COBIT[11], COSO[12], BS 7799-2[13] en ISO/IEC 27002[14] worden een standaard onderdeel van het risicomanagement en ook de security officer krijgt zijn plaats binnen de organisatie. Een organisatie is echter met de implementatie van een informatiebeveiligingsraamwerk en het aanstellen van een security officer nog niet klaar. Vooral de logische, fysieke en organisatorische aspecten van informatiebeveiliging krijgen veel aandacht en zijn voor de security officer tastbaar en controleerbaar. Hoe het gedrag van medewerkers binnen organisaties ten aanzien van informatiebeveiliging zich verhoudt, is echter onduidelijk. Dit komt doordat de aard en oorsprong van de intentie en het werkelijke gedrag van medewerkers ten aanzien van informatiebeveiliging niet onderzocht zijn. Op Stanton e.a. na is er geen wetenschappelijk onderzoek verricht vanuit zowel sociaal wetenschappelijk als informatietechnisch perspectief. In dit onderzoek staan vooral de wetenschappelijke waarden voorop. Het is belangrijk inzicht te krijgen in de aard en de oorsprong van de intentie en het werkelijke gedrag van medewerkers binnen organisaties bij het betrouwbaar omgaan met de informatievoorziening. Het gedrag van deze medewerkers is een

[10] http://www.cbs.nl/nl-NL/menu/methoden/toelichtingen/alfabet/b/bedrijfstak.htm

[11] The control objectives for information and related technology

[12] The committee of sponsoring organizations of the treadway commission

[13] British Standards Institute

[14] Internationale standaard en opvolger van ISO/IEC 17799

belangrijke factor voor de betrouwbaarheid van de informatiebeveiliging binnen organisaties. Het beveiligingsbeleid en -plan kunnen nog zo goed zijn, technisch en organisatorisch kan het ook goed geregeld zijn, maar dan nog moeten de medewerkers wel met de juiste intentie handelen en het juiste gedrag vertonen. De keuze voor medewerkers binnen organisaties in Nederland wordt gevormd doordat zij immers onderworpen zijn aan beleid, richtlijnen, voorschriften en procedures. Hierdoor is de naleving afhankelijk van het individuele gedrag van deze medewerkers. Daarnaast is er een wederzijdse afhankelijkheidsrelatie tussen medewerkers en organisaties, waarbij beiden elkaar nodig hebben om hun doelen te bereiken [KATZ78]. Hier komt dan ook een bijzondere vorm van gedrag ter sprake dat zichtbaar is binnen organisaties. Dit in tegenstelling tot de thuisgebruiker, die thuis of op vakantie niet onderhevig is aan een beleid, richtlijnen, voorschriften of procedures en waarbij er ook geen sprake is van een ruilrelatie zoals tussen medewerker en organisatie. Voor het bewustzijn en kennis van deze thuisgebruiker is er het platform Digibewust[15] dat een samenwerkingsverband is tussen de overheid, voorlichtingsinstanties en het bedrijfsleven in Nederland. Ook is er een compleet ander economisch model tussen medewerkers in organisaties en thuisgebruikers met andere belangen en doelstellingen, die niet met elkaar te vergelijken zijn.

Verder gaat de interesse van de auteurs binnen dit onderzoek uit naar de onderzoeksgebieden arbeids- en organisatiepsychologie en informatiebeveiliging. Hierdoor is de keuze voor gedrag ten aanzien van informatiebeveiliging de grens tussen beide. Voor informatiekundige studenten is dit een geschikt terrein om onderzoek te doen. Dit omdat informatiekunde zich bevindt op het snijvlak van mens, organisatie en technologie. Hierbij vormen de auteurs van dit onderzoek de bruggenbouwers tussen deze drie gebieden. Vanuit de informatica wordt dit onderzoeksgebied te gamma beschouwd. Dit komt doordat het gedrag vanuit een sociale perspectief geen onderdeel uitmaakt van de bèta-wetenschappen. Vanuit de sociale wetenschappen wordt geredeneerd dat het een onderdeel van de bèta-wetenschappen is. Dit heeft als reden dat het een onderwerp met een technische achtergrond betreft. In dit onderzoek is gekozen om de theorie van gepland gedrag te gebruiken in dit onderzoek. Dit slaat dan de brug tussen de gamma-wetenschappen en de bèta-wetenschappen. Uit de COTAN[16]- en literatuurstudie is gebleken dat er niet één studie is verricht naar gedrag ten aanzien van informatiebeveiliging aan de hand van de theorie van gepland gedrag.

2.3 Verankering

Het onderzoek is binnen twee kennisgebieden verankerd, maar heeft zich op één kennisgebied specifiek gericht. Dit specifiek gerichte kennisgebied is het volgende:

- Informatica en informatiekunde
    - Beveiliging
        - Informatiebeveiliging
            - Informatiebeveiligingsbewustzijn
            - Gedrag ten aanzien van informatiebeveiliging

Een nadere beschrijving van bovenstaande kennisgebied, waarbinnen dit onderzoek verankerd is, is in de volgende alinea beschreven.

---

[15] http://www.digibewust.nl

[16] De COTAN (the committee of test affairs netherlands) beoordeeld op basis van een rating systeem de testkwaliteit van Psychometrische instrumenten en is gebaseerd op de volgende criteria: theoretische achtergrond, kwaliteit testmateriaal, handleiding, normering, betrouwbaarheidconstruct, validiteit, criterium validiteit. De COTAN bevat de beschrijvingen van 457 Nederlandstalige psychodiagnostische instrumenten die tot en met 1999 zijn verschenen.

Binnen de informatiebeveiliging is voor verdere inperking gekozen, omdat er specifiek naar het gedrag ten aanzien van informatiebeveiliging bij medewerkers wordt gekeken. Daarnaast is het onderzoek nog binnen een tweede kennisgebied verankerd, aangezien gedrag binnen het kennisgebied van sociale wetenschappen gemeten moet worden. Het tweede kennisgebied waarbinnen het onderzoek verankerd is, ziet er als volgt uit:

- Sociale wetenschappen
    - Gedragswetenschappen
        - Arbeids- en organisatiepsychologie
            - Individueel gedrag in organisaties

Het tweede kennisgebied is in dit onderzoek opgenomen, omdat er binnen de sociale wetenschappen en specifieker binnen gedragswetenschappen de theorie van gepland gedrag ontwikkeld is. Dit om de attitude toward the behavior, subjective norm en perceived behavioral control ten aanzien van specifiek gedrag (bijvoorbeeld: ziekmelden, werken, roken, enz…) van mensen te meten. Dit is belangrijk voor de latere dataverzameling van het onderzoek dat in het hoofdstuk "Methode" aan bod komt en heeft daarom in dit deel van het onderzoeksplan geen verdere toelichting nodig. De verdere verankering vindt plaats binnen de arbeids- en organisatiepsychologie. Hierbinnen wordt het gedrag van de werkende persoon bij het voortbrengen van het arbeidsresultaat in relatie tot kenmerken van de taak van de organisatie en van de persoon bestudeerd. Zoals te zien is, ligt de nadruk op het individuele gedrag in organisaties van medewerkers. De reden hiervoor is dat medewerkers onderhevig zijn aan maatregelen voor informatiebeveiliging die opgelegd zijn vanuit de organisatie.

2.4 Taalkeuze en werkwijze

Voor deze scriptie is om een aantal redenen gekozen voor de Nederlandse taal. Ten eerste zijn beide auteurs dyslectisch, waardoor het schrijven in de moedertaal al een barrière vormt. Daarnaast bestaat de onderzoekspopulatie uit medewerkers binnen organisaties in Nederland. Hierdoor is Nederlands de voertaal in de vragenlijsten. Een belangrijke opmerking is dat door de internationale aandacht voor het onderwerp informatiebeveiliging en gedrag veel termen bekend zijn en/of gebruikt worden in het Engels, en zich niet gemakkelijk naar het Nederlands laten vertalen. Daar waar naar mening van de auteurs de internationale termen de strekking beter weergeeft dan de (vertaalde) Nederlandse termen, is gekozen voor de internationale termen.

Tijdens het inrichten van het onderzoek is ervoor gekozen om een MediaWiki in te richten als interactieve werkplaats. Hierbij hebben wij als onderzoekers de meerwaarde van de MediaWiki werkplaats ondervonden, om op een nieuwe manier samen te leren en te werken binnen dit afstudeeronderzoek. Binnen de MediaWiki werkplaats was het navigatiemenu aangepast, waarbij een aantal subwerkplaatsen onderkend zijn: thesis, discussie, vragenlijst en literatuur. Onder *thesis* stonden alle geschreven hoofdstukken. Hierbij is een onderscheid aangebracht tussen de teksten die nog moesten worden gereviewed en teksten die al volledig afgerond waren. Bij het reviewen werd gebruik gemaakt van verschillende kleuren: geel, rood en blauw. Geel voor opmerkingen of suggesties, rood voor commentaar of kritiek en blauw voor teksten die aangepast waren en nogmaals gereviewed moesten worden. Daarnaast werd veelvuldig gebruik gemaakt van Word documenten die voorzien werden van *track changes*. De werkplaats *discussie* was bedoeld als dumpplaats voor lopende en nog te bespreken onderwerpen. Voor de dagelijkse discussies en besprekingen werd op de momenten dat we niet samen op één locatie waren gebruik gemaakt van Skype. Onder de werkplaats *vragenlijst* stonden alle zaken die te maken hadden met de vragenlijst. Hierbij moet gedacht worden aan de operationalisaties van de vragenlijsten, de contactlijst voor het uitzetten van de vragenlijsten,

enzovoorts. Als laatste werd alle benodigde literatuur samengebracht en verzameld in de werkplaats *literatuur*. Hierbij is een opsplitsing gemaakt tussen boeken, artikelen en grijze publicaties.

Binnen dit onderzoek zijn een aantal hoofdstukken individueel geschreven. Voor de verantwoording van deze hoofdstukken is er per hoofdstuk of paragraaf aangegeven wie de penvoerder is geweest. Hoofdstukken waar geen naam vermeld staan zijn in directe samenwerking geschreven, waarbij meestal beide auteurs op één en dezelfde locatie waren. Met penvoerder wordt diegene bedoeld die de pen heeft gevoerd ten aanzien van de originele tekst. Hierbij heeft de ander gefungeerd als reviewer en criticus. Hierdoor nemen beide auteurs voor het totale geschrift verantwoording.

Het voordeel van deze werkwijze is geweest dat er onderzoek kon worden gedaan dat omvangrijker, faculteit- en domeinoverstijgend was, waarbij er door de constante wederzijdse discussie en kritiek meer diepgang en kwaliteit kon worden bereikt. Daarnaast kon er direct van elkaar geleerd worden en kon er op een gelijkwaardig niveau kennis worden uitgewisseld. Dit in tegenstelling tot twee individuele onderzoeken waarbij van wederzijdse betrokkenheid en afhankelijkheid geen sprake zou zijn geweest, ook niet als er een gedeeltelijke overlap was binnen het onderzoek. De gekozen werkwijze had als nadeel dat er zeer veel overhead was binnen het onderzoek. Dit kwam vooral doordat alle onderzoeksobjecten door beide onderzoekers moesten worden doorlopen.

3. THEORETISCH KADER[17]

In dit hoofdstuk worden relevante theorieën, modellen en concepten op het gebied van de informatiebeveiliging en gedrags- en bedrijfswetenschappen geïnventariseerd. Deze vormen de basis en dienen als kader van dit onderzoek naar het gedrag van medewerkers binnen organisaties in Nederland ten aanzien van informatiebeveiliging. Voor de theorievorming van dit onderzoek is *alleen* paragraaf 3.1.3.1 met betrekking tot de theorie van gepland gedag noodzakelijk. Aangezien er geen theoretisch gefundeerde vragenlijst bestaat voor het meten van het gedrag ten aanzien van informatiebeveiliging, zal er gebruik worden gemaakt van de geïnventariseerde literatuur. Daarnaast is er geen duidelijke omlijning voor het onderzoek dat zich richt op het verklaren en beïnvloeden van gedrag ten aanzien van informatiebeveiliging, waardoor dit ook als verkenning gezien kan worden van de verschillende onderzoeksgebieden.

Als eerste zal er ingegaan worden op de concepten en theorieën van individueel gedrag binnen organisaties. Hierbij zal het individueel gedragsmodel van Robbins als startpunt gebruikt worden en zullen achtereenvolgens de aspecten: attitude, persoonlijkheid, perceptie motivatie, emotie, leren en capaciteiten beschreven worden. Hierbij zal in dit onderzoek en in dit theoretisch kader niet worden ingegaan op aspecten zoals stress of werkomstandigheden wat externe invloedsfactoren zijn.

Daarna volgen een aantal theorieën om het individueel gedrag van mensen te verklaren en te begrijpen. Hierbij zal uitgebreid worden ingegaan op de theorie van gepland gedrag wat het leidende model vormt van dit onderzoek en op basis waarvan de vragenlijst ontwikkeld is. De sociaal-cognitieve theorie, technology acceptance model en de unified theory of acceptance and use of technology komen hierbij summier aan bod en hebben raakvlakken met de theorie van gepland gedrag.

Vervolgens wordt het concept "Behavioral information security" beschreven en worden de verschillende fouttypen en informatieverwerkingsniveaus toegelicht. De brug tussen gedrag en informatiebeveiliging wordt geslagen met het concept van informatiebeveiligingsbewustzijn, waarbij een aantal definities het vertrekpunt zullen zijn en zal er worden gekeken hoe dit concept gemeten zou kunnen worden. Tot slot zal het onderwerp informatiebeveiliging worden beschreven, wat de essentie van dit onderzoek vormt samen met individueel gedrag binnen organisaties.

3.1 Gedrag

In essentie is het gedrag van een persoon alles wat die persoon zegt of doet [BERN94]. Maar welk soort gedrag vertonen individuen binnen organisaties? Psychologen gebruiken woorden als intelligentie, emotie, attitude en motivatie. Vanuit de organisatiepsychologie kunnen deze begrippen in eerste instantie gezien worden als een indeling van werkgedrag. Voor deze verschillende gedragingen geeft Jansen de volgende omschrijving en vraagstelling [JANS02]:

- Intelligentiegedrag is gedrag waarvan op grond van een gegeven probleem gesteld kan worden dat het goed of fout is. Het heeft dus te maken met een voorhanden probleem en de oplossing daarvan binnen een gestelde norm van wat correct of foutief is. De basisvraag is: Klopt dit?

[17] Geschreven door Michiel Dam

- Emotiegedrag is gedrag waarin gevoelens over een object of een aangelegenheid worden uitgedrukt en wel in termen van prettig/fijn of onaangenaam/vervelend. De basisvraag is: Vindt u dit fijn?
- Attitudegedrag is gedrag waarin sprake is van de impliciete of expliciete waardering van een object of stand van zaken. Attitudes hebben betrekking op preferenties, op voorkeuren en afkeuren, op evaluaties van feiten, personen of zaken. De basisvraag is: Bent u het ermee eens?
- Motivatiegedrag is gedrag waarin sprake is van de neiging of intentie om iets te willen doen. De basisvraag is: Wilt u dit?

Hieronder zal verder ingegaan worden op het gedrag van individuen binnen organisaties.

3.1.1 Het individu en de organisatie

Een belangrijke eigenschap voor de relatie tussen individu en organisatie[18] is de wederzijdse afhankelijkheid. Het individu wil een bepaalde behoefte of wens, die zowel materieel als immaterieel van aard kan zijn, bevredigen. Organisaties aan de andere kant hebben de inspanning van mensen nodig om producten, diensten en kwaliteit te kunnen bieden [ALBL05]. Er is sprake van een ruilrelatie waarbij het individu een bepaalde inbreng heeft zoals tijd, prestatie, ervaring of creativiteit en krijgt hier als opbrengst bijvoorbeeld salaris, status, promotie of verantwoordelijkheid voor terug. Deze wederzijdse afhankelijkheid is niet absoluut. Er is maar een gedeeltelijke betrokkenheid van beide partijen [KATZ78]. Betrokkenheid bij het verrichten van arbeid is de mate waar voor een persoon in het werk belangrijke waarden op het spel staan en de mate waarin stemming en gevoelens van een persoon beïnvloed worden door werkervaringen [VOGE90]. Een werknemer is dus betrokken bij een organisatie wanneer hij zich kan identificeren met de organisatie en wanneer de organisatie mede de gevoelens en stemming van de werknemer kan bepalen. Als een werknemer zijn werkzaamheden in iedere organisatie uit zou willen voeren zolang de werkzaamheden identiek zijn, heeft dat als betekenis dat hij niet betrokken is bij de organisatie [HAVE00]. Deze betrokkenheid, ook wel commitment genoemd, is te verdelen in twee soorten, namelijk *attitudinal commitment* en *behavioral commitment*. De eerste heeft te maken met de psychologische band die een werknemer heeft met de organisatie. Hierbij vergelijkt de werknemer zijn persoonlijke doelen en waarden met die van de organisatie. *Behavioral commitment* heeft te maken met het gedrag wat gevormd wordt naarmate de werknemer zich een aantal jaren in de organisatie bevindt [SCHO99].

Een individu binnen een organisatie verricht arbeid[19] wat het verrichten van een prestatie tegen een beloning is. Er moet sprake zijn van een ruil tussen het leveren van een arbeidsprestatie en het daarvoor terugontvangen van een opbrengst. Grumbkow onderscheidt een drietal kenmerken van arbeid [GRUM90]:

- Een individu verricht arbeid met een bepaald oormerk. Arbeid heeft een intentioneel karakter en wordt verricht met bepaalde motieven.
- Arbeid heeft altijd direct nut voor de persoon in kwestie. Er is een koppeling tussen de arbeid en de behoeftebevrediging.
- Arbeid heeft nut voor anderen. Arbeid wordt verricht in de economische context van een markt voor ruilrelaties.

---

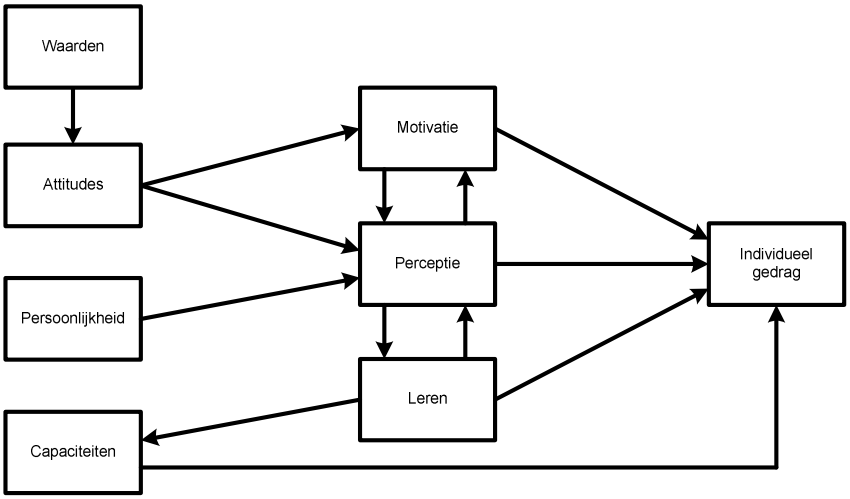
[18] Keuning definieert een organisatie als een doelrealiserend samenwerkingsverband. [KEUN91]

[19] Vanuit de algemene psychologie spreekt men over menselijke arbeid wat als volgt gedefinieerd wordt: *Een proces waarin een individu zijn/haar omgeving doelbewust transformeert onder gebruikmaking van bepaalde psychische verwerkingsmechanismen* [ROE91].

Ondanks het feit dat mensen slechts gedeeltelijk betrokken zijn bij organisaties waar ze werken, kunnen ze toch behoorlijk wat arbeid verrichten. Maar wat zet mensen aan tot het verrichten van arbeid? Op deze vraag zullen we hieronder verder ingaan.

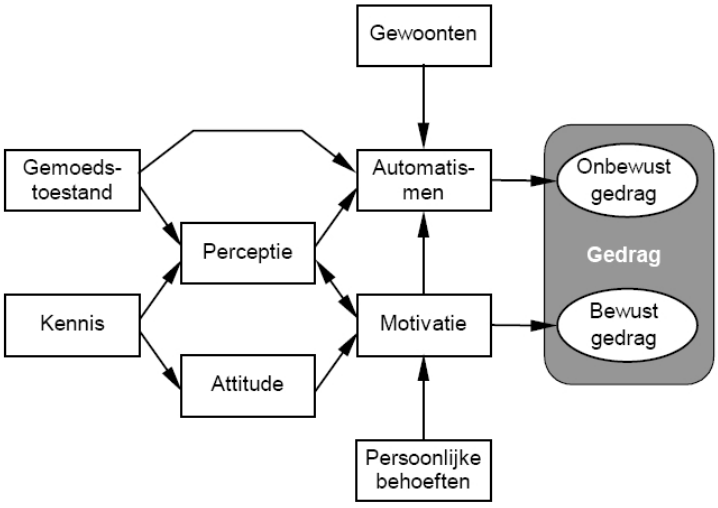
3.1.2 Gedrag in Organisaties

Kort gesteld kan men zeggen dat wanneer een individu een organisatie binnenkomt, hij een betrekkelijk vastomlijnde serie waarden, attitudes en een behoorlijke gevormde persoonlijkheid heeft. In figuur 1 heeft Robbins belangrijke variabelen voor individueel gedrag samengevat [ROBB02].



Figuur 1: Sleutelvariabelen van individueel gedrag [ROBB02]

Hoewel waarden in het individuele gedragsmodel van Robbins geen directe invloed hebben op gedrag, spelen ze een belangrijke rol voor iemands attitudes. Kennis van iemands waardesysteem kan dus inzicht geven in zijn attitudes. Overbeek e.a. hebben het model van Robbins geadopteerd en toegepast op informatiebeveiliging [OVER05].



Figuur 2: Gedrag en de factoren die daarbij een rol spelen [OVER05]

In het model van Overbeek e.a. wordt een duidelijke plaats gegeven aan automatismen en motivatie in relatie tot bewust en onbewust gedrag ten aanzien van informatiebeveiliging. Hierbij geven automatismen aanleiding tot onbewust gedrag. Motivatie geeft daarentegen aanleiding tot bewust gedrag. Deze tweedeling van gedrag is alleen zichtbaar bij het model van Overbeek e.a en dus niet in het model van Robbins. Dit is een duidelijk verschil tussen gamma-wetenschappen en bèta-wetenschappen. Voor het vakgebied van de informatiebeveiliging is het kenmerkend om gedrag ten aanzien van informatiebeveiliging te classificeren in termen van bewust en onbewust gedrag. Of dit vanuit sociaalwetenschappelijk oogpunt mogelijk en wenselijk is, wordt verderop besproken. De gemoedstoestand of emotie heeft binnen het model van Robbins geen prominente plaats, maar zal toch aan bod komen. Gewoontes of routines zullen binnen dit onderzoek geheel buiten beschouwing worden gelaten. Hieronder zal worden ingegaan op de aspecten: attitude, persoonlijkheid, perceptie, motivatie, emotie, leren en capaciteiten. Dit zijn de verschillende aspecten van individueel gedrag volgens het model van Robbins.

3.1.2.1 Attitude

Azjen definieert een attitude als een relatief stabiele stemming die bepaalt of men een positieve of negatieve houding heeft ten opzichte van een concreet object, individu, groep, organisatie, idee, bepaalde gebeurtenis of het eigen werk en de werksituatie [AJZE88]. Deze houding heeft een verloop dat van positief via neutraal naar negatief kan gaan en andersom. De attitude van een individu kan inzicht geven in zijn gedachte. Een belangrijk gegeven is dat individuen consequent willen zijn met hun attitude. Wanneer twee of meer attitudes van een individu met elkaar conflicteren of als attitudes en gedrag tegenstrijdig zijn is er sprake van cognitieve dissonantie.

De cognitieve dissonantietheorie van Festinger stelt dat individuen constant proberen dissonantie en het resulterende ongemak zo gering mogelijk te houden [FEST57]. Het volledig elimineren van dissonantie is onmogelijk. De cognitieve dissonantie is gericht op het gebrek aan evenwicht tussen gedachten, gevoelens, attitudes, opvattingen en gedrag. Hoe gaan individuen om met dissonantie? De sterkte van de drang om de dissonantie te verminderen, hangt af van het belang van de elementen die de dissonantie oproepen, van de hoeveelheid invloed die het individu in kwestie denkt te hebben op de elementen en van de beloning van dissonantie. Zijn de elementen die de

dissonantie oproepen relatief onbelangrijk, dan zal de impuls om het evenwicht te herstellen nihil zijn. Als het individu de dissonantie ervaart als iets dat volledig buiten zijn invloedssfeer valt, dan zal zijn attitude niet snel veranderen. Beloning kan een belangrijke rol spelen voor het motiveren om dissonantie te verminderen. De theorie is een hulpmiddel om te voorspellen of individuen geneigd zijn gedrag en/of attitudes te veranderen. Het gaat vooral in op het proces dat volgt op dissonantie. Zij heeft dus betrekking op wat er gebeurt als een individu er twee dissonante cognities op na houdt en tracht die toestand van geestelijke dissonantie op te heffen. Men kan op twee mogelijke manieren de dissonantie verminderen. Ten eerste kan men de eigen cognities veranderen, dus iets anders gaan denken, willen of voelen. Ten tweede kan men het eigen gedrag veranderen door iets anders te gaan doen.

Er is een grotere kans een significante correlatie te vinden als men zich concentreert op specifieke attitudes en specifiek gedrag. Hoe concreter de attitude en het gedrag die men meet, des te meer kans dat men een verband tussen attitude en gedrag kan aantonen [AJZE88].

3.1.2.2 Persoonlijkheid

Om individuen te kunnen beschrijven in termen als rustig of passief worden ze ingedeeld in categorieën op grond van karaktertrekken. De persoonlijkheid is de samenstelling van psychologische trekken die men gebruikt om individuen te classificeren. Digman beschrijft het vijf- factorenmodel voor persoonlijkheid [DIGM90]. De grote vijf vormen de vijf basisdimensies voor alle facetten van persoonlijkheid en bestaat uit de volgende factoren:

- Extraversie: sociaal, spraakzaam, assertief;
- Inschikkelijkheid: opgewekt, werkt samen, vol vertrouwen;
- Nauwgezet: verantwoordelijk, betrouwbaar, volhardend, prestatiegericht;
- Emotionele stabiliteit: kalm, zelfverzekerd, onzeker, nerveus, enthousiast;
- Openheid voor ervaring: fantasievol, intellectueel, artistiek.

Naast de vijf basisdimensies zijn er in de literatuur nog zes andere relevante persoonlijkheidskenmerken om gedrag in organisaties te verklaren. Achtereenvolgens zullen interne en externe locus of control, autoritarisme, machiavellisme, zelfcontrole, type A of type B en risicotolerantie worden beschreven [JANS02], [ROBB08]. Het eerste kenmerk is de interne en externe locus of control. Interne locus of control gaat er vanuit dat individuen het lot zelf in handen hebben. Deze individuen zullen het eigen gedrag als oorzaak van de beoordeling zien en zullen sneller tevreden zijn met hun werk, zich sneller thuis voelen in de werksituatie en meer betrokken zijn bij het werken, dan mensen met een externe locus of control. Als tweede kenmerk is de autoritarisme dat veronderstelt dat er status- en machtsverschillen tussen individuen binnen organisaties moeten zijn. Machiavellisme is het derde kenmerk, dat verwijst naar een individu met machiavellistische trekjes die manipuleert, emotioneel afstand houdt van anderen en vindt dat het doel de middelen heiligt. Machiavellisme en autoritarisme zijn hierdoor nauw verwant met elkaar. Zelfcontrole of zelf-monitoring geeft aan hoe goed een individu zich kan aanpassen aan verschillende situaties. Individuen met een hoge mate van zelfcontrole voegen zich naar de omgeving en verbergen de ware zelf, zijn alerter op het gedrag van anderen, vertonen in iedere situatie ander gedrag en kunnen zich beter conformeren dan diegene met een lage zelfcontrole. Als vijfde kenmerk kan er onderscheid gemaakt worden tussen 'type A' en 'type B' persoonlijkheid. Individuen met type A persoonlijkheid zijn opvallend competitief, op agressieve wijze betrokken in een onophoudelijke strijd, waarbij het erom gaat meer en meer te presteren in steeds minder tijd, zijn ongeduldig, weten niet wat ze met vrije tijd aanmoeten en hun leven wordt beheerst door zelfopgelegde deadlines. Individuen die tot type B persoonlijkheid worden gerekend, kunnen even ambitieus zijn en eenzelfde

prestatiedrang hebben als een type A. Alleen een type B persoonlijkheid zal zich daarbij niet opgejaagd of geprikkeld voelen, maar zal zich juist rustig en zelfvertrouwd voelen. Het laatste kenmerk is de mate van risicotolerantie bij individuen. Personen verschillen in de bereidheid om risico's te nemen. De mate van risicotolerantie kunnen invloed hebben op de risico's die een individu neemt. Individuen met een hoge risicotolerantie zullen sneller en grotere risico's nemen en veelal ook op basis van minder informatie, dan individuen met een lage risicotolerantie.

3.1.2.3 Perceptie

Perceptie is het proces waarin individuen hun zintuiglijke indrukken ordenen en interpreteren om zin te geven aan hun omgeving. Individuen die hetzelfde waarnemen, kunnen toch een heel verschillende interpretatie hebben. De mens neemt de werkelijkheid niet waar, maar in plaats daarvan maakt men daar een interpretatie van en noemt dat de werkelijkheid. Deze waarneming wordt door een aantal factoren gevormd en vervormd. De waarnemer zelf, het object dat wordt waargenomen of de context van de situatie die wordt waargenomen, zijn factoren die de waarneming kunnen beïnvloeden. Naast deze beïnvloeding zijn er nog persoonlijke kenmerken die invloed hebben, zoals attitudes, persoonlijkheden, motieven, belangen, eerdere ervaringen en verwachtingen [ROBB08].

Niet al het gedrag van individuen komt automatisch tot stand. Voordat men tot bepaald gedrag komt denkt men over de situatie na en de mogelijkheden die er zijn om bepaalde doelen of opbrengsten te verwezenlijken. De motivatie om bepaald gedrag wel of niet te vertonen is de uitkomst van een overwegingsproces [ALBL05]. Er zijn twee theorieën die de overwegingen beschrijven die ten grondslag liggen aan de keuze van gedrag: de attributietheorie en de waarde-verwachtingstheorie. Hier zal alleen ingegaan worden op de attributietheorie. De waarde-verwachtingstheorie komt bij de motivatietheorieën aan bod.

De attributietheorie verklaart waarom individuen verschillend kunnen beoordelen, afhankelijk van de betekenis die men toekent aan bepaald gedrag en laat zien waarom men zich zal inspannen als men het idee heeft dat men met het gedrag de gewenste opbrengst kan verkrijgen [HEID82]. Deze beoordeling gebeurt via het proces van attribueren. De theorie stelt dat wanneer men iemands gedrag observeert, men probeert te bepalen of daaraan interne of externe attribuerende elementen aan ten grondslag liggen. Van interne attributie is sprake als een individu de oorzaken van het probleem toerekent aan factoren binnen zijn invloedssfeer. Bij externe attributie legt een individu de oorzaken van het probleem bij factoren buiten zichzelf, dus bij andere mensen of omstandigheden. Volgens Kelly zijn er voor deze beoordeling drie factoren van belang [KELL72]. Deze drie factoren zijn distinctiviteit, consensus en consistentie:

- De factor distinctiviteit geeft aan of een individu in verschillende situaties ander gedrag vertoont. Bij lage distinctiviteit zal men eerder intern attribueren en bij hoge distinctiviteit eerder extern.
- De factor consensus gaat in op de vraag of anderen die met dezelfde situatie geconfronteerd worden, zich op dezelfde manier gedragen. Bij lage consensus van een individu is hij de enige die problemen heeft, en zal er eerder intern geattribueerd worden.
- Als laatste factor zoekt de waarnemer naar consistentie tussen gedragingen. Hierbij gaat het om de vraag of iemand in dezelfde situatie zich steeds op dezelfde manier gedraagt, of juist steeds verschillend.

Gedrag met een interne oorzaak wordt geacht onder de controle van het individu te vallen. Gedrag met een externe oorzaak valt buiten de invloedssfeer van het individu en wordt door de situatie afgedwongen. Vanuit de attributietheorie komt naar voren dat fouten of vooroordelen de

attributies vertekenen. Wanneer men een ander moet beoordelen worden de externe factoren onderschat en de invloeden van interne factoren overschat. Dit wordt de fundamentele attributiefout genoemd en kan ontstaan door vertekening uit eigenbelang, selectiviteit, veronderstelde overeenkomt, stereotypen, barnum-effect en het halo-effect [JANS02], [ROBB08]. Van vertekening uit eigenbelang is sprake als een individu het succes aan zichzelf toeschrijft en het falen aan andere factoren. Individuen kunnen niet alles verwerken wat ze zien, waardoor er sprake is van selectiviteit. Bij veronderstelde overeenkomt wordt de perceptie over andere mensen sterker beïnvloed door de karakteristieken van de waarnemer zelf, dan door de eigenschappen die bij andere mensen aanwezig zijn. Als men iemand beoordeeld op basis van de perceptie van de groep waartoe iemand behoort, is er sprake van een shortcut stereotype. Het barnum-effect gaat in op het feit dat mensen zichzelf goed in algemene beschrijvingen kunnen herkennen. Het halo-effect treedt op als men zich op basis van één kenmerk zoals intelligentie, omgangsvormen of uiterlijk een algemene indruk vormt.

Naast deze effecten is er vanuit het oogpunt van informatiebeveiliging voor de perceptie van risico's nog een belangrijk effect. Schneier geeft aan dat het verschil tussen gevoel van veiligheid en de veiligheid zoals die in werkelijkheid is, verklaard kan worden door de perceptie van risico's [SCHN08]. De veiligheid is een trade-off, en als men de kwetsbaarheid van een risico verkeerd inschat, dan gaat de trade-off verkeerd. De mens kan sommige risico's, zoals het risico van auto-ongevallen, onderschatten of juist overschatten. Hoe de mens het risico verkeerd inschat, wanneer hij het overschat en wanneer hij het onderschat kan duidelijk worden door een experiment waarin de prospect theorie geïllustreerd werd [GIGE99]. Er waren twee groepen, de eerste groep werd de keuze gegeven tussen deze twee alternatieven:

- Alternatief A: Een zekere winst van $500.
- Alternatief B: Een kans van 50% om $1.000 te winnen.

De tweede groep werd de keuze gegeven tussen:

- Alternatief C: Een zeker verlies van $500.
- Alternatief D: Een kans van 50% om $1.000 te verliezen.

Deze twee compromissen zijn niet hetzelfde, maar ze zijn zeer gelijkwaardig. De traditionele economie voorspelt dat de uitkomst geen verschil maakt. De alternatieven A en B hebben dezelfde verwachte uitkomst: + $500. En de alternatieven C en D hebben dezelfde verwachte uitkomst: -$500. De theorie voorspelt dat mensen de alternatieven A en C samen en B en D samen met dezelfde waarschijnlijkheid kiezen. Dus sommige mensen kiezen er voor om op zeker te spelen en sommige andere mensen kiezen om een gok te wagen. Het feit dat het één winst en het andere verlies betekent, beïnvloedt de wiskunde niet, en zou daarom de keuze ook niet moeten beïnvloeden. De auteurs van dit voorbeeld verklaarden het verschil in keuzes door de "prospect theorie". Deze theorie erkent, in tegenstelling tot de utility theorie, dat mensen bepaalde subjectieve waarden voor winst en verlies hebben. In feite hebben mensen een paar strategieën geëvolueerd die zij in dit soort compromissen kunnen toepassen. De eerste is dat de zekerheid van winnen beter is dan een grotere kans op winst (1 vogel in de hand is beter dan 10 in de lucht). De tweede is dat de zekerheid van verlies slechter is dan de kans op een groter verlies. Deze regels gelden alleen bij gelijkwaardige keuzes, dan beïnvloeden zij de wijzen waarop de mens compromissen sluit. In het algemeen zullen de meeste mensen een gelijke gokkans verwerpen (50% van het winnen, en 50% van het verliezen), tenzij er een mogelijkheid bestaat om minstens tweemaal de grootte van het mogelijke verlies te kunnen winnen.

Een vergelijkbaar voorbeeld is het "Asian disease" probleem van Tversky en Kahneman [TVER81]. Hierbij waren weer twee groepen, de eerste groep werd de keuze gegeven tussen deze twee alternatieven:

- Alternatief A: 200 mensen overleven het.
- Alternatief B: Er is 1/3 kans dat 600 mensen het overleven, en een 2/3 kans dat niemand overleeft.

De tweede groep werd de keuze gegeven tussen:

- Alternatief C: 400 mensen gaan dood.
- Alternatief D: Er is 1/3 kans dat niemand dood gaat, en een 2/3 kans dat 600 mensen dood gaan.

Net als in het eerste experiment hebben alternatieven A en B dezelfde opbrengst van 200 mensen overleven en 400 gaan er dood, waarbij A een zekerheid is en B een risico. Hetzelfde geldt voor alternatieven C en D; het enige verschil is dat A en B als een winst worden gepresenteerd en C en D als een verlies.

De uitkomst van het experiment was dat 72% van de mensen uit de eerste groep de voorkeur van A had en 78% van de mensen uit de tweede groep de voorkeur voor D had. De conclusie was dat mensen verschillende trade-off maken als iets in een winst of in een verliessituatie wordt gepresenteerd. Dit is bekend als het *framing effect* waarbij mensen worden beïnvloed door hoe een trade-off aan hun wordt gepresenteerd. Als een situatie als een winst wordt gepresenteerd zullen mensen geneigd zijn om risico's te mijden. Als een situatie als een verlies wordt gepresenteerd zullen mensen juist risico's nemen.

3.1.2.4 Motivatie

Motivatie gaat in op het bereidheid van een individu om zich in te spannen. Een algemene definitie is dat motivatie de bereidheid is om iets te doen, afhankelijk van de mate waarin het mogelijk is om een behoefte van het individu te bevredigen. Hierbij is een behoefte het fysiologische of psychologische tekort dat een bepaalde uitkomst aantrekkelijk maakt [ROBB02]. Binnen motivatietheorieën wordt er in de literatuur onderscheid gemaakt tussen vroegere theorieën over motivatie, zoals de hiërarchie van behoeften, de X – Y- theorie, de motivatiehygiëne theorie, de ERG- theorie en de drie behoeften theorie en de moderne theorie over motivatie zoals de doelstellingstheorie, de bekrachtigingstheorie, de waarde- verwachtingstheorie en de rechtvaardigheidstheorie [BRAT07], [ROBB08]. Naast dit onderscheid kan er nog naar het waarvoor en het hoe van motivatie gekeken worden. Het waarvoor heeft betrekking op de inhoudstheorieën van motivatie en het hoe op de procestheorieën van motivatie [BRAT07], [HITT05], [JANS02]. Inhoudstheorieën zoals de hiërarchie van behoeften theorie, de X – Y- theorie, de ERG- theorie, de motivatiehygiëne theorie, de drie behoeften theorie gaan in op de vraag: wat wil men bereiken?, Waartoe heeft men de inspanning gedaan?, Waaraan heeft men behoefte?, Waarom gaat het?, Waarnaar streeft men? En waarvandaan wil men? Deze motivatietheorieën houden zich dus bezig met de behoeften van werknemers en welke factoren op het werk deze behoeften kunnen bevredigen. Procestheorieën zoals de doelstellingstheorie, de bekrachtigingstheorie, de waarde-verwachtingstheorie en de rechtvaardigheidstheorie proberen een antwoord te geven op de vraag hoe het zingevings- of constructieproces in elkaar zit. Dit gaat door middel van de manier waarop de verschillende factoren gecombineerd worden om behoeften van werknemers te bevredigen. Hieronder zullen de verschillende motivatietheorieën kort besproken worden.

De hiërarchie van behoeften van Abraham Maslow is een bekende theorie rond motivatie [MASL54]. Zijn hypothese is dat aan het gedrag van ieder individu een hiërarchie van een vijftal basisbehoeften ten grondslag ligt. De behoeften die worden onderscheiden zijn fysiologische, zekerheid/veiligheid, sociale acceptatie, waardering/respect en zelf- verwerkelijking. Deze vijf soorten van behoeften zijn verdeeld in een laag en een hoog niveau in een piramidevorm.

Figuur 3: Hiërarchie piramide van behoeften [MASL54]

Er zijn twee uitgangspunten die Maslow heeft. De eerste is dat als er een tekort aan of onbevredigde behoefte is dit zal leiden tot activiteit en beweging van de mens. De tweede is dat behoeften een vaste hiërarchische ordening hebben. De theorie wordt niet door onderzoeksresultaten bevestigd, maar wordt nog wel veelvuldig toegepast in de bedrijfspraktijk.

De X – Y- theorie van McGregor is een uitwerking voor arbeidsorganisaties van Maslows theorie [MCGR60]. McGregor maakt onderscheid tussen twee verschillende mensbeelden. Het eerste mensbeeld is negatief en vormt de X- theorie. Het tweede mensbeeld is positief en vormt de Y-theorie. Hieronder is de X- en Y- theorie in een schema weergeven:

Uitgangspunten bij theorie X van McGregor:	Uitgangspunten bij theorie Y van McGregor:
• De mens heeft een aangeboren afkeer van werken en is dus lui; • De mens is niet verantwoordelijk en niet zo betrokken bij organisaties; • De mens geeft er de voorkeur aan te worden gestuurd en gecontroleerd; • De mens wil zekerheid.	• De mens is van nature geneigd te werken; • de mens kan zichzelf richten en leiden naar doelstellingen waar hij zich achter heeft gesteld; • De mens voelt zich verantwoordelijkj voor werk en wil betrokken zijn bij de organisatie; • De mens is ambities, vindingrijk en creatief.

Figuur 4: X – Y- theorie van McGregor [MCGR60]

De motivatiehygiëne theorie van Herzberg gaat er vanuit dat iemands relatie tot het werk bepaald is door succes of mislukking [HERZ59]. Hierbij wordt onderscheid gemaakt tussen twee groepen van behoeften. De eerste groep wordt aangeduid als *hygiënische factoren*. Hier moet men denken aan

bijvoorbeeld veiligheid, promotie, salaris, status en werkomstandigheden wat extrinsiek aan het werk is. Voor deze werkextrinsieke motieven geldt dat afwezigheid leidt tot ontevredenheid en bevrediging leidt tot een neutrale toestand van verzadiging en voldoening. De tweede groep wordt aangeduid als werkintrinsieke motieven die te maken hebben met de uitdaging die van het werk zelf uitgaan. Hier moet men denken aan de mogelijkheid tot presteren, erkenning, plezier in het werk en verantwoordelijkheid wat intrinsiek aan het werk is. Voor deze motivators geldt dat afwezigheid leidt tot een neutrale toestand en bevrediging leidt tot voldoening.

De ERG- theorie van Alderfer stelt dat er drie soorten behoeften zijn [ALDE72]. De eerste zijn existentiële behoeften, waarbij behoefte is aan materiële zekerheid, goede werkomstandigheden en een vast salaris. Existentiële behoeften komen overeen met de fysiologische behoeften en veiligheid van Maslow. De tweede zijn relationele behoeften, waarbij behoefte is aan goede relaties met andere mensen, liefde en vriendschap. Relationele behoeften komen overeen met de sociale- en erkenningsbehoeften van Maslow. De derde zijn groeibehoeften waarbij behoefte is aan persoonlijke groei en zelfontplooiing. Groeibehoeften komen deels overeen met de zelfactualiseringsbehoeften van Maslow.

De drie behoeften theorie van McClelland stelt dat er drie belangrijke behoeften bestaan op het werk [MCCL61]. De eerste behoefte is prestatie. Dit komt tot uitdrukking bij de drang om uit te blinken, iets bereiken volgens bepaalde maatstaven of succes te hebben. De tweede behoefte is macht. Dit komt tot uitdrukking om anderen te beïnvloeden zodat zij zich anders gaan gedragen dan ze anders zouden hebben gedaan. Als laatste behoefte noemt McClelland affiliatie. Dit komt tot uitdrukking bij de wens tot vriendschap en interpersoonlijke relaties.

De doelstellingstheorie van Locke heeft betrekking op de relatie tussen veelal door anderen gestelde doelen en gedrag [LOCK84]. Afhankelijk van het object waarop deze theorie zich richt zoals tijd, geld of veiligheid, gaat het om doelen, standaards, taken, enzovoort. Bij deze motivatietheorie is het uitgangspunt dat specifieke en voldoende uitdagende doelen leiden tot betere prestaties. Dit in tegenstelling tot eenvoudige of vage doelen en zelfs helemaal geen doelen. Er zijn wel een viertal voorwaarden die aan specifieke en voldoende uitdagende doelen worden gesteld. Ten eerste is dat de persoon die het doel moet bereiken wel voldoende bekwaam is. Ten tweede moet er sprake zijn van commitment met het te bereiken doel. Ten derde moet er voldoende ondersteuning vanuit de omgeving zijn. Als laatste moet er regelmatig specifieke feedback zijn over de mate waarin de gestelde doelen behaald zijn.

De bekrachtigingstheorie is de tegenhanger van de doelstellingstheorie, wat een cognitieve benadering is die stelt dat het individu zijn daden doelgericht stuurt [LUTH84]. De bekrachtigingstheorie gaat uit van het behaviorisme, dat stelt dat gedrag door bekrachtiging geconditioneerd wordt. Gedrag wordt gestuurd door bekrachtigers of consequenties die direct volgen op een reactie en de kans vergroten dat het gedrag herhaald wordt. De bekrachtigingstheorie gaat voorbij aan de innerlijke belevingswereld en concentreert zich op wat er met een individu gebeurt als hij/zij die actie onderneemt. Strikt genomen is het geen motivatietheorie, omdat de eerste aanzet tot gedrag geen rol speelt. Maar het kan helpen om een goede analyse te maken van mogelijke factoren die het gedrag bepalen.

Bij de waarde-verwachtingstheorie (expectancy-value theory) van Vroom worden individuen gemotiveerd tot een bepaald gedrag als men verwacht daar redelijke opbrengsten mee te kunnen behalen [VROO64]. Hierbij zijn aspecten van de waarde van de opbrengsten die men wil bereiken en de verwachtingen dat die opbrengsten het gevolg zullen zijn van de inspanning die men levert relevant. De neiging om een bepaald gedrag te vertonen wordt bepaald door het product van de verwachting, valentie en de instrumentaliteit. Hierbij is de verwachting uit te drukken als een bepaalde inspanning die leidt tot een bepaalde prestatie. Valentie of subjectieve waardering is de kans

die men denkt te hebben om met meer inspanning betere resultaten, meer opbrengst of beloning te kunnen behalen. De instrumentaliteit van de prestatie is de opbrengst of de beloning.

Als laatste gaat de rechtvaardigheidstheorie in op de vergelijkingen die individuen maken binnen organisaties over inzet en beloning van hun werk in vergelijking met andere, waarbij de rechtvaardigheid de inzet van werknemers kan beïnvloeden [VECC84]. Werknemers wegen de opbrengsten en uitgaven van hun werk tegen elkaar af en vergelijken die met relevante andere. Als het eigen ratio gelijk is aan die van een ander, dan is de situatie gerechtvaardigd. Als het eigen ratio niet gelijk is, kan er sprake zijn van onrechtvaardigheid. Hierbij kunnen werknemers zich onder- of overgewaardeerd voelen en zullen ze deze onrechtvaardigheid proberen te corrigeren. Werknemers zijn niet alleen bezig met absolute inzet en beloning, maar ook met de relatieve verhouding tussen de eigen inzet en beloning, als wel met de beloning en inzet van anderen.

3.1.2.5 Emotie

Aan emoties zijn de termen affect en stemming nauw verwant. Emoties zijn intense gevoelens voor iets of iemand [FRIJ93]. Affect is een algemene term voor een breed scala aan menselijke gevoelens. Het is een overkoepelend begrip waaronder zowel emoties als stemmingen vallen [GEOR96]. Stemmingen zijn gevoelens die minder sterk zijn dan emoties en hebben geen prikkels vanuit de omgeving nodig [WEIS96]. In tegenstelling tot persoonlijkheid zijn emoties geen karaktertrekken. Het is een reactie op een bepaald object en zijn dus objectgebonden. Naast fysieke en mentale arbeid verricht een medewerker ook emotionele arbeid. Emotionele arbeid leidt tot dilemma's voor een medewerker als hun baan verlangt dat ze emoties tonen die niet overeenkomen met hun werkelijke gevoelens. Waardoor de werkelijke emoties worden onderdrukt. Hierbij kan onderscheid gemaakt worden tussen beleving en uiting van emoties [HOCH79]. Beleefde emoties zijn de werkelijke gevoelens die iemand heeft. De uiting van emoties zijn vanuit de organisatie gezien vereist of vanuit een bepaalde functie gezien nodig en zijn niet aangeboren, maar worden juist aangeleerd. Er bestaan een zestal universele emoties: woede, angst verdriet, geluk, afschuw en verbazing [WEIS96]. Emoties kunnen in twee typen situaties worden ingedeeld en met twee daaraan corresponderende soorten emoties. Ten eerste naar voordeelsituaties die aanleiding geven tot bijvoorbeeld vreugde, trots of dankbaarheid. Ten tweede naar nadeelsituaties waarbij er sprake is van schade, verlies of bedreiging die leiden tot bijvoorbeeld woede, angst, schuld, bedroefdheid, afschuw en verbazing.

Bij de cognitieve emotietheorie van Lazaruz wordt er van de volgende drie zaken uitgegaan [LAZA84]. Emotie is altijd:

- Relationeel, dat wil zeggen situatiegebonden;
- Motivationeel, dat wil zeggen emoties gaan altijd ergens om;
- Cognitief, dat wil zeggen dat een inschatting of waardering van de situatie, de aard of kleur van de emotie bepaalt.

Dit betekent dat men zich kan vergissen in een inschatting. Er kan dus een verkeerde emotie bij een individu zijn. In dat opzicht valt over gevoelens best te twisten. Men kan een individu aanleren een bepaalde situatie uitdagend en prettig te vinden in plaats van angstaanjagend en eng. Emoties kunnen aangeleerd of veranderd worden [JANS02].

3.1.2.6 Leren

Er wordt vanuit gegaan dat medewerkers iets doen omdat ze *zo zijn*, omdat ze het dus *zo willen*. Vergeten wordt dat medewerkers meestal niet op een bepaalde, bijvoorbeeld ineffectieve, manier handelen omdat ze dat zo willen, maar omdat de omgeving hen daartoe conditioneert. Gedrag is geconditioneerd door situatiekenmerken [JANS02]. Vrijwel alle complexe gedragingen van mensen zijn aangeleerd. Willen we gedrag verklaren, voorspellen of sturen, dan moeten we begrijpen hoe mensen leren [ROBB08]. Daarnaast wordt gedrag niet alleen gestuurd door de aanwezigheid van behoefte, maar ook door kenmerken van de situatie [ALBL05]. Er zijn twee populaire leertheorieën die ingaan op de relatie tussen behoefte en situatie. De eerste theorie is de instrumentele conditionering van Skinner [SKIN71]. Volgens deze theorie streven mensen naar bevrediging van hun behoefte. Hoe de mens dat doet en het gedrag dat men daarbij vertoont is afhankelijk van een leerproces, dat conditionering wordt genoemd. Veel gedrag van mensen komt automatisch tot stand. De mens heeft dat gedrag in de loop van zijn leven aangeleerd door het proces van instrumentele conditionering. Dit leerproces begint al op zeer jonge leeftijd. Het leerproces loopt dan vooral via gissen en missen. Dit leren is gebaseerd op de wet van het effect. Het proces loopt via een reeks van willekeurige handelingen die gericht zijn op het bevredigen van een behoefte. Als er in de reeks een handeling is die gevolgd wordt door succes, wordt de kans groter dat die handeling de volgende keer opnieuw vertoond wordt. De gevolgen van een handeling bepaalt of deze herhaald wordt. Wanneer de gevolgen aangenaam zijn, is dat een positieve bekrachtiging van de handeling. Gedrag dat gunstige gevolgen heeft zal dan worden herhaald. Als de gevolgen niet bevredigend zijn zal het negatief bekrachtigd worden, waardoor ze uit het handelingsrepertoire verdwijnen. Het gedrag met ongunstige gevolgen zal niet worden herhaald. Leren dat via conditionering plaatsvindt, verloopt onbewust en het individu vertoont het geleerde gedrag automatisch, zonder er bij na te denken. Het gedrag wordt geactiveerd door de aanwezigheid van een bepaalde behoefte. Maar welk gedrag precies tot stand komt wordt veroorzaakt door een bepaalde situatie.

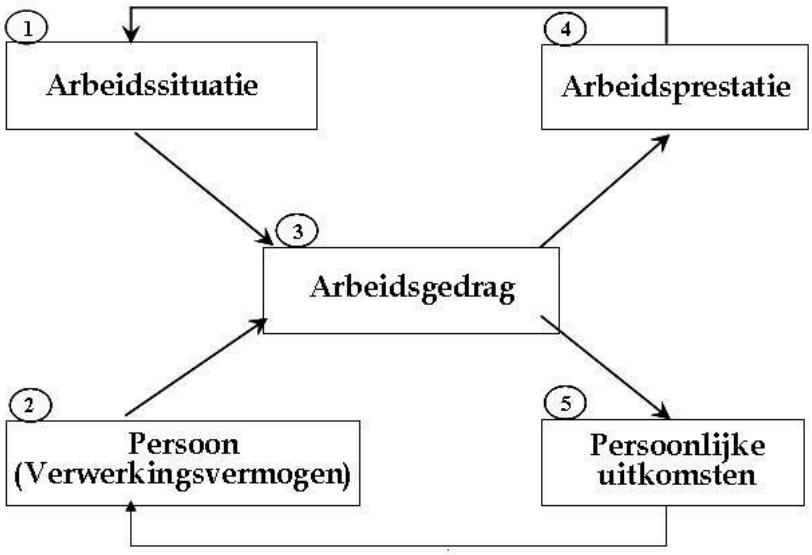
De tweede leertheorie is de sociaal-cognitieve leertheorie van Bandura, die een aanvulling vormt op de instrumentele conditionering van Skinner [BAND77]. Deze theorie stelt dat individuen via de observatie van wat er met andere mensen gebeurt en door het zelf direct te ervaren kunnen leren. Men kan dus ook leren door observatie en directe ervaring. De aanname van deze theorie is dat het gedrag van een individu een functie is van het gevolg, daarnaast reageren mensen door hoe zij bepaalde gevolgen waarnemen en niet zoals de objectieve gevolgen zelf zijn. Er is dus een verschil tussen de werkelijke gevolgen en de gevolgen zoals die door de mens wordt ervaren.

3.1.2.7 Capaciteiten

Robbins heeft *capaciteiten* toegevoegd aan zijn model, aangezien gedrag mede bepaald wordt door intelligentie, talenten en vaardigheden die iemand bezit en het vermogen om prestaties te leveren. Uiteraard zijn de capaciteiten van een individu in de loop der tijd ontwikkeld en zullen deze capaciteiten door nieuwe leerprocessen blijven veranderen. Van Dale geeft aan dat intelligentie een verstandelijk vermogen is. Intelligentie bij mensen is dan het verstandelijke vermogen van een individu. Veenman geeft aan dat intelligentie als situationele gedragssoort op de volgende drie zaken berust [VEEN94]:

- De beheersing van een aantal basale intellectuele vaardigheden (basisintelligentie).
- Het op de hoogte zijn van alle *ins* en *outs* van het veld waarin het vraagstuk ingebed is (domeinkennis).
- Het bezitten van kennis en kunde over hoe het vraagstuk aan te pakken (probleemaanpak).

Het verstandelijke vermogen van een individu bepaalt mede wat de mentale arbeidsbelasting van een individu is. Kompier en Houtman stellen dat mentale belasting die vorm van arbeidsbelasting is, welke het gevolg is van de opname, opslag en verwerking van informatie en de vertaling daarvan in motorische reacties. Mentale belasting is te omschrijven als de mate waarin taakeisen de informatieverwerkende capaciteit van de mens in beslag nemen [KOMP04].



Figuur 5: Het X-model voor arbeid van Roe en zijstra [ROE91]

In het X-model van de handelingstheorie is te zien dat het persoonlijke verwerkingsvermogen invloed heeft op het arbeidsgedrag dat een individu kan vertonen. De concepten uit het X-model zijn in figuur 5 schematisch weergegeven en kunnen als volgt worden toegelicht: De arbeidssituatie (1) zijn omstandigheden, voorwaarden en verhoudingen waaronder de arbeid wordt verricht. Daarnaast bepaaldt het verwerkingsvermogen of verwerkingscapaciteit van een persoon (2) hoe goed hij of zij in staat en bereid is om de arbeidstaak naar behoren uit te voeren De arbeidssituatie samen met het verwerkingsvermogen van een persoon bepalen de uikomst van het arbeidsgedrag (3), door in de praktijk de arbeidshandelingen uit te voeren. leidt tot de arbeidprestatie (4) en een persoonlijke uitkomsten (5). De arbeidsprestatie is hierbij de mate waarin aan de kwaliteit en kwantiteit gestelde normen wordt tegemoet gekomen, die op zijn beurt weer de arbeidssituatie beïnvloedt. De persoonlijke uitkomsten zijn de positieven- (satisfactie, leren) en negatievenuitkomsten (stress, vermoeidheid) voor de taakuitvoerder. De handelingstheorie en het X-model kunnen worden beschouwd als een raamwerk waarin verschillende modellen en hypothesen uit de cognitieve en ergonomische psychologie tot een samenhangend geheel geïntegreerd zijn [ROE91].

Volgens deze theorie kan het arbeidsgedrag van een mens beschouwd worden als opgebouwd zijnde uit afzonderlijke handelingen, die weer verder onderverdeeld kunnen worden in verschillende deelhandelingen en die weer in operaties. Hierbij is een handeling gedefinieerd als de kleinste eenheid van activiteit waarbij nog sprake is van een gerichtheid op een zelfstandig, bewust ervaren doel; dit in de zin van een bepaald arbeidsresultaat. Hierbij omvatten handelingen zowel motorische als sensorische en cognitieve processen. Middels een handelingsplan, ofwel een innerlijk model, worden handelingen uitgevoerd. Dit handelingsplan heeft een hiërarchisch-sequentiële opbouw die loopt van handeling naar deelhandeling en uiteindelijk leidt tot een operatie. De feitelijke opbouw van een handeling en de handelingsstructuur kan bij hetzelfde doel zeer verschillend zijn door invloeden van

interne en externe factoren. Er zijn dynamische verschillen in handelingsstructuren bij dezelfde persoon. De handelingsstructuren worden vormgegeven door een reeks van regulerende processen. Zo wordt een arbeidsopdracht vertaald naar een arbeidsopgave. Dit behelst de oriëntatie op persoonlijke- en omgevingsvoorwaarden, waarna een gedragsprogramma wordt ontworpen of gereproduceerd indien er reeds een eerder ontwerp is. Vervolgens moet er een keuze plaatsvinden binnen de aanwezige ruimte om een gedragsprogramma om te zetten tot een plan voor het handelen of een eerder gekozen handelingsplan te actualiseren, waarmee de handelingsvoorbereiding ten einde is. Uiteindelijk wordt stapsgewijs het handelingsplan uitgevoerd onder voortdurende cognitieve controle, wat de handelingsuitvoering vormt.

Regulerende processen spelen zich op drie niveaus van informatieverwerking af [RASM83] [20]. Sensomotorische regulering (skill-based): de handelingsuitvoering wordt gestuurd door een eerder gevormd handelingsplan en verloopt voor een groot deel onbewust via geautomatiseerde operaties of bewegingen. Perceptief-conceptuele regulering (rule-based): hierbij is sprake van een eerder gevormd handelingsplan waarvan de afwikkeling in sterke mate afhankelijk is van de waarnemingen, enerzijds van signalen of prikkels, anderzijds van het verloop en de gevolgen van het eigen handelen, waarbij er bewust beslissingen worden genomen die verlopen volgens vaste regels. Intellectuele regulering (knowledge-based): in dit geval worden nieuwe handelingsplannen ontwikkeld door analyse van doel en randvoorwaarden. Het handelingsplan wordt bewust en stapsgewijs uitgevoerd. Aan de hand van feedback over het resultaat kan het handelingsplan eventueel worden bijgesteld.

De drie reguleringsniveaus verschillen in de mate waarin ze een beroep doen op de mentale capaciteit die voor de uitvoering nodig is. Daarnaast kunnen de reguleringsniveaus elkaar afwisselen binnen eenzelfde handeling. Het afwisselen van reguleringsniveaus treedt onder andere op wanneer de taakuitvoerder fouten maakt of zichzelf in onverwachte situaties bevindt.

De handelingsregulering is ook afhankelijk van de fysieke en mentale conditie van de taakuitvoerder. Mensen hebben de neiging tot vergroting van de handelingsefficiëntie, enerzijds door het bewust zoeken naar mogelijkheden voor rationalisering tijdens de handelingsvoorbereiding, anderzijds door leerprocessen tijdens de handelingsuitvoering. Door meer ervaring in de taakuitoefening en wanneer het leerproces verder is voortgeschreden, zal het reguleringsniveau lager zijn.

Ieder individu beschikt over een uitgebeid handelingsrepertoire en een omvangrijke kennis waarop in de handelingsvoorbereiding en -uitvoering een beroep kan worden gedaan. Het handelen heeft gevolgen voor de taakuitvoerder, enerzijds biedt het gelegenheid tot leren waardoor de kennis, kundigheid en het gedragsrepertoire worden vergroot. Anderzijds brengt het, al naar gelang de geleverde inspanning, belasting en vermoeidheid teweeg.

3.1.3 Sociaal psychologische modellen

We hebben tot nu toe attitude, persoonlijkheid, perceptie, motivatie, emotie, leren en capaciteiten behandeld, wat aspecten zijn die het individuele gedrag in organisaties beïnvloeden. Maar leidt een positieve attitude van individuen ten aanzien van informatiebeveiliging ook tot het zorgvuldig handelen van een individu met betrekking tot informatiebeveiliging? Leidt een hogere perceptie van een individu ten aanzien van informatiebeveiliging tot het gewenste gedrag van een individu ten aanzien van informatiebeveiliging? Dit zal niet automatisch het geval zijn. Als men bijvoorbeeld de attitude of motivatie van een individu weet, dan is het gedrag van datzelfde individu nog niet

[20] De drie niveaus van informatieverwerking worden verderop besproken.

voorspelbaar. Dit komt doordat er nog een andere factor is die een rol speelt. Zo kan de relatie tussen attitude of motivatie met betrekking tot het gedrag in de ene situatie sterk zijn, maar in een andere situatie juist weer zwak. Als eerste zal de theorie van gepland gedrag besproken worden die als uitgangspunt voor dit onderzoek geldt. Hierna zal worden ingegaan op de sociaal-cognitieve theorie die net als de theorie van gepland gedrag, een verklaring geeft voor gedrag om het te kunnen begrijpen, te kunnen voorspellen en te kunnen veranderen. Als laatste zal ingegaan worden op de user acceptance models die specifiek ingaan op het verklaren waarom mensen informatie technologie zouden gebruiken.

3.1.3.1 Theorie van Gepland Gedrag

Het uitgangspunt wordt gevormd door de intentie van een individu om bepaald gedrag te vertonen, wat de gedragsintentie (behavioral intention) wordt genoemd. Welke rol dit speelt wordt duidelijk in het model van de *Theorie van Gepland Gedrag* (TpB) die door Ajzen en Fishbein is ontwikkeld [AJZE91]. De theorie van gepland gedrag is een uitbreiding op de *Theorie van Beredeneerde Actie* [AJZE75], [FISH80]. Deze theorie is familie van de Expectancy Value theorie en is gebaseerd op het concept dat gedrag gemotiveerd wordt door de verwachtingen die men heeft over de gevolgen van het gedrag en de waarde die men hecht aan die gevolgen. Hier neemt men aan dat mensen rationele wezens zijn, maar deze veronderstelling van rationaliteit is niet zonder kritiek. Mensen zijn beperkt in hun cognitieve capaciteiten en deze spelen een belangrijke rol bij het maken van vele keuzes. Hierdoor zouden routines of gewoontes een barrière kunnen vormen voor de toepasbaarheid van de theorie van gepland gedrag [AART98], [VERP98]. Daarnaast is er geen plaats voor emotionele aspecten. Als laatste veronderstelt men dat behoeften onverzadigbaar zijn en dat mensen enkel uit eigenbelang handelen. De theorie van beredeneerde actie beschrijft de invloed van *attitude toward the behavior* en de *subjective norm* op de gedragsintentie; hierbij werd geen aandacht besteed aan de *perceived behavioral control*[21]. De uitbreiding hierop was noodzakelijk, omdat het originele model beperkingen vertoonde bij gedrag, waarover het individu niet de volledige controle heeft. In de theorie van gepland gedrag is de individuele intentie een centrale factor om bepaald gedrag te vertonen. De Theorie van Gepland Gedrag van Ajzen gaat ervan uit dat gedrag te voorspellen is door naar de intentie van mensen te vragen die zij hebben ten aanzien van bepaald gedrag. Daarbij wordt verondersteld dat de intenties de motivationele factoren zijn die het gedrag beïnvloeden. Deze motivators bepalen hoe graag een individu bereid is om een bepaalde hoeveelheid inspanning te leveren om bepaald gedrag te vertonen. Hoe sterker de intentie om bepaald gedrag te vertonen, des te waarschijnlijker het is dat dit gedrag ook daadwerkelijk wordt vertoond. Daarbij is de attitude met betrekking tot een bepaald object niet zozeer van belang, maar met name de attitude tegenover een bepaald gedrag[22] is beslissend voor het al dan niet vertonen van dat gedrag. Een voorwaarde is dan wel dat dit gedrag onder de controle moet zijn van het desbetreffende individu, zodat hij kan beslissen om het gedrag wel of niet te vertonen, zodanig dat een individu de vereiste mogelijkheden, middelen en intenties heeft om bepaald gedrag te vertonen. Hierbij wordt de menselijke actie geleid door drie soorten *beliefs*. De *behavioral beliefs* gaan in op de waarschijnlijke resultaten van het gedrag en de evaluaties van deze resultaten. De *normative beliefs* zijn de normatieve verwachtingen of sociale druk (*strength of normative beliefs*) van andere mensen en motivaties (*motivation to comply*) om deze verwachtingen na te leven. De *control beliefs* gaan in op de aanwezigheid van factoren die het gedrag kunnen vergemakkelijken of juist kunnen belemmeren. Een *belief* kan men beschouwen als een cognitie met een bepaalde sterkte, welke de *belief*-sterkte wordt genoemd.

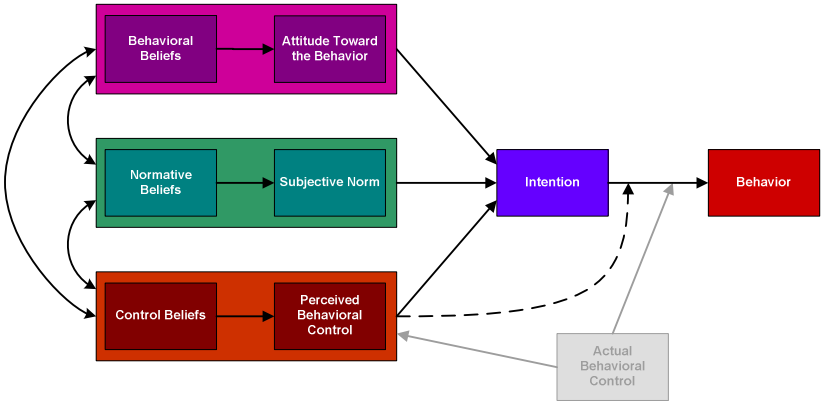
[21] Niet te verwaren met interne en externe locus of control waarbij het gaat om een grootte verscheidenheid aan gedragingen en verwijst niet naar de verwachte eenvoud of moeilijkheid waarmee men gedrag kan uitvoeren.

[22] Zoals in dit onderzoek gedrag ten aanzien van informatiebeveiliging.

Bij deze drie *beliefs* wordt een beroep gedaan op de *salient beliefs* van een individu. De *salient beliefs* zijn de eerste zaken die bij een respondent in zijn gedachten opkomen als er een vraag wordt gesteld zoals: *wat zijn de voordelen voor u bij het uitvoeren van gedrag X?* [SUTT03]. Hierbij wordt ook wel verwezen naar *accessible beliefs*, waarmee *beliefs* worden aangesproken die gemakkelijk en direct toegankelijk zijn in het geheugen. Hierbij kan onderscheid gemaakt worden tussen *personal salient beliefs* en *modal salient beliefs*. De *personal salient beliefs* gaan in op zaken die bij een individuele respondent uniek in zijn gedachten opkomen, in tegenstelling tot *modal salient beliefs* waarbij het gaat om zaken die bij een groep of populatie als gemeenschappelijke gedachten gelden.

Vanuit de *behavioral beliefs* komt een positieve of negatieve *attitude toward the behavior*. De *normative beliefs* geven invulling aan de *subjective norm* en de *control beliefs* leiden tot de *perceived behavioral control*. De combinatie van de *behavioral beliefs,* de *normative beliefs* en de *control beliefs* vormen samen een gedragsintentie. Er wordt verondersteld dat de gedragsintentie direct vooraf gaat aan het gedrag. Als algemene regel geldt dat hoe gunstiger de *attitude toward the behavior*, de *subjective norm* is, en hoe groter de *perceived behavioral control* is, des te sterker zal de intentie van de persoon zijn om het gedrag in kwestie uit te voeren. De *attitude toward the behavior*, de *subjective norm* en de *perceived behavioral control* vormen de drie centrale onafhankelijke *directe* variabelen. De *behavioral beliefs*, de *normative beliefs* en de *control beliefs* vormen de drie centrale onafhankelijke *indirecte* variabelen.

De gedragsintentie wordt verklaard door de *attitude toward the behavior*, de *subjective norm* en de *perceived behavioral control*. Het werkelijke gedrag wordt uiteindelijk bepaald door de intentie om het gedrag te vertonen en door de *perceived behavioral control*. Als algemene regel geldt dat, hoe positiever de drie determinanten samenhangen, hoe sterker de intentie van de persoon zal zijn, om het gedrag in kwestie uit te voeren. Als laatste wordt verwacht dat een persoon zijn intentie tot gedrag zal omzetten tot werkelijk gedrag, als de situatie zich voordoet en als er voldoende werkelijke controle is over het gedrag. Hieronder is de theorie van gepland gedrag schematisch weergegeven, daarnaast zullen de verschillende concepten binnen dit model worden toegelicht[23]. [AJZE70], [AJZE73], [AJZE77], [AJZE80], [AJZE85], [AJZE88], [AJZE91], [AJZE02], [AJZE06], [AJZE08], [AJZE08a], [AJZE08b], [FISH67], [FISH75], [FISH76].



Figuur 6: Theorie van gepland gedrag [AJZE06]

De *attitude toward the behavior (a)* heeft twee componenten: enerzijds een directe evaluatie of waardering, waarbij bepaald gedrag wordt geëvalueerd op basis van een dimensie, bijvoorbeeld: *goed* versus *slecht* of *prettig* versus *vervelend*. De evaluatie of waardering gaat in op de mate waarin bepaalde prestaties om gedrag te vertonen, positief of negatief worden beoordeeld. Anderzijds is er een

[23] http://people.umass.edu/aizen/tpb.diag.html

indirecte component de *behavioral beliefs* die men kan beschouwen als een cognitie met een bepaalde sterkte, welke de *behavioral belief strength (b)* wordt genoemd. Hierbij wordt op basis van kennis of ervaring een zekere subjectieve waarschijnlijkheid toegekend aan het optreden van bepaalde consequenties van gedrag. Daarnaast vindt er een evaluatie plaats van de consequenties van dat gedrag, wat de *outcome evaluation (e)* vormt. Hoewel een individu vele *behavioral beliefs* kan hebben ten aanzien van bepaald gedrag, is er slechts een klein aantal gemakkelijk toegankelijk op een bepaald moment. De veronderstelling is dat de *behavioral belief strength (b)*, in combinatie met de subjectieve waarden van de verwachte *outcome evaluation (e)*, samen de *attitude toward the behavior (a)* bepalen. De afzonderlijke bijdrage van de *behavioral beliefs* aan de uiteindelijke *attitude toward the behavior (a)* kan nu worden berekend door de *behavioral belief strength (b)* te vermenigvuldigen met de *outcome evaluation (e)* van een bepaalde gedragsconsequentie. De *attitude toward the behavior (a)* als geheel is gebaseerd op de som van alle mogelijke geëvalueerde *behavioral beliefs* en ziet er als volgt uit: $a = \sum b_i e_i$.

De *subjective norm (sn)* is de norm die vanuit de sociale omgeving druk uitoefent op een individu om bepaald gedrag wel of niet te vertonen. Het gaat hierbij om indrukken die een individu heeft van de normatieve opvattingen van andere individuen, die verondersteld worden een belangrijke rol te spelen bij het verklaren van intenties en gedragingen. Hierbij wordt er onderscheid gemaakt tussen *descriptive-* en *injunctive norms*. De *descriptive norms* gaan in op de perceptie die een individu heeft ten aanzien van wat referentiepersonen uit de omgeving werkelijk doen. De *injunctive norms* gaan in op de perceptie die een individu heeft ten aanzien van wat referentiepersonen uit de omgeving vinden dat hij of zij zou moet doen. Verondersteld wordt dat men de *subjective norm (sn)* door de totale reeks toegankelijke *normative beliefs strengths (n)* betreffende de verwachtingen van belangrijke referentiepersonen kan worden bepaald. De sterkte van de *normative beliefs* wordt bepaald aan de hand van waarderingen over de opvattingen van referentiepersonen uit de omgeving van het individu, die voor hem of haar belangrijk zijn. Daarnaast vindt er een waardering plaats die aangeeft in welke mate een individu zich wil conformeren met de referentiepersonen in kwestie, wat de *motivation to comply (m)* vormt. De *motivation to comply (m)* kan hier beschouwd worden als een intentie tot bepaald gedrag. De *normative beliefs strengths (n)* verwijzen naar de waargenomen gedragsverwachtingen van dergelijke belangrijke referentiepersonen of groepen zoals de supervisor of naaste collega's van een individu. Daarnaast is het belangrijk om te weten in hoeverre men zich iets aantrekt van de verwachte opvattingen van anderen. Hierbij hoeft de sociale norm die men waarneemt niet overeen te komen met de daadwerkelijke sociale normen die optreden. Men veronderstelt dat deze *normative beliefs strengths (n)*, in combinatie met de *motivation to comply (m)* van het individu om de verschillende normatieve opvattingen na te leven, de *subjective norm* bepaalt. Het schatten van de opvattingen van andere mensen binnen de sociale context van een individu worden de *normative beliefs strengths (n)* genoemd. De mate waarin men geneigd is zich iets aan te trekken van de mening van een ander vormt de *motivation to comply (m)*, en is de motivatie om te conformeren aan de gewenste sociale context. De *subjective norm (sn)* als geheel is gebaseerd op de som van alle *normative beliefs strengths (n)* gewogen door de *motivation to comply (m)*. Aan beide begrippen wordt een waarde en een sterkte toegekend waardoor de formule er als volgt uit ziet: $sn = \sum n_i m_i$.

De *perceived behavioral control (pbc)* verwijst naar de verwachte eenvoud of moeilijkheid waarmee men gedrag kan uitvoeren. Verondersteld wordt dat zowel eerdere ervaringen als verwachte hindernissen of obstakels erin naar voren komen. Hierbij gaat het om een zelfwaarneming van de mate waarin een individu zelf denkt succesvol te zijn in het uitvoeren van bepaald gedrag. Hierbij gaat het om de perceptie van een individu ten aanzien van zijn capaciteit (*self-efficacy*) en controle (*controllability*) om bepaald gedrag uit te voeren. Het is een conceptuele aanvulling op de *Theorie van Beredeneerde Actie*, om gedragsintenties en rechtstreeks gedrag uit te voeren. Door dit concept aan het model toe te voegen kunnen gedragingen worden verklaard, waarbij sprake is van gedrag dat niet onder de controle is van een individu of buiten zijn capaciteit ligt. In analogie met de verwachtingstheorie veronderstelt men dat de *perceived behavioral control (pbc)* een totale reeks toegankelijke *control beliefs strengths (c)* geven die een waardering vormen van een individu ten aanzien

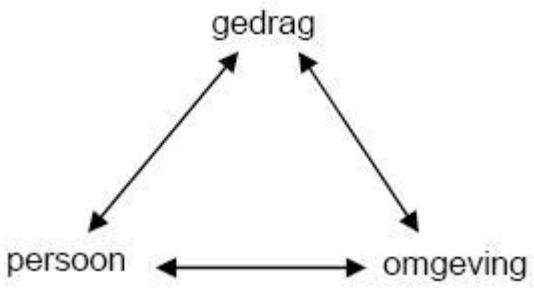
van de mogelijkheden om het gedrag uit te voeren. Hierbij kan de sterkte van de *control beliefs* het gedrag vergemakkelijken of belemmeren. Daarnaast vormt de *control belief power (p)* een subjectieve waarschijnlijkheid dat een individu, tegenwerking of obstakels kan overwinnen zodat het gedrag uitgevoerd kan worden. Alle *control beliefs strengths (c)* worden vermenigvuldigd met de *control belief power (p)*. De *perceived behavioral control (pbc)* formule ziet er als volgt uit: $pbc = \sum c_i p_i$.

Het *daadwerkelijk gedrag* en de *gedragsintentie* vormen de twee centraal afhankelijke variabelen. De eerste is de intentie (intention) tot gedrag, die wordt bepaald door de *attitude toward the behavior*, de *subjective norm* en de *perceived behavioral control*. De *gedragsintentie* is een indicatie van de bereidheid om bepaald gedrag uit te voeren, en het wordt beschouwd als direct voorafgaand aan het *actual behavioral control*. De tweede is het feitelijk gedrag (behavior) dat de manifestatie is van de waarneembare reactie bij een individu in een bepaalde situatie met betrekking tot een bepaald doel. Er zijn een tweetal problemen die zich voordoen bij het meten van het gedrag. Ten eerste is het lastig om gedrag te meten. Ten tweede komt het gedrag altijd na de gedragsintentie, waardoor het niet gelijktijdig gemeten kan worden.

Het *actual behavioral control* verwijst naar de mate waarin een individu de vaardigheden, kennis, eigen middelen en andere eerste vereisten nodig heeft om bepaald gedrag uit te voeren of te kunnen vertonen. Het succesvol uitvoeren van gedrag hangt niet alleen af van een positieve gedragsintentie, maar hangt ook van een voldoende niveau van *perceived behavioral control* af. Dit moet zodanig zijn dat de *perceived behavioral control* nauwkeurig is, omdat het een afspiegeling is van de feitelijke controle over gedrag. De *perceived behavioral control* ten opzichte van het uit te voeren gedrag bepaalt gezamenlijk met de gedragsintentie of het gedrag uitgevoerd wordt. Het verwachte directe verband tussen *perceived behavioral control* en de gedragsintentie berust op de veronderstelling dat *perceived behavioral control* motivationele implicaties heeft voor de gedragsintentie. Situationele belemmeringen zorgen ervoor dat, wanneer een individu bepaald gedrag wil vertonen, dit door interne en externe barrières belemmerd wordt. Van interne barrières is sprake wanneer iets in de persoon zelf weerstand biedt om bepaald gedrag uit te voeren. Van externe barrières is sprake wanneer er omgevingsfactoren zijn die een individu ervan weerhoudt om bepaald gedrag uit te voeren.

3.1.3.2 Sociaal-cognitieve theorie

Naast de theorie van Ajzen [AJZE91] is er door Bandura de sociaal-cognitieve theorie [BAND86], [BAND99] ontwikkeld, wat een uitwerking is van de sociale leertheorie [BAND77]. Het geeft, net als de theorie van Ajzen, een verklaring voor gedrag om het te kunnen begrijpen, te kunnen voorspellen en te kunnen veranderen. Hierbij wordt menselijk gedrag gezien als een interactie tussen persoonlijke factoren, gedrag en omgeving. Hieronder is het model van de sociaal-cognitieve theorie schematisch weergegeven, daarnaast zal er een korte toelichting worden gegeven met betrekking tot de verschillende concepten binnen dit model.

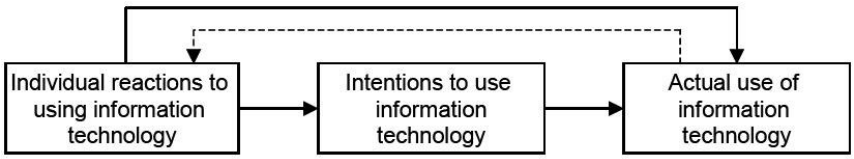


Figuur 7: Sociaal-cognitieve theorie [BAND86]

Het model impliceert dat de interactie tussen de persoon en het gedrag bepaald wordt door de invloeden van de gedachten en de acties van een persoon. De interactie tussen de persoon en de omgeving impliceert de menselijke overweging of *belief* als wel de cognitieve bekwaamheden die worden ontwikkeld door sociale invloeden of gewijzigd worden door invloeden vanuit de omgeving. De derde interactie vindt plaats tussen de omgeving en het gedrag. Deze interactie impliceert dat het gedrag van een persoon de aspecten van zijn omgeving bepaalt en omgekeerd wordt het gedrag van een persoon gewijzigd door zijn omgeving. Binnen het model van Bandura spelen de verwachte gevolgen van gedrag, c.q. de verwachting of men in staat is om het gedrag uit te voeren en het zelf stellen van doelen[24] en strategieën hanteren om deze te bereiken, een belangrijke rol. Het ASE-model van de Vries [VRIE88] is gebaseerd op de theorie van gepland gedrag en inzichten van de sociaal-cognitieve theorie, waardoor het geen aanvulling is voor de theorievorming en niet verder toegelicht zal worden.

3.1.3.3 User Acceptance Models

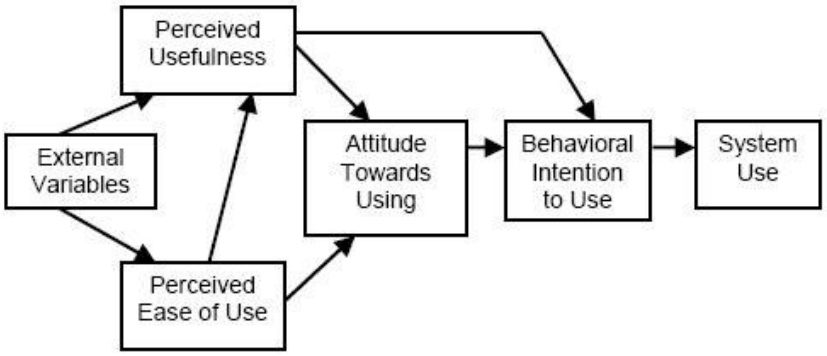
Naast de ontwikkelde theorieën door Ajzen en Bandura om gedrag te verklaren is er vanuit het informatiesystemenonderzoek een theorie ontwikkeld die tracht te verklaren waarom mensen informatietechnologie zouden gebruiken. Het basisconcept hierbij is dat individuele reacties om informatietechnologie te gebruiken bepalend zijn voor de gedragsintentie om een informatiesysteem te gebruiken. Vervolgens is deze gedragsintentie bepalend voor het werkelijk gebruik van informatietechnologie. Hieronder is het basisconcept voor het gebruik van informatietechnologie schematisch weergegeven:



Figuur 8: Het basisconcept van User Acceptance Models [VENK03]

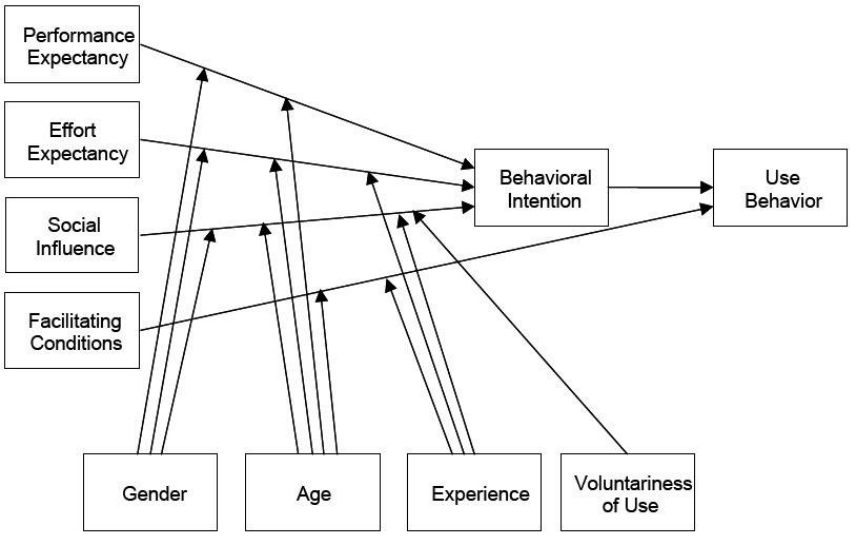
Het *technology acceptance model* is ontwikkeld door Davis en is gebaseerd op de *theorie van beredeneerde actie*, waarbij aanpassingen zijn gemaakt om het te kunnen gebruiken binnen het onderzoeksgebied van de informatietechnologie [DAVI89]. Het model van Davis gaat er vanuit dat de *perceived usefulness* en de *perceived ease of use* de onafhankelijke variabelen zijn die de individuele gedragsintentie om de informatietechnologie te gebruiken bepalen. Vervolgens bepaalt deze gedragsintentie of de informatietechnologie ook werkelijk wordt gebruikt. De *perceived usefulness* is de mate waarin de informatietechnologie als beter wordt gezien. Het bepaalt in hoeverre de acceptatie van de informatietechnologie in de ogen van de gebruiker een voordeel oplevert. De *perceived ease of use* is hierbij de mate waarin een individu verwacht dat het gebruiken van de informatietechnologie gemakkelijk of moeilijk zal zijn. De *perceived usefulness* heeft volgens Davis invloed op de *attitude toward using* en op de gedragsintentie tot acceptatie. de *perceived ease of use* heeft volgens dit model invloed op de *perceived usefulness* en ook direct op de *attitude toward using*. De *attitude toward using*, gedragsintentie, *attitude toward using* en het *daadwerkelijk gedrag* zijn ook terug te vinden in de *theorie van beredeneerde actie*. Hieronder is het model van Davis schematisch weergegeven:

[24] Dit wordt binnen de sociaal-cognitieve theorie met de term self-efficacy aangeduid en is in analogie met perceived behavioral control uit de theorie van gepland gedrag.



Figuur 9: Technology acceptance model [DAVI89]

De *unified theory of acceptance and use of technology* is ontwikkeld door Venkatesh e.a en is gebaseerd op een aantal modellen en theorieën, waaronder het *technology acceptance model*, de *theorie van beredeneerde actie*, de *theorie van gepland gedrag*, *innovation diffusion theory*, *model of PC Utilization*, *Motivation Theory* en de *sociaal-cognitieve theorie*. Volgens Venkatesh zijn er meer factoren die de gedragsintentie en het gebruik van informatietechnologie beïnvloeden. Deze factoren zijn ondergebracht in de *unified theory of acceptance and use of technology* en is hieronder schematisch weergegeven [VENK03]:



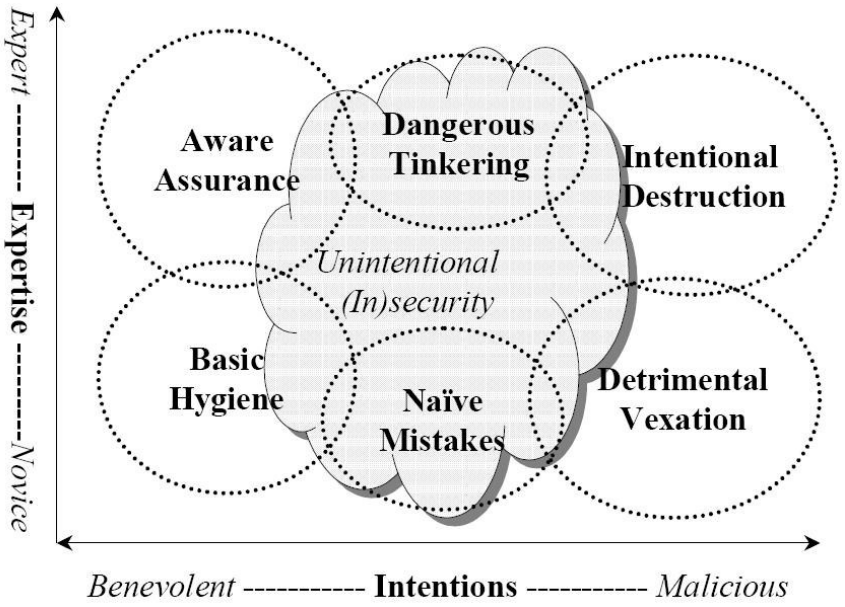
Figuur 10: Unified theory of acceptance and use of technology [VENK03]

Binnen het model wordt verondersteld dat er vier onafhankelijke variabelen zijn die de gedragsintentie en het gebruikersgedrag (use behavior) verklaren. De eerste is de *performance expectancy* wat vergelijkbaar is met de *perceived usefulness* uit het *technology acceptance model*. De tweede is de *effort expectancy* wat vergelijkbaar is met de *perceived ease of use* uit het *technology acceptance model*. De derde zijn de *facilitating conditions*: de overweging van een individu of er een organisatorische en technische infrastructuur aanwezig is om het gebruik te ondersteunen. Als laatste de *social influence*: de mate waarin een individu ervaart dat relevante anderen vinden dat hij of zij een technologie moet gebruiken. Daarnaast worden er nog een viertal aspecten geïdentificeerd die een significante invloed uitoefenen op de gedragsintentie en/of het werkelijke gebruik: geslacht, leeftijd, ervaring en vrijwilligheid van gebruik.

3.1.4 Behavioral information security

Gedrag in relatie tot informatiebeveiliging wordt in de literatuur voor het eerst concreet gemaakt door Stanton e.a. met de term *behavioral information security*. Deze term wordt als volgt gedefinieerd: *complexes of human action that influence the availability, confidentiality, and integrity of information systems.* [STAN03a]. Het eerste stuk van de definitie gaat in op alle handelingen die het menselijke gedrag kan vertonen. Het tweede stuk gaat in op de invloed die deze handelingen uitoefenen op de betrouwbaarheidseisen van informatiesystemen.

Het onderzoek van Stanton e.a. omvat 110 interviews met informatietechnologie specialisten, managers en normale medewerkers. De centrale vraag was om te beschrijven wat het voor- en nadelige gedrag was bij het gebruik van informatietechnologie, met als uitgangspunt dat het effect moest hebben op de informatiebeveiliging van de organisatie waar de eindgebruiker werkzaam was. Middels 70 van deze interviews zijn er 93 gedragingen (zie Bijlage 8.1 "Employee Security-Related Behavior List") geïnventariseerd [STAN06]. Op basis van brainstormsessies met 12 informatietechnologie specialisten zijn de 93 gedragingen verdeeld over 6 categorieën (zie Bijlage 8.2 "Two factor taxonomy of security behaviors") voor gedrag ten aanzien van informatiebeveiliging. Hierbij is er een onderscheid gemaakt tussen de dimensies expertise en intentie [STAN03a], [STAN05a].



Figuur 11: Six-Category Behavioral Taxonomy [STAN03a], [STAN05a]

De categorieën basic hygiene, aware assurance, naive mistakes, dangerous tinkering, detrimental misuse, intentional destruction zijn ingedeeld naar expertise en intentie. Daarnaast is er een wolk in het midden wat de unintentional (in)security beschrijft. Hieronder vallen alle handelingen van gedrag, waarvan de intentie niet direct kwaadwillend of goed is. Het is als het ware een grijs gebied. Hieronder zullen de verschillende categorieën kort besproken worden (een uitgebreidere beschrijving is te vinden in bijlage 8.2 "Two factor taxonomy of security behaviors"):

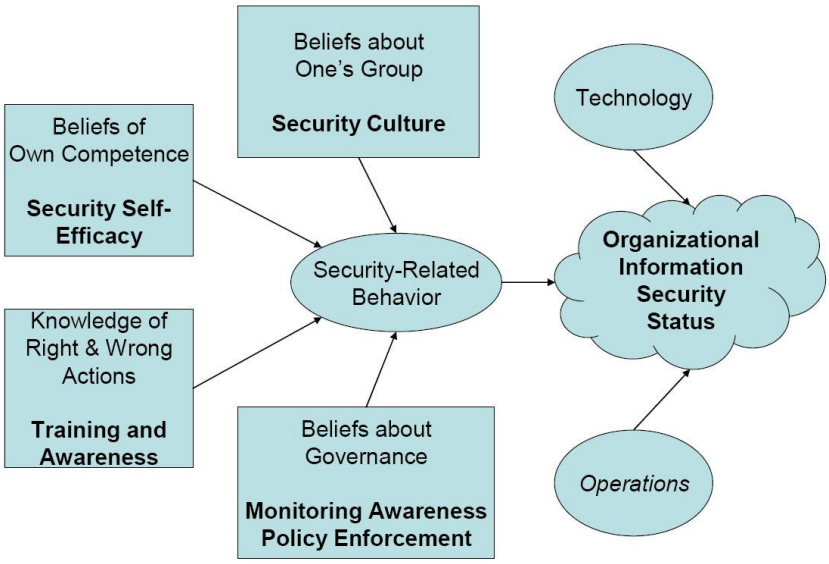
- Aware assurance: vereist veel technische deskundigheid samen met een sterke bedoeling om goed te doen en de informatiebeveiliging van een organisatie te beschermen.

- Basic hygiene: vereist geen technische deskundigheid maar omvat een duidelijke bedoeling om goed te doen en de informatiebeveiliging van een organisatie te beschermen.
- Naive mistakes: vereist minimale technische deskundigheid en heeft geen duidelijke kwaadwillende bedoeling tegenover de informatiebeveiliging van een organisatie.
- Dangerous tinkering: vereist veel technische deskundigheid maar heeft geen duidelijke kwaadwillende bedoeling tegenover de informatiebeveiliging van een organisatie.
- Detrimental misuse: vereist minimale technische deskundigheid maar omvat een duidelijke kwaadwillende bedoeling om de informatiebeveiliging van een organisatie in gevaar te brengen.
- Intentional destruction: vereist veel technische deskundigheid samen met een sterke kwaadwillende bedoeling om de informatiebeveiliging van een organisatie in gevaar te brengen.

De taxonomie met 6 categorieën is getoetst door 49 informaticastudenten via een 5-puntsschaal, waarbij de 93 gedragingen beoordeeld moesten worden op expertise, intentie en positie binnen de taxonomie. Bij alle 6 categorieën was voor zowel de expertise als de intentie een significante correlatie aangetoond. Vervolgens zijn er een tweetal vragenlijsten uitgezet, waarbij het doel was om zicht te krijgen in wat het gedrag ten aanzien van informatiebeveiliging van eindgebruikers is in relatie tot motivatie [STAN04]. Beide vragenlijsten zijn gelijktijdig gehouden en waren beide summier waarbij alleen wachtwoordmanagement centraal stond. Het onderzoek is uitgevoerd binnen 14 verschillende organisaties, waarbij de grootte van de organisaties verschilde van zes tot tweeduizend medewerkers.

Uit de eerste vragenlijst zijn een aantal resultaten gekomen die mogelijk van belang kunnen zijn voor vervolgonderzoek [STAN03c]. Ten eerste zouden de resultaten aantonen dat de organisatorische verplichting van medewerkers een belangrijke gedragsvoorspeller is voor informatiebeveiligingsgerelateerd gedrag. Daarnaast zou de werkhouding en de werkmotivatie ook zeer relevant zijn voor informatiebeveiligingsgerelateerd gedrag. Stanton e.a. stellen dan ook voor om bij vervolgonderzoek deze variabelen mee te nemen als voorspellingsvariabelen. Ten tweede zouden de resultaten aantonen dat er een tegeninitiatief bestaat ten opzichte van een aanvaardbaar gebruiksbeleid. Hierbij hadden medewerkers met een hoge mate van organisatorische verplichting, een lagere mate van naleving van een aanvaardbaar gebruiksbeleid.

In de tweede vragenlijst is er gekeken naar de *beliefs* die medewerkers hadden op basis van een raamwerk dat bestond uit: security culture, security self-efficacy, training and awareness, monitoring awareness, enforcement of acceptable use policy, om te voorspellen hoe succesvol de informatiebeveiliging van de organisatie zou zijn. Hieronder zijn de verschillende variabelen schematisch weergegeven [STAN05b]:



Figuur 12: Variabelen van de *beliefs* in relatie tot het gedrag ten aanzien van informatiebeveiliging [STAN05b]

Uit de tweede vragenlijst zijn de volgende resultaten gekomen die mogelijk van belang kunnen zijn voor vervolgonderzoek [STAN06]. Ten eerste was er een sterke relatie tussen de *beliefs* die medewerkers hebben in de mate van "training and awareness" binnen de organisatie en de mate van succes van de informatiebeveiliging. In het geval van een positieve "security culture" bleek dat als er overeenstemming was in de mate hoe een groep hierover dacht, dat er dan een sterke relatie bestond met de mate waarin de organisatie succesvol was met haar informatiebeveiliging. Ten tweede bleek dat medewerkers met een hoge mate van vertrouwen voor de informatiebeveiliging van de organisatie, er zelf een verenigbaar waardesysteem op na hielden. Hierbij kwamen de volgende redeneringen voor: medewerkers die veel voorlichting kregen van IT-professionals, voelden zich gemachtigd die informatie te gebruiken om een positieve "security culture" en informatiebeveiliging te krijgen. Medewerkers met een tegenovergestelde persoonlijke overtuiging dachten negatief over de mate van succes van de informatiebeveiliging binnen de organisatie. Een mogelijke oorzaak hiervoor zou kunnen zijn dat deze persoonlijke overtuiging zowel logisch als emotioneel aantrekkelijk is voor medewerkers. Daarnaast geven deze resultaten niet aan dat het geven van training of het verhogen van bewustzijn, een positievere uitkomst op de mate van succes van informatiebeveiliging zal opleveren. Zoals Stanton e.a. aangeven moeten de resultaten en conclusies uit de vragenlijsten met een korreltje zout worden genomen [STAN06].

3.1.4.1 Informatieverwerkingsniveau en het menselijk falen

In de psychologie heeft men het niet over bewust en onbewust gedrag, maar over gecontroleerd en automatische gedrag. Er is geen strikte scheiding tussen gecontroleerd (bewust, wakker, geconcentreerd, aandachtig, enzovoort) en automatische (onbewust, automatisch, slapend, in een roes, afgeleid, enzovoort) gedrag. Hardonk geeft aan dat er eerder sprake is van een geleidelijke overgang in de wijze van informatieverwerking, die loopt van het ene uiterste waarbij er volledig automatische informatieverwerking plaatsvindt tot het andere uiterste waarbij er totaal gecontroleerde informatieverwerking plaatsvindt [HARD94]. Geautomatiseerde cognitieve processen verlopen snel, spelen zich vrijwel onbewust af, gaan parallel, kosten weinig energie en maken nauwelijks aanspraak op het korte-termijngeheugen. In tegenstelling tot gecontroleerde processen die traag verlopen, veel

aandacht vergen, serieel verlopen, veel energie kosten en veel vergen van de capaciteit van een mens [KAHN73].

Rasmussen maakt onderscheid tussen drie niveaus van informatieverwerking. Dit zijn de niveaus: skill-based, rule-based en knowledge-based [RASM83]. Het skill-based gedrag wordt verwerkt door een serie van voorgeprogrammeerde acties. Voorbeelden hiervan zijn de manier waarop men in een auto rijdt en van de ene versnelling naar de andere schakelt en de eenvoud van het plaatsen van een persoonlijke handtekening. Dit zijn veelal goedgeleerde en simpele handelingen. De verwerking van skill-based gedrag wordt gedefinieerd door het routinematige karakter van de opdracht, automatische verbinding tussen signaal en reactie, het continue karakter van de opdracht en het ontbreken van feedback. Het rule-based gedrag wordt verwerkt door het gebruik van algemene regels, die toepasbaar zijn in een groot aantal verschillende situaties. Voorbeelden hiervan zijn het voorrang geven aan verkeer van rechts of het uitsteken van je hand als je afdraait. Dit zijn veelal goedgeleerde complexe gedragingen, waarbij de cognitieve stappen voor de hand liggen. De verwerking van rule-based gedrag vindt plaats als de opdracht uit relatief veel voorkomende actiesequenties bestaat die beginnen na de gecontroleerde keuze van een regel of procedure en de beschikbare informatie niet automatisch het gedrag bepaalt, maar gebruikt wordt bij het gecontroleerd kiezen van een regel. Als er bij het skill-based en rule-based niveau te veel of te weinig aandacht besteed wordt aan een handeling, dan kunnen er fouten op dit niveau ontstaan. Knowledge-based verwerking van gedrag wordt gebruikt in volstrekt nieuwe situaties waarvoor geen vaste regels gelden en via redeneren, creativiteit en analytisch inzicht problemen moeten worden opgelost. Een voorbeeld hiervan is het verzinnen van een nieuwe route wanneer een gedeelte van de snelweg is geblokkeerd. Hierbij gaat het om het echte denkwerk, zoals eerder gezegd via redeneren of creativiteit. Het knowledge-based gedrag wordt gekarakteriseerd door nieuwheid van de situatie, de noodzaak om abstracte kennis te gebruiken, het feit dat er een oplossing wordt gezocht om een bepaald doel te bereiken en het feit dat er een keuze wordt gemaakt tussen alternatieve plannen, die eventueel eerst in gedachten zijn getest met behulp van een intern model. Binnen skill-based, rule-based en knowledge-based informatieverwerking kan er sprake zijn van overgang in de wijze waarop één en dezelfde handeling wordt verwerkt. Een voorbeeld hiervan is het nemen van een strafschop door een voetballer op de training. Er is hier sprake van een skill-based informatieverwerking, maar als dezelfde voetballer een strafschop moet nemen op de wereldkampioenschappen kan er een verschuiving plaatsvinden van skill-based via rule-based naar knowledge-based informatieverwerking. Door deze verschuiving van automatische naar gecontroleerde handelingen kunnen er fouten ontstaan. De keuze voor het te gebruiken niveau is afhankelijk van ervaring en van verwerkingsvermogen. Mensen hebben daarbij de neiging te streven naar handelingsefficiëntie, waarbij het informatieverwerkingssysteem van de mens zo efficiënt en effectief mogelijk dient te werken. Veel fouten zijn terug te koppelen naar situaties waarin automatische verwerking zijn gang gaat, terwijl dat in de betreffende situatie niet correct is, dus waarin eigenlijk gecontroleerde informatie de zaak had moeten bijsturen.

Om terug te komen op het model van Overbeek e.a kan er nu gekeken worden vanuit de drie informatieverwerkingsniveaus van Rasmussen. Hierbij kunnen de automatismen van Overbeek e.a gezien worden als informatieverwerking op skill-based en rule-based niveau. Deze geautomatiseerde operaties geven invulling aan het onbewuste gedrag ten aanzien van informatiebeveiliging, welke volgens Overbeek e.a via automatismen tot stand komt. Motivatie vertoont overeenkomsten met knowledge-based informatieverwerking die invulling geeft aan bewust gedrag. Er is sprake van gecontroleerd gedrag die volgens Overbeek e.a via motivatie tot stand komt en het bewuste gedrag vormt. Vanuit de theorie van gepland gedrag zou motivatie opgevat kunnen worden als de gedragsintentie, maar het verschil hierbij is dat motivatie ingaat op de behoefte van mensen, terwijl dat bij gedragsintentie niet het geval hoeft te zijn. Behavioristen willen de termen "bewust" en "onbewust" helemaal uit de taal van de psychologie verbannen. Zover zal in dit onderzoek niet gegaan worden, maar het is wel belangrijk om exact aan te geven waar men over spreekt en wat men bedoelt. In dit onderzoek zal niet gesproken worden over bewust en onbewust gedrag ten aanzien

van informatiebeveiliging, maar over automatisch en gecontroleerd gedrag ten aanzien van informatiebeveiliging.

Niet elke vorm van gedrag ten aanzien van informatiebeveiliging is wenselijk; mensen maken automatisch of gecontroleerd en zelfs met opzet fouten [REAS90], [WAGE89]. Reason maakt onderscheid tussen drie soorten fouten. De eerste soort fout zijn blunders, die ontstaan wanneer een individu een routinematige of automatische handeling verricht. De tweede soort fout zijn afdwalingen, die ontstaan wanneer een handeling niet verricht wordt doordat een signaal uit de omgeving ontbreekt of als de handeling vergeten wordt. Bij zowel blunders als afdwalingen is het doel en de intentie van de handeling correct, maar ontstaat er toch een foute handeling. Als derde soort fout zijn er de vergissingen die kunnen ontstaan door een gebrek aan deskundigheid. Bij vergissingen is de oorsprong van het doel en de intentie bij het handelen al niet correct, waardoor er fouten ontstaan. Daarnaast zijn er nog overtredingen die zowel te goeder trouw, als met boze opzet kunnen plaatsvinden. Hierbij gaat het om handelingen waarbij willens en wetens de wet, de regels of de voorschriften genegeerd worden. Dit kunnen zowel incidentele als structurele overtredingen te goeder trouw zijn of overtredingen met een criminele achtergrond zoals hacking, fraude of sabotage.

Koppelen we hier het informatieverwerkingsniveau van Rasmussen aan dan vinden blunders en afdwaling plaats op een skill-based niveau. Vergissingen daarentegen vinden zowel plaats op rule-based als op knowledge-based niveau. De informatieverwerkingsniveaus van Rasmussen in relatie tot de drie typen fouten van Reason zien er als volgt uit.

Performance level	Primary error type
Skill-based level	Slips and Lapses
Rule-based level	Rule-based mistakes
Knowledge-based level	Knowledge-based mistakes

Figuur 13: De classificatie van typen fouten in relatie tot de informatieverwerkingniveaus [RASM86]

De cognitieve fases; planning, opslag en uitvoering kunnen hierbij ook nog gekoppeld worden aan de typen fouten [RASM83]. Planning verwijst naar het proces om doelen te identificeren en te beslissen hoe deze bereikt kunnen worden. Opslag gaat in op de verwerking van de verschillende intenties van handelen. De uitvoering gaat in op het proces waarbij de opgeslagen intentie van handelen wordt geïmplementeerd. De cognitieve fases van Rasmussen in relatie tot de drie typen fouten van Reason zien er als volgt uit.

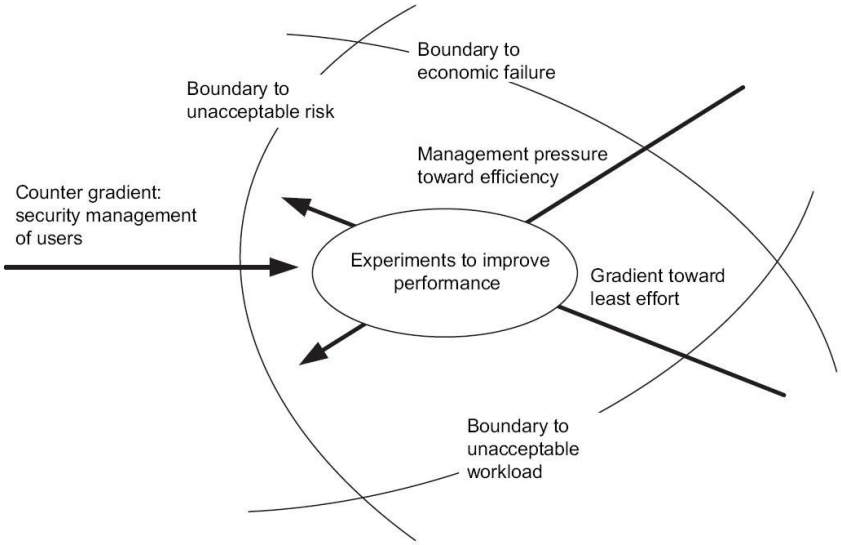
Cognitive Stage	Primary error type
Planning	Mistakes
Storage	Lapses
Execution	Slips

Figuur 14: De classificatie van typen fouten in relatie tot de cognitieve fases [REAS90]

Als er vervolgens nog de Behavioral Taxonomy van Stanton e.a. tegen aangelegd wordt, dan horen de blunders en afdwalingen tot het gedrag van de naive mistakes. Vergissingen op zowel rule-based als knowledge-based horen bij het gedrag van het dangerous tinkering. De detrimental misuse

en de intentional destruction behoren beiden tot de overtredingen. Als laatste behoren de aware assurance en de basic hygiene niet tot één van de drie soorten fouten, aangezien er hier geen sprake is van een fout.

Er wordt door Rasmussen een mogelijke verklaring gegeven voor de druk van economisch rendement, onaanvaardbare werkbelasting, informatiebeveiligingsbeheer en onaanvaardbare risico's, waardoor fouten kunnen worden gecreëerd [RASM97].



Figuur 15: Handelingen van gedrag vindt plaats binnen bepaalde grenzen [RASM97]

De grenzen van de druk van economisch rendement, onaanvaardbare werkbelasting en onaanvaardbare risico's beïnvloeden het gedrag van individuen. De eerste gaat in op de druk die door organisaties wordt uitgeoefend om een zo hoog mogelijk economisch rendement te behalen. De onaanvaardbare werkbelasting ontstaat doordat individuen constant de psychische en sociale omgeving toetsen en deze informatie gebruiken om een mentaal model van de werkomgeving en activiteiten te maken. Als laatste wordt het gedrag van individuen richting de grens van onaanvaardbare risico's geduwd door de krachten van de druk van economisch rendement en de onaanvaardbare werkbelasting. Fouten ontstaan meestal doordat geprobeerd wordt een balans te vinden voor de verschillende grenzen die niet in overeenstemming zijn met elkaar. De druk vanuit de verschillende grenzen kan zo groot worden dat het overtreden of het maken van fouten de beste optie is.

3.1.4.2 Informatiebeveiligingsbewustzijn

In de literatuur worden de automatische en gecontroleerde handelingen van informatiebeveiliging met een aantal andere zowel Nederlandse[25] als Engelse[26] begrippen aangeduid. Hierbij kan onderscheid gemaakt worden tussen beveiliging in de brede zin van het woord en beveiliging van de betrouwbaarheid van informatie. Eerst zal gekeken worden wat (informatie)beveiligingsbewustzijn precies inhoudt en wat het doel is. Vervolgens zal er gekeken worden hoe het gemeten wordt.

[25] Beveiligingsbewustzijn en informatiebeveiligingsbewustzijn

[26] Security awareness en information(technology) security awareness

Het Information Security Forum (ISF) definieert informatiebeveiligingsbewustzijn als volgt:

Information security awareness is the degree or extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organisation, their individual security responsibilities, and acts accordingly. [INFO93], [INFO02]

In deze definitie komt naar voren dat het gaat om de mate waarin medewerkers begrijpen wat het belang, het niveau en de verantwoordelijkheden zijn die hij heeft ten opzichte van informatiebeveiliging voor de organisatie en er ook naar handelt. Zowel Neys als Hofland hebben dezelfde definitie van het Information Security Forum geadopteerd:

Security awareness is de mate waarin elke medewerker de volgende punten begrijpt: het belang van informatiebeveiliging, het niveau van informatiebeveiliging dat voor de organisatie noodzakelijk is en er ook naar handelt. [HOFL05], [NEYS03]

Het enige verschil met de definitie van het Information Security Forum is dat het punt van de individuele verantwoordelijkheid is weggelaten. Omdat dit volgens Neys verwoord wordt binnen het informatiebeveiligingsbeleid, wat volgens haar het minimale vereiste niveau is voor een organisatie. Het National Institute of Standards and Technology (NIST) geeft voor awareness de volgende definitie:

Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance. [NIST98]

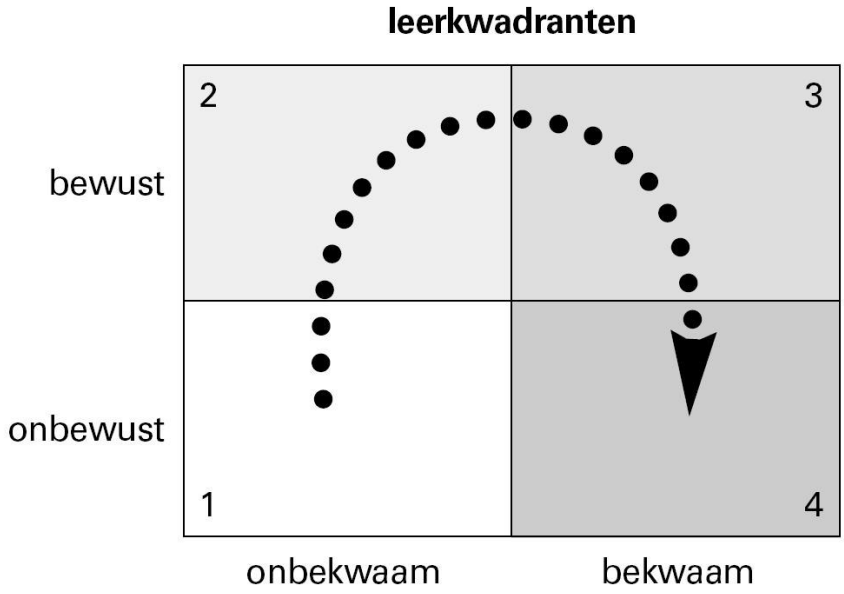
Zowel de definitie van de NIST als die van de ISF komen op belangrijke punten met elkaar overeen. Beide gaan in op het begrijpen van het belang en de verantwoordelijkheden ten opzichte van informatiebeveiliging. Daarnaast spreken beide over *acts* of *respond accordingly*, wat er op neerkomt dat een medewerker er ook naar handelt vanuit zijn gedrag. Wanneer een medewerker vanuit het gedrag handelt volgens de definitie van de NIST en het ISF ontstaat er een *human firewall*. Met de term "human firewall" wordt bedoeld dat de medewerker zelf meewerkt om een goede beveiliging te creëren. De medewerker neemt actief deel aan de beveiliging van de informatie die zij tot hun beschikking hebben [KOOT06].

Naast informatiebeveiligingsbewustzijn als term wordt er in de literatuur ook gesproken over campagnes voor bewustwording van informatiebeveiliging. Volgens Killmeyer zijn er doelstellingen en belangen die bereikt moeten worden bij informatiebeveiligingsbewustwordingscampagnes. Deze doelen houden in [KILL06]:

- Werknemers moeten hun verantwoordelijkheden kennen, om de informatieinfrastructuur van het bedrijf te beschermen.
- Werknemers moeten de waarde van informatiebeveiliging begrijpen.
- Werknemers moeten potentiële informatiebeveiligingsincidenten herkennen en wanneer deze optreden moeten ze de verantwoordelijken kunnen inlichten.
- Het niveau van security awareness moet onder de huidige werknemers hoog blijven, doordat zij er ook correct naar handelen.

Maar is een campagne voor bewustwording van informatiebeveiliging wel zinvol? In de literatuur zijn er zowel voor- als tegenspraken te vinden wat betreft deze vraag. De waarheid hierover zal in het midden gelaten worden om te kunnen kijken op welke wijze informatiebeveiligingsbewustzijn gemeten wordt.

Het eerste meetmodel is beschreven door Hofland wat geadopteerd is uit de literatuur[27] [HOFL05].

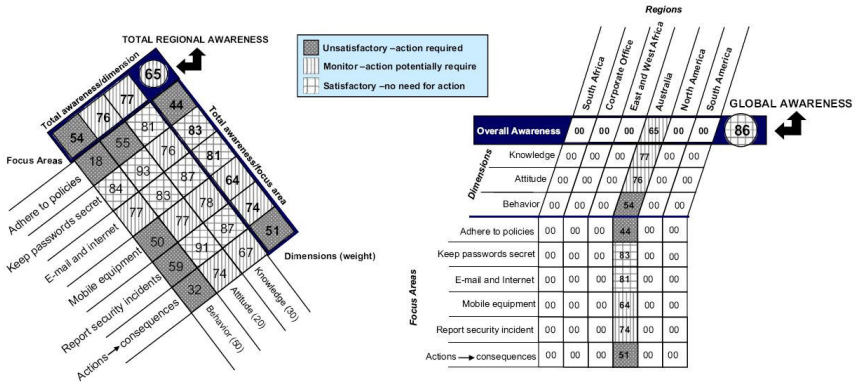


Figuur 16: Leerkwadranten [BOSC04], [MAGN04]

De leerkwadranten vertonen een groei waarbij informatiebeveiligingsbewustzijn van *onbewust/onbekwaam* verloopt via *bewust/onbekwaam* naar *bewust/bekwaam* en uiteindelijk naar *onbewust/bekwaam*. Helaas past dit model niet bij bewust en onbewust gedrag, als men spreekt over gecontroleerd en automatische gedrag. Ten eerste omdat er geen strikte scheiding is tussen gecontroleerd en automatische gedrag. En ten tweede omdat er sprake is van een geleidelijke overgang van de ene fase naar de andere, waarbij zowel van gecontroleerd naar automatische als wel van automatische naar gecontroleerd gekomen kan worden.

Kruger en Kearney beschrijven een prototype om het informatiebeveiligingsbewustzijn te meten [KRUG06]. Hierbij gaan ze uit van 35 vragen die ingaan op de aspecten *attitude*, *kennis* en *gedrag*, waarbij per aspect de dimensies *adhere to policies*, *keep passwords secret*, *e-mail and internet*, *mobile equipment*, *report security incidents*, *actions consequences* worden onderscheiden. De uitkomst van de meting van informatiebeveiligingsbewustzijn kan er als volgt uitzien:

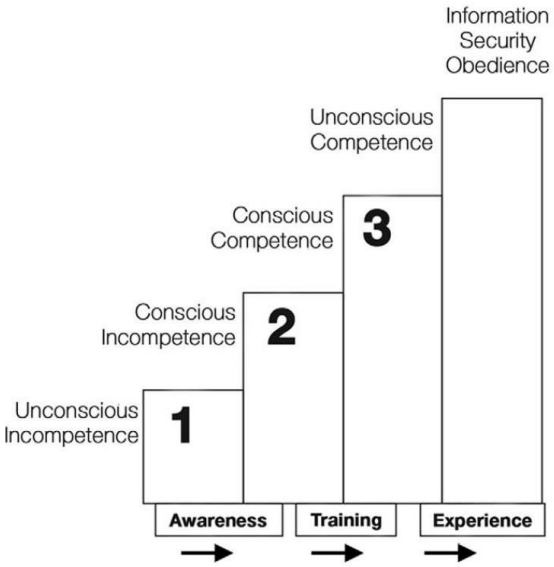
[27] Ten tijde van het onderzoek is het model, dat Vincent Hofland heeft ontwikkeld, verschillende malen teruggevonden in verschillende literaire stukken (zie [BOSC04] en [MAGN04]).



Figuur 17: Gemeten informatiebeveiligingsbewustzijn [KRUG06]

Het uitgangspunt van de aspecten *attitude*, *kennis* en *gedrag* is in overeenstemming met wat Jentjes en Basten stellen ten aanzien van het verkrijgen van het gewenste en werkende informatiebeveiligingsbewustzijnsniveau [BAST03], [JENT04]. Of het bewustzijn via attitude, kennis en gedrag gemeten kan worden is voor ons als auteurs niet zo aannemelijk. Het bewustzijn gaat in op de regulerende processen die zich afspelen op de drie niveaus van informatieverwerking. In hoeverre deze gemeten kunnen worden door de attitude, kennis en gedrag is voor ons als auteurs twijfelachtig.

Thomson en von Solms, beschrijven een informatiebeveiligingscompetentie volwassenheidsmodel, waarin een medewerker van ongetraind en onzeker groeit tot een medewerker met volledig begrip van informatiebeveiliging en veel ervaring [THOM06].

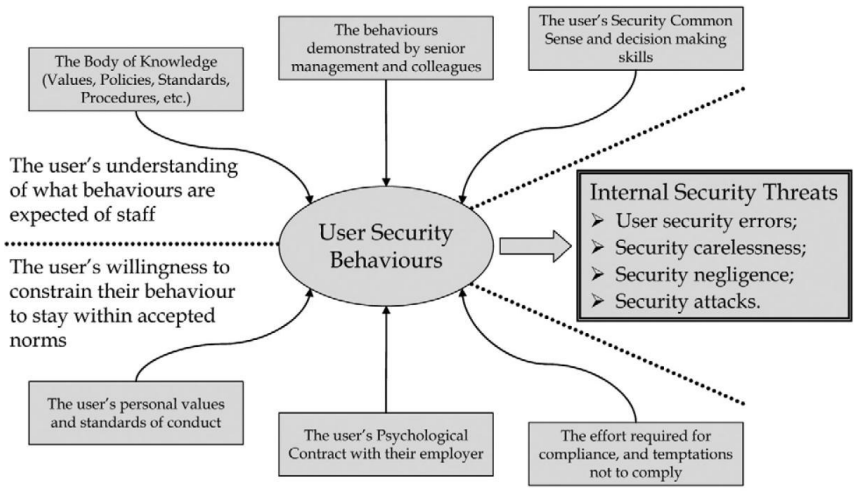


Figuur 18: Volwassenheidsmodel [THOM06]

Een medewerker start in stage 1, waarbij hij volledig onbewust en onervaren is met informatiebeveiliging. In stage 2 heeft de medewerker campagnes voor bewustwording van informatiebeveiliging doorlopen. In stage 3 doorloopt de medewerker een trainingsprogramma voor informatiebeveiliging. Een medewerker komt pas in stage 4, wanneer hij genoeg ervaring heeft opgedaan en informatiebeveiliging een soort van tweede natuur is geworden. De volwassenheid loopt dus van bewustwordingscampagnes via trainingsprogramma's naar ervaring, waarbij een medewerker

in het hoogste niveau is gekomen. Het bewustzijn wat hier wordt beschreven gaat in op de ontwikkeling van de regulerende processen. Naarmate een individu zich verder ontwikkelt zal het arbeidsgedrag van het knowledge-based- naar het rule-based- en uiteindelijk naar het skill-based niveau gaan. Maar in hoeverre de volwassenheid van een individu iets zegt over het te vertonen gedrag is onduidelijk en of hier dan nog steeds een onderscheid bestaat tussen bewust en onbewust gedrag is ook onduidelijk.

Als laatste geeft Leach een model waarin zes factoren staan die mogelijk een sterke invloed hebben op het gedrag ten aanzien van informatiebeveiliging [LEAC03]. Hierbij worden de sleutelfactoren genoemd waarmee een organisatie stappen kan ondernemen om het gedrag van haar medewerker ten aanzien van informatiebeveiliging te verbeteren, waarmee de interne bedreigingen en incidenten moeten afnemen. Hieronder staat het model; het gedrag van informatiebeveiliging wordt hierbij omringd door de factoren die invloed hebben op dit gedrag. De grijze pijl geeft aan wat het effect van gedrag is voor de informatiebeveiliging.



Figuur 19: Gedragsinvloed [LEAC03]

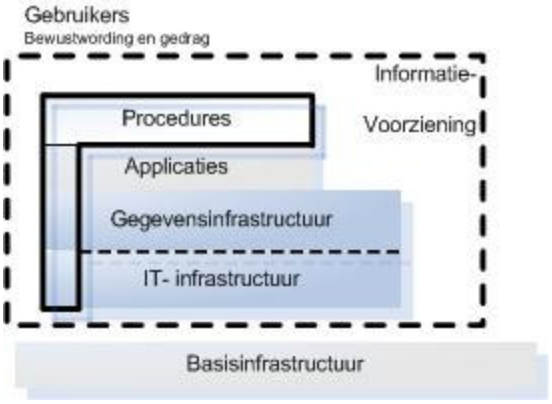
Of dit daadwerkelijk de factoren zijn die invloed hebben op het gedrag van informatiebeveiliging en dan gekeken naar de mate waarin deze factoren invloed hebben is nog sterk de vraag. Er zijn geen onderzoeken die de resultaten en conclusies van Leach bevestigen. Dus wat de wetenschappelijke meerwaarde van dit model is anders dan zoekend en richtinggevend moet in het midden gelaten worden.

3.2 Informatiebeveiliging

3.2.1 Gegevens, informatie en informatievoorziening

Gegevens en informatie zijn uitgegroeid tot de smeerolie die processen binnen organisaties sneller en beter laten verlopen. Voor veel organisaties is het verwerken van informatie zelfs het belangrijkste proces. Informatie wordt steeds vaker gezien als vierde productiefactor naast arbeid, natuur en kapitaal [OVER05]. Hierbij valt te denken aan persoonsgegevens, klantgegevens of financiële gegevens. Tussen de begrippen gegevens en informatie zit een belangrijk verschil. Gegevens kunnen gezien worden als de objectief waarneembare weerslag van feiten in een

gegevensdrager (harde schijf bijvoorbeeld). Informatie is de betekenis die mensen aan de hand van bepaalde afspraken aan gegevens toekennen, of de kennistoename als gevolg van het ontvangen en verwerken van bepaalde gegevens [OVER05]. Een voorbeeld hiervan is een telefoonboek dat gevuld is met gegevens, het wordt pas informatie als een persoon daadwerkelijk een telefoonnummer zoekt. De relatie tussen gegevens en informatie is vergelijkbaar met de relatie tussen een grondstof en een eindproduct. Gegevens kunnen verwerkt worden tot informatiesystemen[28], hierbij kunnen gegevens die in een voor de ontvanger niet te gebruiken vorm staan, verwerkt worden tot gegevens die bruikbaar zijn en voor de ontvanger de betekenis van informatie hebben [OVER05]. Wylder beschrijft drie eigenschappen van informatie die bedreigingen en kwetsbaarheden ervan kunnen verklaren [WYLD04]. De eerste eigenschap is *portability*; deze geeft aan dat informatie in de meeste bestandsformaten gemakkelijk te verplaatsen is. De tweede eigenschap is *usability*; deze geeft aan dat de waarden van informatie afhankelijk zijn van de bruikbaarheid voor andere mensen. Als laatste eigenschap wordt *shelf life* genoemd; deze geeft aan dat de waarden die informatie heeft voor mensen over de tijd genomen neigt minder te worden. Gegevens zijn ondergebracht in de informatievoorziening (zie figuur 20) en is het geheel van IT-infrastructuur (het geheel van automatiseringsmiddelen), gegevensinfrastructuur (het geheel van één of meer gegevensverzamelingen), applicaties (programmatuur) en organisatie, dat tot doel heeft om te voorzien in de informatiebehoefte van de processen van een organisatie. Informatievoorziening is het geheel van activiteiten dat voor een bedrijf moet worden uitgevoerd om iedereen de informatie te verstrekken die nodig is om toegewezen functies te vervullen [LOOI04]. De basisinfrastructuur (gebouwen, elektriciteitsvoorziening) en gebruikersprocedures maken geen deel uit van de informatievoorziening maar zijn wel noodzakelijk voor het functioneren van de informatievoorziening [OVER05].



Figuur 20: De componenten voor informatievoorziening [OVER05]

3.2.2 Bedreigingen, kwetsbaarheid en risico's

3.2.2.1 Bedreigingen

De informatievoorziening van een organisatie staat voortdurend bloot aan verschillende bedreigingen. Bedreigingen zijn in vier categorieën te onderscheiden: bedreigingen van natuurlijke

[28] Looijen beschrijft geautomatiseerde informatiesystemen als een geheel van apparatuur met bijbehorende basisprogrammatuur en toepassingsprogrammatuur, gegevensverzamelingen, procedures en personen voor het kennen en/of het besturen/onderhouden van reële systemen ofwel bedrijfsprocessen. [LOOI04]

aard (bliksem), opzettelijke aard (diefstal), niet opzettelijke aard (brand) en technische aard (storing in apparatuur) [LOOI04]. Een bedreiging is een proces of een gebeurtenis die in potentie een verstorende invloed heeft op de betrouwbaarheid van objecten in de informatievoorziening. Praat onderscheidt vier kwaliteitsaspecten: effectiviteit, efficiency, betrouwbaarheid, continuïteit [PRAA02]. Bedreigingen worden onderverdeeld naar de aspecten van betrouwbaarheid die ze negatief beïnvloeden [OVER05]. Betrouwbaarheid bestaat uit de aspecten beschikbaarheid, integriteit en vertrouwelijkheid. Deze worden in het onderzoek als volgt omschreven [CVIB02], [NEN7510]:

- Beschikbaarheid (B): het zekerstellen dat gegevens en informatiediensten op de gewenste momenten beschikbaar zijn voor gebruikers.
- Integriteit (I): het waarborgen dat gegevens niet ongecontroleerd worden gewijzigd of verloren gaan.
- Vertrouwelijkheid (V): het beschermen van gegevens tegen onbevoegde kennisname.

Deze begrippen worden ook wel aangeduid met continuïteit, betrouwbaarheid en exclusiviteit. Het zijn in feite paraplubegrippen die de mens in staat stellen globaal iets te zeggen over: schadecategorieën, onderzoeksobjecten of confrontatieprocessen [NGI92].

Naast de bovengenoemde elementaire aspecten van betrouwbaarheid, zijn er ook nog de volgende zekerheidsbegrippen voor informatiebeveiliging [CVIB02], [NEN7510]:

- Onweerlegbaarheid: het waarborgen dat het vastleggen van gegevens of het verzonden bericht niet kan worden ontkend.
- Verantwoordelijkheid: het waarborgen dat van gegevens en verwerkingen van gegevens vaststaat wie daarvoor welke verantwoordelijkheid draagt.
- Authenticiteit: het zekerstellen dat gegevens, informatiediensten, organisaties en gebruikers van de juiste identiteit zijn voorzien.
- Betrouwbaarheid: het waarborgen van overige kwaliteitseisen ten aanzien van informatie, de bron ervan, de route die de gegevens volgen en verwerkingen die erop plaatsvinden.

Bedreigingen kunnen nog verder worden onderverdeeld op basis van de kenmerken die ieder aspect van betrouwbaarheid heeft (zie figuur 21: *Aspecten en kenmerken van betrouwbaarheid*).

Aspect	Kenmerk	Bedreiging	Voorbeeld
Beschikbaarheid	Tijdigheid	Vertraging	Overbelasting infrastructuur
	Continuïteit	Uitval	Distributed Denial of Service
Integriteit	Correctheid	Wijziging	Onrechtmatig wijzigen
	Volledigheid	Verwijdering/Toevoeging	Onrechtmatig verwijdering/Toevoeging
	Geldigheid	Veroudering	Gegevens niet up-to-date houden
	Authenticiteit	Vervalsing	Frauduleuze transactie
	Onweerlegbaarheid	Verloochening	Ontkennen berichten te hebben verstuurd
Vertrouwelijkheid	Exclusiviteit	Onthulling/Misbruik	Afluisteren van netwerk, Hacking

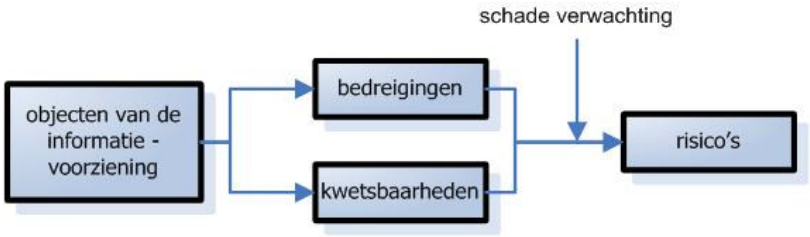
Figuur 21: Aspecten en kenmerken van betrouwbaarheid [OVER05]

3.2.2.2 Kwetsbaarheid

Naast bedreigingen is er ook nog de kwetsbaarheid van de informatievoorziening. Dit is de mate waarin de informatievoorziening gevoelig is voor bedreigingen. Deze gevoeligheid [29] ontstaat doordat één of meer objecten (gegevensinfrastructuur, applicaties) van de informatievoorziening het mogelijk maken dat één of meer bedreigingen (diefstal, virus of hacking) leiden tot een negatieve invloed op één van de betrouwbaarheidsaspecten (Beschikbaarheid, Integriteit en Vertrouwelijkheid) [OVER05], [PRAA02]. Gevoeligheid is hier de mate waarin gereageerd wordt op een binnenkomend signaal of een bepaald fysisch verschijnsel [NGI92].

3.2.2.3 Risico's

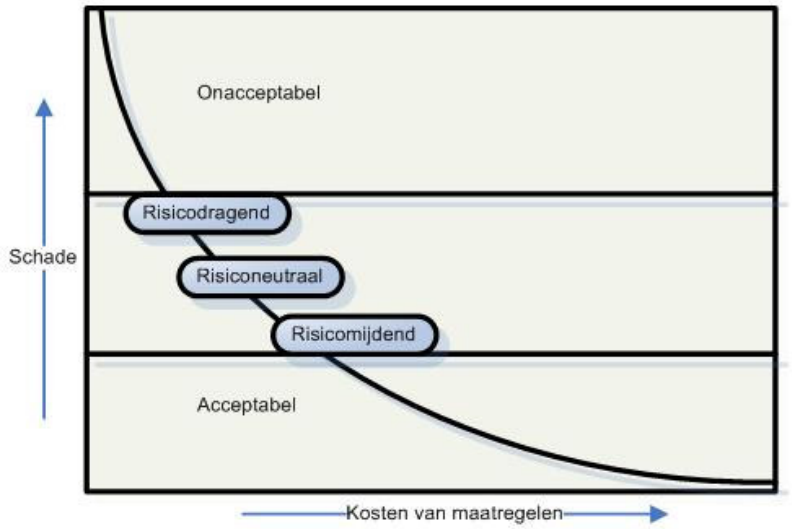
Als laatste zijn er nog risico's. Een risico is de gemiddelde schade over een gegeven tijdsperiode, die verwacht wordt doordat één of meer bedreigingen leiden tot een mogelijke (ver)storing van één of meer objecten van de informatievoorziening en wel zodanig dat dit leidt tot (ver)storing in de beschikbaarheid, integriteit en/of vertrouwelijkheid van de gegevensverwerking en informatievoorziening. Dit betekent dat er sprake is van een risico als één of meer objecten van de informatievoorziening door één of meer bedreigingen getroffen kunnen worden. Een risico is te beschouwen als "de kans op schade x schade", ofwel de schadeverwachting over een gegeven tijdsperiode. Hierbij bestaat "de kans op schade" uit een bedreiging x kwetsbaarheid. De formule voor risico is dan als volgt: Risico = (bedreiging x kwetsbaarheid) x schade. De schade kan al dan niet van financiële aard zijn en omvat directe schade (apparatuur of programmatuur) en indirecte schade (verlies van opdrachten of imagoschade). Een risico heeft altijd betrekking op één of meer objecten van de informatievoorziening, en op één of meer bedreigingen waarvoor de desbetreffende objecten een zekere kwetsbaarheid hebben [ISMH04], [LOOI04], [OVER05], [PRAA02]. De relatie tussen objecten binnen de informatievoorziening en risico's is in figuur 22 schematisch weergegeven.



Figuur 22: Relatie tussen de informatievoorziening en risico's

Een organisatie kan op verschillende manieren omgaan met de risico's die kunnen leiden tot ernstige, maar niet fatale, verstoringen van de bedrijfsprocessen. Men kan er voor kiezen om zo min mogelijk risico te lopen door veel in beveiliging te investeren wat redelijkerwijs acceptabel is. Beveiliging duidt hier op de mate waarin informatiesystemen zijn beschermd tegen al dan niet opzettelijke toegang, wijzigingen of vernietigingen [LOOI04]. Deze Beveiliging zorgt voor de implementatie van maatregelen in een organisatie, ten behoeve van de bescherming van deze organisatie tegen verstoringen, die schade op kunnen leveren voor (een deel van) de organisatie [OVER05].

[29] Gevoeligheid: de mate waarin gereageerd wordt op een binnenkomend signaal of een bepaald fysisch verschijnsel. [NGI92]



Figuur 23: Risicodragend, risiconeutraal en risicomijdend [OVER05]

Het stelsel maatregelen is erop gebaseerd een zo gering mogelijk risico ongeregeld te laten. Men werkt dan risicomijdend. Als men er voor kiest om de kosten voor beveiliging min of meer in evenwicht te houden met de kosten die gemoeid zijn met schade, dan werkt men risiconeutraal. Als men er voor kiest om meer risico te accepteren dan men afdekt, dat werkt men risicodragend. Het geheel is in figuur 23 verduidelijkt [NGI92], [OVER05], [PRAA02]. Voor de beheersing van risico's zijn de volgende algemene strategieën onderkend [STAR02]: risico-eliminatie, risicobeperking middels overdracht of vermindering en risicobehoud. Hierbij gaat risico-eliminatie in op het treffen van maatregelen tegen het risico waardoor deze wordt weggenomen. Risicobeperking door overdracht gaat in op het risico te laten dragen via een andere partij die daarmee dus het risico overneemt. Risicobeperking door vermindering gaat in op het treffen van maatregelen die het risico zoveel mogelijk reduceert. Als laatste gaat het risicobehoud in op de situatie die zich voor kan doen als eliminatie, overdracht of vermindering niet mogelijk is. Dan zal het risico behouden blijven.

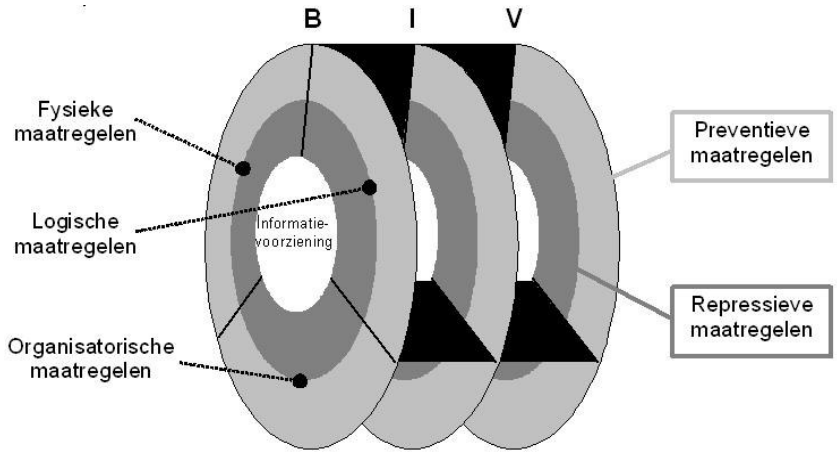
3.2.2.4 Beveiligingsmaatregelen

Beveiligingsmaatregelen kunnen worden ingedeeld middels de wijze waarop ze gerealiseerd worden (zie figuur 24): Organisatorische-, logische-, en fysieke maatregelen die als volgt omschreven kunnen worden [OVER05]:

- Organisatorische maatregelen hebben betrekking op de organisatie als geheel. Voorbeelden hiervan zijn: functiescheiding, interne controle of een portier bij de hoofdingang.
- Logische maatregelen zijn geprogrammeerd en verwerkt in programmatuur. Voorbeelden hiervan zijn: login/wachtwoordenauthenticiteit in besturingssysteem, encryptieprogrammatuur of een digitale handtekening in elektronische post.
- Fysieke maatregelen zijn gebaseerd op apparatuur of andere materiële zaken zoals: noodstroomvoorziening, brandblussers of sloten.

Informatiebeveiliging richt zich zoals eerder beschreven is op de betrouwbaarheidsaspecten beschikbaarheid, integriteit en vertrouwelijkheid. Iedere beveiligingsmaatregel richt zich op één of meerdere van deze aspecten. Daarnaast zijn er voor de verschillende beveiligingsaspecten specifieke

beveiligingsmaatregelen. In het onderstaande figuur zijn de beveiligingsmaatregelen ingedeeld middels de wijze waarop ze gerealiseerd worden binnen de betrouwbaarheidsaspecten [OVER05].



Figuur 24: Beveiligingsmaatregelen ingedeeld middels de wijze waarop ze gerealiseerd worden [OVER05]

3.2.2.5 Wat is informatiebeveiliging

Het woord "informatiebeveiliging" heeft meer dan één definitie. De Code voor Informatiebeveiliging definieert het als volgt:

Informatie is een bedrijfsmiddel dat, net als andere belangrijke bedrijfsmiddelen, waarde heeft voor een organisatie en voortdurend op een passende manier beveiligd dient te zijn. Informatiebeveiliging beschermt informatie tegen een breed scala aan bedreigingen, om de continuïteit van de bedrijfsvoering te waarborgen, de schade voor de organisatie te minimaliseren en het rendement op investeringen en de kansen van de organisatie te optimaliseren. Informatie komt in veel vormen voor. Het kan afgedrukt of beschreven zijn op papier, elektronisch opgeslagen zijn, per post of via elektronische media worden verzonden, getoond worden in films of de gesproken vorm aannemen. Welke vorm informatie ook heeft, of op welke manier ze ook wordt gedeeld of verzonden, ze dient altijd passend beveiligd te zijn. [CVIB02]

De Nederlandse norm voor informatiebeveiliging in de zorg geeft de volgende definitie:

Informatiebeveiliging is een stelsel van maatregelen om verstoringen in de zorgvuldige en doelmatige informatievoorziening te voorkomen en eventuele schade als gevolg van desondanks optredende verstoringen te beperken. [NEN7510]

Een studie door het Telematica Research Centrum over informatiebeveiliging in Nederland geeft de volgende definitie:

Het geheel van maatregelen en procedures dat ervoor zorgt dat er (zo adequaat mogelijk) wordt voldaan aan de eisen van vertrouwelijkheid, authenticiteit, integriteit en beschikbaarheid. [TETT95]

Overbeek e.a. geven de volgende definitie:

Informatiebeveiliging is het treffen en onderhouden van een samenhangend pakket maatregelen om de betrouwbaarheid[30] (beschikbaarheid, integriteit en vertrouwelijkheid) van de informatievoorziening te waarborgen. [OVER05]

Stanton e.a. definiëren het als volgt:

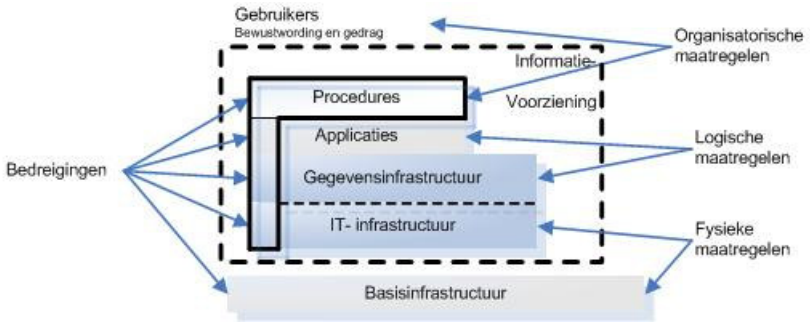
Information security is the range of technical and social approaches to keeping information confidential, integral, and available. [STAN06]

De Code voor Informatiebeveiliging stelt voorop dat informatie altijd passend beveiligd dient te zijn. De Nederlandse norm voor informatiebeveiliging noemt het een stelsel van maatregelen die er zorgvuldig en doelmatig voor zorgen dat er geen verstoring of schade optreedt aan de informatievoorziening. Het Telematica Research Centrum geeft aan dat het een geheel van maatregelen en procedures betreft die er voor zorgen dat er aan de eisen van vertrouwelijkheid, authenticiteit, integriteit en beschikbaarheid wordt voldaan. In de beschrijving van Overbeek e.a. komt duidelijk naar voren dat het gaat om het treffen en onderhouden van een samenhangend pakket van maatregelen, die de betrouwbaarheid (beschikbaarheid, integriteit en vertrouwelijkheid) van de informatievoorziening moet waarborgen. Stanton e.a. benadrukken dat het gaat om een reeks technische en sociale benaderingen om er voor te zorgen dat informatie vertrouwelijk, integer en beschikbaar blijft. In dit onderzoek zal de volgende definitie gebruikt worden voor informatiebeveiliging:

Informatiebeveiliging is een samenhangend geheel van technische en sociale benaderingen die er voor zorgen dat de informatievoorziening altijd beschikbaar, integer en vertrouwelijk blijft.

Informatiebeveiliging is een multidisciplinaire aangelegenheid van zowel technische, organisatorische en juridische aspecten. Maar veelal wordt informatiebeveiliging als iets technische benaderd. Overbeek e.a. geven aan dat het juist de organisatorische aspecten zijn die het succes van informatiebeveiliging bepalen in de praktijk. Daarnaast geven ze aan dat organisatorische maatregelen betrekking hebben op de organisatie als geheel, waaronder het beveiligingsbeleid, de richtlijnen en de procedures vallen. Deze maatregelen zijn volgens Overbeek e.a. toepasbaar op menselijke en organisatorische zaken, zoals: het beveiligingsbewustzijn van gebruikers, het gebruikersgedrag en de procedures [OVER05]. Hieruit blijkt dat de organisatorische maatregelen gekoppeld zijn aan de bewustwording en het gedrag van gebruikers. Daarnaast is er door Overbeek e.a. een splitsing aangebracht tussen het bewustzijn en het gedrag van gebruikers, maar waarom dit wordt gedaan is niet duidelijk. Binnen dit onderzoek staan deze twee termen centraal in relatie tot informatiebeveiliging en zijn onafhankelijk van elkaar behandeld in paragraaf "Behavioral information security". In de de paragraaf over "beveiligingsmaatregelen" is een indeling gegeven naar de wijze waarop beveiligingsmaatregelen gerealiseerd worden (organisatorische, logische en fysieke maatregelen). Beveiligingsmaatregelen verschillen niet alleen hierin, maar ook in de type objecten waarop ze werkzaam zijn (zie figuur 25).

[30] De betrouwbaarheid van de informatievoorziening geeft de mate aan waarin een organisatie zich kan verlaten op die informatievoorziening. De informatievoorziening omvat apparatuur, programmatuur, opgeslagen gegevens, procedures en mensen. [OVER05]

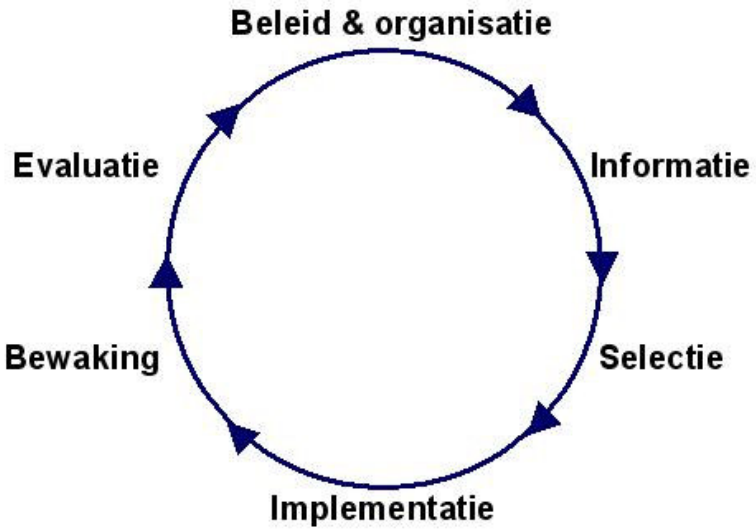


Figuur 25: Beveiligingsmaatregelen en hun werkingsgebied [OVER05], bewerkte versie van *figuur 20*.

Voorop staat dat organisatorische maatregelen wel geheel op zichzelf werkzaam zijn. Logische en fysieke maatregelen daarentegen hebben altijd aanvulling nodig van één of meer organisatorische maatregelen. Hierdoor zijn logische en fysieke maatregelen alleen effectief als de bijbehorende organisatorische maatregelen voldoende zijn ingevuld. Het goed organiseren van beveiligingsmaatregelen is nog geen garantie voor een goede beveiliging. Het vereist ook dat alle betrokken personen goed gemotiveerd zijn en hun verantwoording nemen. Bovendien zijn de baten van een goede informatiebeveiliging onzichtbaar, omdat er dan immers geen beveiligingsproblemen zijn [OVER05].

3.2.2.6 Het informatiebeveiligingsproces

Informatiebeveiliging krijgt gestalte door een samenhangend pakket van beveiligingsmaatregelen te treffen en te onderhouden. Omdat organisaties en hun omgeving constant veranderen, zullen zowel de risico's veranderen, als de eisen en randvoorwaarden die vanuit de organisatie aan informatiebeveiliging gesteld worden. Om te kunnen waarborgen dat er een adequaat niveau van informatiebeveiliging gehandhaafd blijft, dient hieraan constant aandacht besteed te worden. Informatiebeveiliging kan volgens Overbeek e.a. beschouwd worden als een iteratief proces [OVER05]. In dit proces worden zes stappen genoemd (zie figuur 26). In de stap *beleid en organisatie* worden de eisen en randvoorwaarden die gesteld worden aan de informatievoorziening geformuleerd en gedocumenteerd ten aanzien van informatiebeveiliging. Bij de stap *informatie* worden de relevante risico's inzichtelijk gemaakt doormiddel van een risicoanalyse. Nadat er inzicht is verkregen in de risico's kunnen er tijdens de *selectie* beveiligingsmaatregelen geselecteerd worden waarmee de risico's worden ingeperkt. De stap *implementatie* zorgt er voor dat door het management verantwoordelijk gestelde personen, er voor zorgen dat de voor de geselecteerde beveiligingsmaatregelen benodigde apparatuur, programmatuur en faciliteiten beschikbaar komen. Daarnaast moeten de noodzakelijke procedures gerealiseerd worden. Vervolgens kunnen de beveiligingsmaatregelen worden geïmplementeerd. Vervolgens is voortdurende bewaking van de informatiebeveiliging noodzakelijk. Daarnaast evalueert het management in hoeverre de geselecteerde beveiligingsmaatregelen op een juiste wijze geïmplementeerd zijn, en of de werknemers de daarbij behorende werkwijze volgen. Bovendien wordt geëvalueerd of de relevante risico's wel in voldoende mate en op een kosteneffectieve wijze zijn gereduceerd.



Figuur 26: Informatiebeveiliging als iteratief proces [OVER05]

4. METHODE[31]

In dit hoofdstuk zal de methode van het onderzoek behandeld worden. De methode is opgesplitst in twee delen: het vooronderzoek en het hoofdonderzoek. Binnen deze twee delen zal worden ingegaan op de dataverzameling en de dataverwerking.

4.1 Empirische ondersteuning van de TpB

In het "theoretisch kader" is al uitgebreid de theorie van gepland gedrag in kaart gebracht. In dit hoofdstuk vormt de theorie van gepland gedrag de basis voor het onderzoek. Hier zijn verschillende redenen voor. De theorie wordt gesteund door veel empirisch bewijs. Met betrekking tot het voorspellen van gedrag, hebben 222 medische studies gepubliceerd in de Medline database[32] en 610 psychologische studies gepubliceerd in de PsycINFO database[33] de voorspellende geldigheid van gedragsintenties onderzocht [FRAN04]. Sheeran heeft tijdens reviews van verschillende meta-analyses in verschillende gedragsdomeinen een correlatie van .53 gevonden tussen de gedragsintentie en het werkelijk uitgevoerde gedrag [SHEE02]. Verder is tijdens deze reviews gebleken dat de toevoeging van perceived behavioral control de voorspellende waarde van gedrag aanzienlijk kan verhogen, vooral wanneer het uit te voeren gedrag moeilijk is [MADD92].

Er zijn meta-analyses in de empirische literatuur die bewezen hebben dat de theorie voor uiteenlopende soorten gedrag, de gedragsintentie kan voorspellen middels de attitude toward the behavior, de subjective norm en de perceived behavioral control [ALBA01], [ARMI01], [HAGG02], [SHEE99]. Deze theorie geldt dus ook voor gedrag ten aanzien van informatiebeveiliging. Voor uiteenlopende soorten gedrag zijn attitudes gevonden die correleren met gedragsintenties; in de verschillende meta-analyses zijn correlaties tussen de .45 en .60 gevonden. Voor het voorspellen van de gedragsintentie vanuit de subjective norm lagen de correlaties tussen de .34 en .42 en voor het voorspellen van de gedragsintentie vanuit de perceived behavior control lagen de correlaties tussen de .35 en .46. De meervoudige correlaties voor het voorspellen van de gedragsintentie lagen tussen de .63 en .71.

Daarnaast heeft de meta-analyse van Armitage en Connor bewijs opgeleverd voor de bewering dat attitudes, subjective norms en perceptions of control voorspeld kunnen worden door overeenkomstige sets van beliefs. De correlatie tussen de expectancy-value index van behavioral beliefs en de directe meting van attitude toward the behavior was .50. Dezelfde correlatie werd gevonden tussen the normative belief index en subjective norm. De control belief index had een correlatie van .52 met perceived behavioral control [ARMI01].

De theorie van beredeneerd gedrag van Fishbein en Ajzen werd alleen geldig verondersteld onder bepaalde voorwaarden. Sheppard e.a. geven deze als volgt weer [SHEP88]. Ten eerste moet er sprake zijn van werkelijk "gedrag" en niet van gedragsuitkomsten als resultaat. Het afhankelijke gedrag dat men meet, moet betrekking hebben op het feitelijk gedrag en niet op het resultaat dat nagestreefd wordt met dit gedrag. Bijvoorbeeld "afvallen" of "aan de lijn doen" is een vorm van gedrag, waarbij het afgenomen gewicht of het aantal verloren kilo's het resultaat is. Een tweede voorwaarde houdt in, dat het gedrag binnen dit attitude-gedragsmodel moet gaan over het wel of niet, of over het meer of minder vertonen van bepaald gedrag, en niet om keuzes tussen

[31] Geschreven door Kevin Wessels

[32] http://medline.cos.com/

[33] http://www.apa.org/psycinfo/

verschillende gedragsalternatieven. Een derde uitgangspunt bij het gebruik van de theorie van beredeneerd gedrag is dat de gedragsintentie uit een werkelijk voornemen moet bestaan, en niet uit een verwachting. Bij de eerste wordt een intentie gemeten aan de hand van de vraag "Do you intend to do X?", terwijl bij een zogenaamde "estimation" gevraagd wordt: "Are you likely to do X?" of "Will you do X?". In de volgende alinea zal hier nog op teruggekomen worden.

Een andere belangrijke meta-analyse van Sheppard e.a. gaat in op gedragsalternatieven [SHEP88]. Deze meta-analyse is uitgevoerd op de theorie van beredeneerd gedrag, maar heeft ook betrekking op de theorie van gepland gedrag. Gedrag dat wordt geoperationaliseerd aan de hand van verschillende gedragsalternatieven leidt tot sterkere correlaties tussen attitude toward the behavior en subjective norm enerzijds en de gedragsintentie als voornemen anderzijds, dan wanneer er slechts van één gedragsalternatief sprake is. Bij de verwachting van het gedrag (in tegenstelling tot gedragsintentie als voornemen) was het verschil tussen één of meerdere gedragsalternatieven als afhankelijke variabele minder groot. Ook het verband tussen gedragsintentie als voornemen en gedrag blijkt sterker te zijn in het geval men meerdere gedragsalternatieven heeft, dan wanneer er sprake is van slechts één gedragsvorm. De voorspellende waarde van de theorie van beredeneerd gedrag lijkt dus groter te zijn wanneer er sprake is van een keuze uit verschillende gedragsalternatieven, terwijl Fishbein en Ajzen juist als restrictie aan hun theorie verbonden dat er slechts sprake mocht zijn van één gedraging als te verklaren variabele. Sheppard e.a. concludeerden dat de theorie weliswaar grote voorspellende waarde heeft wanneer aan de door Fishbein en Ajzen genoemde basiscondities wordt voldaan, maar dat de voorspellende kracht groter is wanneer niet aan de oorspronkelijke condities is voldaan.

Sheppard e.a. zijn ook nagegaan of de theorie van beredeneerd gedrag meer voorspellende waarde krijgt indien niet aan de drie eerder genoemde oorspronkelijke uitgangspunten werd voldaan [SHEP88]. De relatie tussen de attitude toward the behavior, subjective norm en gedragsintentie bleek inderdaad, zoals de theorie aangeeft, sterker te zijn wanneer expliciet gevraagd werd naar de gedragsintentie als voornemen ("ik ben van plan om het gedrag uit te voeren"), dan wanneer gevraagd werd naar de verwachting dat men tot het gedrag zou overgaan ("ik zal het gedrag uitvoeren"). Maar aan de andere kant leverde het hanteren van de verwachting, en niet van de gedragsintentie, juist een sterker verband op met het gedrag zelf.

4.2 Vooronderzoek

In dit deel van het onderzoek is de pilot-vragenlijst ontwikkeld en getest. De doelstelling van deze pilot-vragenlijst was het verkrijgen van informatie op grond waarvan een betrouwbaar en valide meetinstrument voor het hoofdonderzoek ontwikkeld kon worden. In dit deel wordt de uitzetprocedure, de onderzoekselementen en procedure, het meetinstrument en de operationalisatie van de pilot-vragenlijst behandeld.

4.2.1 Onderzoekselementen en procedure

De data voor de pilot-vragenlijst is verzameld in de maand juli 2008 over een periode van twee weken. Het verzamelen van deze data is geschied middels de online vragenlijst applicatie: LimeSurvey (http://www.limesurvey.org/). In bijlage 8.3 "Introductiepagina vragenlijst" is de introductiepagina van de vragenlijst weergegeven. Voor een zo veilig mogelijke uitwisseling van gegevens tussen respondent en de online vragenlijst applicatie is gebruik gemaakt van het HTTPS-protocol. Om deze online vragenlijst applicatie te hosten is samenwerking met CNCZ binnen de Radboud Universiteit Nijmegen aangegaan. Aangezien de pilot-vragenlijst een grote vragenlijst betrof is er voor gekozen om deze uit te zetten binnen Capgemini Nederland. Binnen deze organisatie is weer een opsplitsing

gemaakt naar een aantal afdelingen. Deze afdelingen zijn intern via de e-mail benaderd. De pilot-vragenlijst is binnen deze afdelingen gestuurd naar 365 medewerkers. Dit uitzetten is geschied middels een uitzetbrief (zie Bijlage 8.4 "Uitzetbrief") om de medewerkers op de hoogte te stellen en informatie te geven over het onderzoek. Er is met opzet gekozen voor een *selecte steekproef* omdat de bedoeling van de pilot-vragenlijst niet is om een goede afspiegeling te vormen van de gehele populatie medewerkers binnen organisaties in Nederland, maar om te meten of de vragenlijst methodologisch goed in elkaar zit volgens de eisen die Ajzen eraan stelt. Deze eisen zullen toegelicht worden in de delen "meetinstrument" en "operationalisaties". De verantwoording van de externe validiteit is om deze reden niet van toepassing op het vooronderzoek. Er is binnen de groep medewerkers *indirect* onderscheid gemaakt in functie en specialisme. Dit komt doordat er in de vragenlijst gevraagd wordt naar bepaalde functies en bepaalde specialismen van de medewerkers, maar deze worden in de pilot-vragenlijst niet meegenomen. Uiteindelijk is het responsepercentage erg laag gebleken. Van de 365 benaderde medewerkers waren er 63 potentiële respondenten (medewerkers die op de link van de pilot-vragenlijst hebben geklikt), hiervan hebben 16 respondenten de pilot-vragenlijst volledig ingevuld. Dit is dus een response van 4,4%. Van de volledige respondenten was 62,5% man en 37,5% vrouw. Er zijn verklaringen voor het lage responsepercentage, maar deze zullen worden toegelicht in het nu volgende deel.

4.2.2 Meetinstrument

In dit onderzoek is gebruik gemaakt van een online vragenlijst applicatie. De pilot-vragenlijst bestond uit 8 feiten- en opinievragen en 13 subcategorieën. De subcategorieën en vraagstellingen zijn gebaseerd op de handleidingen van Ajzen en Francis [AJZE02], [FRAN04]. De items zijn ontwikkeld aan de hand van de componenten voor de informatievoorziening: *procedures*, *applicaties*, *gegevensinfrastructuur* en *IT-infrastructuur*. Op basis van deze componenten zijn de 93 gedragingen (zie Bijlage 8.1 "Employee Security-Related Behavior List") van Stanton gecategoriseerd [STAN06]. Dit is de reden dat er veel items in de pilot-vragenlijst zaten. Ajzen gaat ervan uit dat voor het meten van één specifiek gedrag *minimaal* 41 items nodig zijn. Uiteindelijk moest de pilot-vragenlijst voldoen aan de "Employee Security-Related Behavior List gerelateerd aan de informatievoorziening waar informatiebeveiliging op van toepassing is" (zie Bijlage 8.5 "Employee Security-Related Behavior List gerelateerd aan de informatievoorziening") die zes hoofdonderwerpen bevat: *bedrijfsgegevens*, *bedrijfssoftware*, *bedrijfshardware*, *policy*, *actieve of passieve informatiebeveiliging* en *training en bewustwording*. Door deze hoofdonderwerpen is er in dit onderzoek sprake van meerdere gedragsalternatieven. Deze gedragsalternatieven vormen samen het geheel van de informatievoorziening waar informatiebeveiliging op van toepassing is. Hiervoor is gekozen omdat gedrag dat wordt geoperationaliseerd aan de hand van verschillende gedragsalternatieven leidt tot sterkere correlaties tussen attitude toward the behavior en subjective norm enerzijds en de gedragsintentie als voornemen anderzijds, dan wanneer er slechts van één gedragsalternatief sprake is. Door het onderscheid in de zes hoofdonderwerpen betekende het dat er zes gedragingen x 59 items = 354 items in de pilot-vragenlijst zaten. Een gemiddelde medewerker binnen een organisatie in Nederland heeft geen tijd om een vragenlijst van deze omvang vrijwillig in te vullen. Dit is een reden waarom er niet veel respondenten voor de pilot-vragenlijst waren. De items uit de subcategorieën konden worden ingevuld aan de hand van een 5-punts Likert schaal, van 1 tot en met 5 en van -2 tot en met 2. Er waren verschillende antwoordcategegoriën gebonden aan deze schalen [OSGO57]. De overige vragen waren feitenvragen en opinievragen. Aangezien dit een nieuw ontwikkeld meetinstrument is, stelt Ajzen de eis dat er een pilot-vragenlijst uitgezet dient te worden om de volgende reden: een set van items moet een hoge correlatie hebben met elkaar. Dit betekent dat de meting van de set van items een hoge interne consistentie moet hebben. Hiervoor wordt meestal de Cronbach's alpha gebruikt [AJZE02]. Hoe deze Cronbach's alpha berekend is op de verschillende set van items komt in het volgende deel aan bod.

4.2.3 Operationalisaties

Om de pilot-vragenlijst te operationaliseren geeft de TpB handleiding van Ajzen aan dat op voorhand de zogenaamde ***T***(arget) ***A***(ction) ***C***(ontext) ***T***(ime) elementen van een bepaald gedrag moet worden gedefinieerd [AJZE02]. Deze TACT elementen van een bepaald gedrag definiëren het geheel op een theoretisch niveau. Dit ziet er als volgt uit:

T(arget): de informatievoorziening.

A(ction): het beveiligen en veilig omgaan met.

C(ontext): binnen de organisatie.

T(ime): gedurende de tijd dat de medewerker bezig is met werkzaamheden voor de organisatie.

In het volgende deel zullen de verschillende variabelen uit de theorie van gepland gedrag geoperationaliseerd worden naar de items uit de pilot-vragenlijst. Hierbij wordt niet op item niveau ingegaan. Ajzen adviseert om de "personal salient beliefs" en "modal salient beliefs" via interviews met mensen te inventariseren. Hier is in dit onderzoek van afgeweken, omdat medewerkers binnen organisaties in Nederland veelal onderworpen zijn aan beleid, richtlijnen, voorschriften en procedures. De "personal salient beliefs" en "modal salient beliefs" zijn in dit onderzoek geïnventariseerd via de literatuur, een vragenlijst van Stanton, de "Employee Security-Related Behavior List gerelateerd aan de informatievoorziening waar informatiebeveiliging op van toepassing is" en de checklist met betrekking tot informatiebeveiliging.

Gedragsintentie

Er zijn zes hoofdonderwerpen uit de "Employee Security-Related Behavior List gerelateerd aan informatiebeveiliging" onderscheiden en per hoofdonderwerp is er naar één item met betrekking tot de intentie gevraagd. Hiervoor is gekozen om de pilot-vragenlijst niet nog groter te laten worden dan dat deze al was. Intenties zijn indicatoren van hoe hard men bereid is zijn best te doen of hoeveel moeite men wil doen om het gedrag uit te voeren [AJZE91]. De pilot-vragenlijst bevat bij zes items drie verschillende schalen die ontwikkeld zijn door Ajzen. Deze schalen bevragen of men "de intentie heeft", of men "van plan is", of men "wil" en of men "verwacht" [AJZE02], [FRAN04]. De Cronbach's alpha voor deze schalen kan niet berekend worden, aangezien er maar één item met betrekking tot de intentie per hoofdonderwerp gevraagd is.

Attitude toward the behavior

De attitude ten opzichte van de zes hoofdonderwerpen uit de "Employee Security-Related Behavior List" is gemeten met schalen die zijn gebaseerd op schalen uit de TpB handleiding van Ajzen [AJZE02]. Hij onderscheidt instrumental items (of het gedrag iets bereikt, bijvoorbeeld: nuttig – nutteloos) en experiential items (hoe het voelt om het gedrag uit te voeren, bijvoorbeeld: prettig – onprettig) van de attitude. Er is in de pilot-vragenlijst gekozen voor drie instrumental items en twee experiential items. De schalen nuttig – nutteloos en gemakkelijk – moeilijk zijn ook terug te koppelen naar het "Technology acceptance model" van Davis [DAVI89]. De schaal nuttig – nutteloos gaat in op de *perceived usefulness* en de schaal gemakkelijk – moeilijk gaat in op de *perceived ease of use*. Deze items zijn gekozen op basis van toepasbaarheid op de zes hoofdonderwerpen. Voorbeelden zijn: "Ik vind het veilig omgaan met de informatievoorziening van de organisatie verstandig", "Ik vind het veilig onbeheerd achterlaten van mijn computer vervelend" en "Ik vind het volgens het bedrijfsbeleid

handelen omtrent het veilig omgaan met de informatievoorziening van de organisatie voor mij nuttig". Aangezien er zes hoofdonderwerpen zijn zullen er ook zoveel Cronbach's alphas voor deze schaal berekend worden.

Subjective norm

De items binnen de subjective norm zijn gebaseerd op twee verschillende soorten: descriptive norm en injunctive norm. Items met een injunctive norm hebben betrekking op het gedrag wat belangrijke (lees invloedrijke) mensen in de omgeving denken van het vertoonde gedrag van de persoon in kwestie, bijvoorbeeld: "Mijn direct leidinggevende vindt dat ik (nooit – altijd) veilig om moet gaan met mijn computer(s), het bedrijfsnetwerk en de randapparatuur". Maar items van deze vorm hebben een probleem. Vaak wordt een lage veranderlijkheid gevonden bij antwoorden op dit soort items, omdat belangrijke mensen vaak gewenst gedrag goedkeuren en ongewenst gedrag afkeuren. Om dit probleem op de lossen zijn er items met descriptive norm toegevoegd. Items met een descriptive norm hebben betrekking op het gedrag van andere mensen die betrekking hebben op de persoon in kwestie, bijvoorbeeld: "De meeste mensen die belangrijk voor mij zijn gaan veilig om met hun computer(s), het bedrijfsnetwerk en de randapparatuur" (zeer mee oneens – zeer mee eens) [AJZE02]. De gebruikte schalen voor de subjective norm zijn gebaseerd op de schalen genoemd in Ajzen en Francis [AJZE02], [FRAN04]. De schaal is op sommige items aangepast, zodat deze aansluit op het gedrag in kwestie.

Perceived behavioral control

De items binnen de perceived behavioral control zijn gebaseerd op twee verschillende soorten: self-efficacy en controllability. Items met betrekking tot de self-efficacy gaan in op de vraag of de respondent capabel is om het gedrag in kwestie te vertonen. Sommige items kunnen dan ingaan op de moeilijkheidsgraad van het te vertonen gedrag, andere items kunnen ingaan op de waarschijnlijkheid dat het gedrag vertoond wordt. Voorbeelden van deze items zijn: "Voor mij is het verzinnen van een complex wachtwoord (zeer gemakkelijk – zeer moeilijk)" en "Ik ben ervan overtuigd dat ik volgens het e-mail beleid kan handelen (zeer mee oneens – zeer mee eens)". Items met betrekking tot de controllability richten zich op de overtuiging van mensen dat zij de controle hebben over het gedrag in kwestie, waarbij het niet uitmaakt wiens prestatie het is. Voorbeelden van deze items zijn: "Ik heb het maken van back-ups van mijn bedrijfsgegevens volledig onder controle (zeer mee oneens – zeer mee eens)" en "Of ik handel volgens het Internet beleid is volledig aan mij (zeer mee oneens – zeer mee eens)" [AJZE02]. De gebruikte schalen voor de perceived behavioral control zijn gebaseerd op de schalen genoemd in Ajzen en Francis [AJZE02], [FRAN04]. De schaal is op sommige items aangepast, zodat deze aansluit op het gedrag in kwestie.

Feiten- en opinievragen

Er zijn in het begin van de vragenlijst verschillende feiten- en opinievragen gesteld. Eerst zullen de verschillende feitenvragen kort toegelicht worden. Er is gevraagd naar "geslacht", "leeftijd", "managementfunctie", "aantal jaar werkzaam als professional op de arbeidsmarkt", "branche", "aantal uur per week binnen de organisatie werkzaam met automatiseringsmiddelen en progamma's" en "aantal uur per week privé werkzaam met automatiseringsmiddelen en programma's". Er is één opinievraag gesteld in de pilot-vragenlijst. Deze opinievraag ging over of de respondent zich beschouwt als een IT-specialist.

4.2.3.1 Interne validiteit

Om de interne validiteit van de pilot-vragenlijst te waarborgen is veel aandacht besteed aan de kwaliteit van de vragen. De interne validiteit is vergroot, doordat de vragen die in de gesloten vragenlijst zitten afkomstig en mede ontwikkeld zijn vanuit het kennisgebied van de arbeids- en organisatiepsychologie. Binnen de arbeids- en organisatiepsychologie zijn verschillende vragenlijsten beschikbaar om verschillende aspecten van gedrag te meten. Binnen dit onderzoek is de TpB handleiding van Ajzen als leidraad gebruikt om de pilot-vragenlijst te construeren met op de achtergrond de beschikbare kennis van de arbeids- en organisatiepsychologie. De item elementen van de determinanten (attitude toward the behavior, subjective norm, perceived behavioral control en gedragsintentie) zijn gedefinieerd op basis van precies dezelfde elementen die beschreven staan in de eerdergenoemde TACT. Dit wil dus zeggen dat alle elementen binnen de items compatibel zijn met de TACT elementen. Op deze manier is er dus voor gezorgd dat alle elementen binnen alle items in de vragenlijst terugkomen zodat deze een één op één relatie hebben met de vooraf gedefinieerde TACT elementen. Zo wordt de mogelijkheid geminimaliseerd dat er items worden geconstrueerd die niet voldoen aan de vooraf gedefinieerde grammatica. Sommige items zijn binnen de vragenlijst vanuit praktisch oogpunt gespecialiseerd of gegeneraliseerd. Ajzen zegt dat dit *geen* reden is dat de desbetreffende items niet meer compatibel zijn met de TACT elementen [AJZE02]. Binnen de pilot-vragenlijst is er voor gekozen om de items uit de subcategorieën in te laten vullen aan de hand van een 5-punts Likert schaal, omdat deze schriftelijke methode er voor zorgt dat moeilijk te kwantificeren gegevens toch kunnen worden ondervraagd [LIKE32]. Dit zorgt er voor dat de respondent gemakkelijker een passend antwoord kan vinden op een vraag, wat resulteert in betrouwbaardere resultaten. Verder is de Cronbach's alpha bepaald om te zorgen dat een set van items bij de *directe* meting een hoge correlatie heeft met elkaar (zie Bijlage 8.6 "Cronbach's alpha vooronderzoek"). Dit betekent dat de meting van de verschillende sets van items een zo hoog mogelijke interne consistentie hebben met elkaar. Door eventueel items binnen een set van items te schrappen is ervoor gezorgd dat de Cronbach's alpha zo hoog mogelijk was, waardoor een set van items betrouwbaarder is geworden omdat deze items een hoge onderlinge consistentie hadden. Een Cronbach's alpha van .60 of hoger is acceptabel voor de interne betrouwbaarheid van een set van items [FRAN04]. De Cronbach's alpha scores zijn vergelijkbaar met de cijfers in een rapport. Om te zorgen dat een set van items bij een *indirecte* meting een hoge interne consistentie met elkaar hebben moet dezelfde vragenlijst door dezelfde respondenten op verschillende tijdstippen beantwoord worden (Test-Retest Reliability). Dit is voor de pilot-vragenlijst vanwege tijdsgebrek niet haalbaar gebleken. Maar Ajzen stelt dat er geen aanname is dat "salient beliefs" intern consistent zijn. Verder is interne consistentie voor de indirecte meting van een set van items niet noodzakelijk [AJZE02]. Om te zorgen dat respondenten de vragenlijst via een gestructureerde manier in konden vullen is er voor gekozen om de items per blok te stellen; dus eerst *gedragsintentie*, dan *attitude toward the behavior*, dan *subjective norm* en dan *perceived behavioral control*. Dit is tegen het advies van de TpB handleiding in, maar vanuit praktisch oogpunt is daarvan afgeweken. Om de vragen betrouwbaar te houden en niet teveel te eisen van de leescapaciteit van de respondenten is hiervan afgeweken. Verder zijn alle items nog eens aan het ***T***(topic) ***A***(pplicability) ***P***(erspective) criteria onderworpen om er zeker van te zijn dat elke vraag een juiste en concrete vraagstelling had.

De pilot-vragenlijst was binnen dit onderzoek een essentieel onderdeel aangezien hier de interne validiteit van de verschillende itemsets is onderzocht. Vanuit deze pilot-vragenlijst is middels aanpassing op basis van de inzichten uit dit vooronderzoek, getracht een zo'n betrouwbaar mogelijke final vragenlijst te construeren, waarbij alleen itemsets gebruikt worden die hoog op de Cronbach's alpha scoren. Uiteindelijk zijn de benodigde data voor de pilot-vragenlijst verkregen via respondenten op vrijwillige basis. De pilot-vragenlijst was anoniem en vertrouwelijk afgenomen om zo te zorgen dat de resultaten hiervan zo betrouwbaar mogelijk waren. Sociaal wenselijke antwoorden worden door het garanderen van anonimiteit en vertrouwelijkheid geminimaliseerd. De pilot-vragenlijst was in zoverre anoniem dat de respondenten wel bepaalde feiten- en opinievragen moesten

beantwoorden, maar de informatie die uit deze vragenlijst naar voren zou komen, zou uitsluitend gebruikt worden voor dit onderzoek.

Voor het online uitzetten van de vragenlijst is gebruik gemaakt van LimeSurvey. Dit had een aantal redenen die bijdragen aan de betrouwbaarheid van de itemsets:

- Het maakt gebruik van een vriendelijk gebruikersinterface. Hierdoor was het voor de respondenten gemakkelijk om antwoord te geven op de items.
- De vragenlijst kon op ieder gewenst moment opgeslagen worden om zo na een gewenste tijd weer verder te kunnen gaan.
- De data staan in de vragenlijst gestructureerd en kan een directe export naar een statistische applicatie maken, waardoor er geen kans bestaat op fouten bij het overtypen of inlezen van de antwoorden.

4.3 Hoofdonderzoek

In dit deel van het onderzoek is de hoofdvragenlijst (zie Bijlage 8.8 "Item lijst") ontwikkeld en getest. Deze hoofdvragenlijst is gebaseerd op de pilot-vragenlijst. De doelstelling van deze hoofdvragenlijst is om te kijken of de vooraf opgestelde deelvragen beantwoord kunnen worden. In dit hoofdstuk wordt de uitzetprocedure, de onderzoekselementen en procedure, het meetinstrument en de operationalisatie van de hoofdvragenlijst behandeld. De term vragenlijst zal in het vervolg gebruikt worden in plaats van de term hoofdvragenlijst. Deze twee termen hebben dezelfde betekenis.

4.3.1 Onderzoekselementen en procedure

Voorafgaand aan de uitzet van de vragenlijst is een gewenste situatie ontwikkeld. Deze gewenste situatie bevat de gewenste onderzoekselementen en procedure. Aangezien tijdens de uitzet van de vragenlijst niet kon worden voldaan aan de gewenste onderzoekselementen is besloten om van sommige punten af te zien en te focussen op *haalbare* onderzoekselementen. Binnen de "gewenste onderzoekselementen en procedure" zullen alleen de punten worden behandeld die voor de uitzet van de vragenlijst als gewenst gezien waren en afwijken van de "werkelijke onderzoekselementen en procedure". De gewenste procedure week nauwelijks af van de werkelijke procedure en zal dus niet behandeld worden in het deel "gewenste onderzoekselementen en procedure". In het laatste deel zullen de "gevolgen van werkelijke onderzoekselementen en procedure" behandeld worden. Hierin komt aan bod waarom het in de werkelijke situatie anders is gegaan dan in de gewenste situatie en wat de gevolgen hier dan van zijn.

4.3.1.1 Gewenste onderzoekselementen en procedure

Binnen dit deel zullen alleen de punten worden behandeld die voor de uitzet van de vragenlijst als gewenst gezien waren en afwijken van het volgende deel de "werkelijke onderzoekselementen en procedure". De gewenste onderzoekselementen voor dit onderzoek waren 664 medewerkers binnen organisaties in Nederland. Deze 664 medewerkers zouden onderverdeeld worden binnen verschillende branches: hightech industrie, overige industrie, kennisintensieve dienstverlening en overige dienstverlening. Dit zou leiden tot een optimale verdeling van ongeveer 166 medewerkers per branche. Deze werden, net als de werkelijke situatie, ook weer onderverdeeld in verschillende bedrijfsrollen; managers, IT-specialisten en overige medewerkers. Dit betekende dat in elke groep 56

medewerkers zouden zitten. De vereiste steekproefgrootte van 664 medewerkers binnen organisaties in Nederland was gebaseerd op de totale populatie van 7.409.000 medewerkers[34] binnen bovengenoemde branches. De vereiste steekproefgrootte was gebaseerd op een foutmarge[35] van 5% en een betrouwbaarheidsniveau[36] van 99%. Dit betekent dat in 99% van de gevallen de proportie binnen het universum 5% onder of boven de gevonden steekproefverhouding ligt[37]. Deze percentages zijn berekend op basis van de totale populatie medewerkers binnen organisaties in Nederland. Onderstaande tabel geeft een duidelijk beeld weer van de gewenste opsplitsing, waarbij de getallen als aantal medewerkers geïnterpreteerd moeten worden.

Tabel 9
Indeling gewenste onderzoekselementen

Bedrijfsrol / Branche	Manager				
	IT-specialist	Niet-IT-specialist	IT-specialist	Overige medewerker	**Totaal**
Hightech industrie	≈ 28	≈ 28	≈ 56	≈ 56	166
Overige industrie	≈ 28	≈ 28	≈ 56	≈ 56	166
Kennisintensieve dienstverlening	≈ 28	≈ 28	≈ 56	≈ 56	166
Overige dienstverlening	≈ 28	≈ 28	≈ 56	≈ 56	166
Totaal	≈ 111	≈ 111	≈ 221	≈ 221	664

Bovenstaande tekst heeft alleen betrekking op de onderzoekselementen. De procedure in de gewenste situatie was hetzelfde als in de werkelijke situatie en zal dus in het volgende deel beschreven worden.

4.3.1.2 Werkelijke onderzoekselementen en procedure

De data voor de vragenlijst is verzameld in de maanden augustus en september 2008. Het verzamelen van deze data is net als de pilot-vragenlijst ook geschied middels de online vragenlijst applicatie: LimeSurvey. Voor een nog veiligere mogelijke manier van gegevensuitwisseling tussen respondent en deze online vragenlijst applicatie is gebruik gemaakt van het HTTPS-protocol, gehost op een server met betere performance dan de server waar de pilot-vragenlijst op gehost was. De vragenlijst is uiteindelijk uitgezet onder tientallen organisaties. Hierbij varieerde het aantal medewerkers per organisatie van minimaal 2 tot meer dan 10.000. Eerst zijn *sponsoren* binnen verschillende branches gezocht. Dit zoeken naar sponsoren is geschied middels sociale netwerken, vakgroeporganisaties en alumni groepen. Sponsoren zijn medewerkers binnen organisaties die bereid waren om medewerkers binnen hun organisatie of mensen binnen hun eigen netwerk te benaderen om de vragenlijst in te vullen. Het voordeel van sponsoren is dat er een centraal aanspreekpunt voor een bepaalde organisatie is. Een ander voordeel is dat medewerkers eerder iemand (in dit geval een

[34] De totale populatie medewerkers is gebaseerd op cijfers van het CBS.
http://statline.cbs.nl/StatWeb/publication/?VW=T&DM=SLNL&PA=7511nr&D1=0-4,7,14-16,18&D2=0&D3=a,!0-12&HD=080401-1658&HDR=T&STB=G1,G2

[35] De foutmarge is de grootte van de fout die wordt toegestaan.

[36] Het betrouwbaarheidsniveau is de mate van onzekerheid die wordt toegelaten.

[37] https://www.wetenschapsinformatienetwerk.be/uploads/documentenbank/b5ddb69395b05e08926bf690c78dbc4b.pdf

sponsor) vertrouwen die bekend voor ze is dan iemand (in dit geval de onderzoekers) die onbekend voor ze zijn. Alle gevonden sponsoren zijn vastgelegd in een contactlijst om zo bij te houden wie benaderd was, wie zelf deelnam aan de vragenlijst en wie de vragenlijst uit zou zetten binnen zijn organisatie en eigen netwerk. Deze sponsoren zijn veelal via e-mail benaderd. Om het voor de sponsoren gemakkelijk te maken om potentiële respondenten te vinden is er voor gekozen om een uitzetbrief mee te sturen (zie Bijlage 8.4 "Uitzetbrief"). Deze uitzetbrief was er om de benaderde medewerkers door de sponsoren op de hoogte te stellen en informatie te geven over het onderzoek. Een belangrijk toegelicht punt in de uitzetbrief was wat de potentiële respondenten zelf aan het onderzoek zouden hebben (de incentive).

De onderzoekselementen voor dit onderzoek zijn 224 medewerkers binnen organisaties in Nederland. Van deze 224 medewerkers vallen acht medewerkers buiten de doelpopulatie omdat zij minder dan twee uur per week binnen de organisatie werkzaam zijn met automatiseringsmiddelen en progamma's. De reden hiervoor is dat deze medewerkers te weinig met automatiseringsmiddelen en progamma's werken en dus te weinig bezig zijn met informatiebeveiliging ten opzichte van dit onderzoek. Het meenemen van de antwoorden van deze medewerkers zou vertekende resultaten kunnen opleveren. Voor de externe validiteit is dit noodzakelijk om de data te generaliseren. De 224 medewerkers zijn wel meegenomen voor de interne validiteit omdat deze niet ingaat op de afspiegeling van de werkelijkheid, maar op de betrouwbaarheid van het meetinstrument. Deze 216 medewerkers zijn onderverdeeld binnen verschillende branches; hightech industrie, overige industrie, kennisintensieve dienstverlening en overige dienstverlening. Dit heeft uiteindelijk niet geleid tot een optimale verdeling van ongeveer 50 medewerkers per branche. Er zaten namelijk veel meer medewerkers in de kennisintensieve dienstverlening en overige dienstverlening. Dit heeft natuurlijk als gevolg dat niet elke groep 13 medewerkers bevat. De uiteindelijke steekproefgrootte van 216 medewerkers binnen organisaties in Nederland is, zoals beschreven in de "gewenste onderzoekselementen", gebaseerd op de totale populatie van 7.409.000 medewerkers binnen bovengenoemde branches. De uiteindelijke steekproefgrootte is gebaseerd op een foutmarge van 6% en een betrouwbaarheidsniveau van 92%. Deze percentages zijn, zoals beschreven in de "gewenste onderzoekselementen", berekend op basis van de totale populatie medewerkers binnen organisaties in Nederland. Onderstaand schema geeft een duidelijk beeld van de opsplitsing waarbij de getallen als aantal medewerkers geïnterpreteerd moeten worden.

Tabel 10
Indeling werkelijke onderzoekselementen

Bedrijfsrol / Branche	Manager				
	IT-specialist	Niet-IT-specialist	IT-specialist	Overige medewerker	**Totaal**
Hightech industrie	2	3	4	1	10
Overige industrie	0	6	0	3	9
Kennisintensieve dienstverlening	37	15	44	27	123
Overige dienstverlening	13	19	18	24	74
Totaal	52	43	66	55	216

De steekproef heeft als volgt plaatsgevonden. Er zijn *sponsoren* binnen verschillende branches gezocht. Aan de sponsoren is gevraagd of zij andere medewerkers binnen hun organisatie of mensen binnen hun eigen netwerk wilden benaderen om de vragenlijst in te vullen. Maar dan ook weer met de vraag of de benaderde mensen door de sponsoren precies hetzelfde wilden doen. Op deze manier

is de steekproef steeds groter geworden en heeft het een soort van sneeuwbaleffect gekregen. Binnen dit onderzoek is dus sprake van een sneeuwbalsteekproef. Een sneeuwbalsteekproef is een niet-aselecte steekproef[38]. Er is gekozen voor een niet-aselecte steekproef omdat de benodigde middelen (niet voldoende "eigen contacten", geen budget en onvoldoende tijd) om een aselecte steekproef te trekken niet aanwezig waren. De sneeuwbalsteekproef past ook in dit onderzoek aangezien het een gerichte keuze steekproef is. In een gerichte keuze steekproef worden alleen analyse-eenheden opgenomen die aan bepaalde vooraf afgesproken kenmerken voldoen. Dit heeft uiteindelijk verschillende respondenten opgeleverd die werkzaam zijn binnen organisaties in verschillende branches. Aan alle respondenten is de feitenvraag gesteld of zij een managementfunctie bekleden en opinievragen of zij zichzelf als een IT-specialist beschouwen. Er is dus een onderverdeling gemaakt in branche en in bedrijfsrol. Deze verdeling is toegepast omdat het wel of niet hebben van een managementfunctie, de IT kennis en vaardigheden en de branche mogelijk invloed hebben op de gedragsintentie.

Non-response is in dit onderzoek tegengegaan door de vragenlijst anoniem en vertrouwelijk te maken. Het is zo dat mogelijke respondenten eerder reageren wanneer zij anoniem blijven en er vertrouwelijk met zijn of haar gegevens wordt omgegaan. Verder is het zo dat de vragenlijst eerder naar waarheid ingevuld wordt als deze anoniem en vertrouwelijk blijft. Sociaal wenselijke antwoorden worden door het garanderen van anonimiteit en vertrouwelijkheid geminimaliseerd. Ten tweede is dit tegengegaan door de respondenten niet rechtstreeks te benaderen om te vragen of ze de vragenlijst in wilden vullen, maar via de bovengenoemde sponsoren binnen de organisaties. Ten derde is de drempel lager om een online vragenlijst in te vullen dan een vragenlijst met pen en papier. Uiteindelijk is het responsepercentage over het totaal aantal benaderde medewerkers moeilijk te berekenen. Dit komt doordat de vragenlijst via sponsoren is uitgezet. De beschreven manieren om non-response tegen te gaan waren helaas niet voldoende om response te krijgen vanuit gevoelige sectoren als politie of defensie. Het responsepercentage over het aantal medewerkers dat geklikt heeft op de link van de vragenlijst is natuurlijk wel te berekenen. Van de 403 medewerkers die geklikt hebben op de link waren er 224 volledige respondenten. Dit is dus een response van 55,6%. Per organisatie varieerde het aantal respondenten van 1 tot maximaal 40. Van de respondenten die de vragenlijst volledig hebben ingevuld zijn verschillende demografische gegevens bekend (zie Bijlage 8.7 "Demografische gegevens").

4.3.1.3 Gevolgen van werkelijke onderzoekselementen en procedure

Het belangrijkste verschil tussen de werkelijke situatie en de gewenste situatie is het aantal onderzoekselementen. Er zijn verschillende redenen waarom dit verschil is opgetreden:

- Het privacy beleid van de organisatie waarbinnen de medewerker actief is liet het niet toe om aan de vragenlijst deel te nemen.
- Vanuit privacy oogpunt van de medewerker zelf is besloten om niet aan de vragenlijst deel te nemen.
- Door het grote aantal items in de vragenlijst is de respondent afgehaakt.
- Door het grote aantal eentonig gestelde items in de vragenlijst is de respondent afgehaakt.
- Medewerkers hebben niet deelgenomen aan de vragenlijst omdat ze twijfelde aan de vertrouwelijkheid en gevoeligheid van de gegevens die eruit zouden komen.
- Medewerkers hebben niet deelgenomen aan de vragenlijst omdat ze angst hadden om antwoord te geven op de items.

[38] Een niet-aselecte steekproef is een steekproef waarbij de kans om in de steekproef terecht te komen onbekend is.

- De vragenlijst is in de vakantieperiode uitgezet.
- Bepaalde organisaties konden door het blokkeren van de proxyserver van de desbetreffende organisatie het internetadres van de vragenlijst niet benaderen.

Het gevolg van het beperkte aantal onderzoekselementen was dat het betrouwbaarheidsniveau en de foutmarge aangepast moest worden. In de gewenste situatie was de steekproefgrootte gebaseerd op een betrouwbaarheidsniveau van 99% en een foutmarge van 5%. In de werkelijke situatie is de steekproefgrootte gebaseerd op een betrouwbaarheidsniveau van 92% en een foutmarge van 6%. Dit betekent voor de foutmarge dat de grootte van de fout die wordt toegestaan in de werkelijke situatie 1% hoger is dan in de gewenste situatie. Voor het betrouwbaarheidsniveau betekent dit dat de mate van onzekerheid die wordt toegelaten in de werkelijke situatie 7% hoger is dan in de gewenste situatie. De percentages van de foutmarge en het betrouwbaarheidsniveau in de werkelijke situatie worden binnen de statistiek als valide beschouwd.

4.3.1.4 Externe validiteit

Om de externe validiteit te waarborgen is het onderzoekselement zo gekozen dat deze representatief is voor alle medewerkers binnen organisaties in Nederland. Het onderzoek kan niet uitgevoerd worden binnen één organisatie, omdat niet één organisatie binnen alle branches in Nederland opereert. Daarom is gekozen om organisaties binnen verschillende branches te onderzoeken.

Het is niet mogelijk om alle organisaties binnen alle branches in Nederland te onderzoeken, maar om toch te zorgen dat de te onderzoeken organisaties binnen de branches representatief zijn voor alle organisaties in Nederland is tijdens het zoeken naar organisaties rekening gehouden met de opsplitsing van branches: hightech industrie, overige industrie, kennisintensieve dienstverlening en overige dienstverlening. Deze vier branches omvatten samen alle organisaties in Nederland. Voor elke branche zijn verschillende sponsoren gezocht die werkzaam zijn binnen organisaties in de desbetreffende branche. Uiteindelijk zijn deze sponsoren op basis van "eigen contacten" ook gevonden.

Door de toegepaste sneeuwbalsteekproef blijkt het onvermijdelijk dat er *onderdekking* ten opzichte van de doelpopulatie is opgetreden. Onderdekking treedt op wanneer niet de volledige doelpopulatie bereikt kan worden. Er zijn in dit onderzoek medewerkers die nooit in de steekproef hebben kunnen komen. Een verklaring hiervoor is dat leden van de doelpopulatie die minder bekend of minder populair zijn of wiens meningen botsen met die van de respondent een kleine kans hebben om te worden geselecteerd. Door de sneeuwbalsteekproef blijkt het ook dat er *overdekking* is opgetreden. Overdekking treedt op wanneer er per ongeluk toch personen in de steekproef terechtkomen die niet tot de doelpopulatie behoren. Er zijn in dit onderzoek medewerkers in de steekproef terechtgekomen die niet tot de doelpopulatie behoren. Hier is rekening mee gehouden door respondenten die minder dan twee uur per week binnen de organisatie werkzaam zijn met automatiseringsmiddelen en progamma's uit het steekproefkader te verwijderen. De non-response is geprobeerd zoveel mogelijk terug te dringen door de vragenlijst anoniem en vertrouwelijk af te nemen. Er waren 403 medewerkers die geklikt hebben op de link van de vragenlijst. Daarvan hebben 179 medewerkers de vragenlijst niet afgemaakt. De non-response was dus 44,4%. De werkelijke non-response is niet te berekenen. Dit komt doordat het onbekend is wat de totale steekproef is geweest.

Doordat LimeSurvey gebruikt maakt van sessies en cookies was het voor de respondent moeilijker om de vragenlijst meerdere keren in te vullen. Het was niet onmogelijk om dit te doen, maar de kans dat dit zou gebeuren is enigszins gereduceerd. Door deze functie van LimeSurvey is gezorgd dat er minder fouten opgetreden zijn in de response. Dit is door de grootte van de

vragenlijst en de bereidheid van medewerkers om hem in te vullen niet heel erg relevant. Maar als er toch medewerkers bijzitten die het onderzoek willen verstoren met spam, is het op bovenstaande manier toch enigszins gereduceerd.

4.3.2 Meetinstrument

Zoals genoemd is ook de vragenlijst afgenomen middels de online vragenlijst applicatie LimeSurvey. De vragenlijst bestond uit 9 feiten- en opinievragen en 13 subcategorieën. De subcategorieën en vraagstellingen zijn precies hetzelfde als in de pilot-vragenlijst. Ook zijn de meeste ontwikkelde items hetzelfde gebleven. Maar doordat er in de pilot-vragenlijst veel items zaten, zijn alle items op basis van de volgende hoofdonderwerpen verwijderd uit de vragenlijst: *bedrijfssoftware*, *bedrijfshardware*, *actieve of passieve informatiebeveiliging*. De hoofdonderwerpen *policy* en *training en bewustwording* zijn voor een *deel* geschrapt uit de vragenlijst. De vragenlijst heeft zijn focus dus gekregen op het hoofdonderwerp *bedrijfsgegevens*. Hiervoor is gekozen omdat dit hoofdonderwerp het meest fundamentele deel van de informatievoorziening is. Verder zijn de items met betrekking tot dit hoofdonderwerp op een gemakkelijke basale manier uit te drukken. Onder het hoofdonderwerp *bedrijfsgegevens* ligt namelijk de focus op de onderwerpen: ***B***(eschikbaarheid) ***I***(ntegriteit) ***V***(ertrouwelijkheid) van bedrijfsgegevens, wachtwoordgebruik en back-up. Binnen het hoofdonderwerp in de vragenlijst komen ook nog items over de hoofdonderwerpen *policy* en *training en bewustwording* aan bod. Deze items zijn dan wel gesteld in relatie tot het hoofdonderwerp *bedrijfsgegevens*. Doordat er nog steeds over verschillende onderwerpen items worden gesteld is er sprake van meerdere gedragsalternatieven. Alleen vormen de gedragsalternatieven nu het geheel van bedrijfsgegevens waar informatiebeveiliging op van toepassing is. Dit betekende dat er drie gedragingen x 59 items = 177 items in de vragenlijst zaten. Het bleek dat de gemiddelde medewerker binnen een organisatie in Nederland nu wel een vragenlijst van deze omvang vrijwillig in wilde vullen. Er is om de items in te vullen ook weer gebruik gemaakt van een 5-punts Likert schaal, van 1 tot en met 5 en van -2 tot en met 2. Ook de verschillende antwoordcategorieën gebonden aan deze schalen zijn hetzelfde gebleven. De feitenvragen en opinievragen zijn ook hetzelfde gebleven ten opzichte van de pilot-vragenlijst. Er is alleen één opinievraag toegevoegd.

De Cronbach's alpha, berekend op de verschillende set van items, komt in het volgende deel aan bod.

4.3.3 Operationalisaties

Voor de vragenlijst zijn ook de ***T***(arget) ***A***(ction) ***C***(ontext) ***T***(ime) elementen van een bepaald gedrag gedefinieerd. Deze TACT elementen zien er in de vragenlijst hetzelfde uit als in de pilot-vragenlijst.

In het volgende deel zullen de verschillende variabelen uit de theorie van gepland gedrag geoperationaliseerd worden naar de items uit de vragenlijst. Hierbij zal per determinant worden ingegaan op itemniveau. Dit itemniveau zal beschreven worden aan de hand van de itemomschrijving, schaalnaam en eventuele categorie. In bijlage 8.8 "Item lijst" zijn alle items van de vragenlijst te vinden met de bijbehorende itemcodes, itemomschrijvingen, schaalnamen en schaalscores. Verder worden de relaties beschreven die gelden tussen de onafhankelijke variabelen (attitude toward the behavior, subjective norm, perceived behavioral control) en de afhankelijke variabele (gedragsintentie). Tevens zullen deze relaties terug te koppelen zijn naar de deelvragen.

In dit onderzoek zijn de mogelijke externe factoren niet specifiek opgenomen, omdat Ajzen en Fishbein veronderstellen dat externe factoren niet rechtstreeks een gedragsintentie beïnvloeden, maar

via de attitude toward the behavior, subjective norm of perceived behavioral control bijdragen aan het ontstaan van een gedragsintentie [AJZE80], [AJZE88]. De feiten- en opinievragen zouden wel als externe factoren opgenomen kunnen worden, maar in dit onderzoek gelden ze als demografische gegevens.

Gedragsintentie

Er is één hoofdonderwerp uit de "Employee Security-Related Behavior List gerelateerd aan informatiebeveiliging" onderscheiden, namelijk: het betrouwbaar omgaan met bedrijfsgegevens. Binnen dit hoofdonderwerp zijn weer de volgende onderwerpen onderkend: beschikbaarheid-integriteit-vertrouwelijkheid van bedrijfsgegevens, wachtwoordgebruik en back-up. Over elk onderwerp zijn drie items met betrekking tot de intentie gevraagd, namelijk: het beschermen van bedrijfsgegevens, het zekerstellen van bedrijfsgegevens en het veilig omgaan met wachtwoordgebruik. De vragenlijst bevat bij elke onderwerp (welke dus uit drie items bestaat) drie verschillende schalen die zijn gebaseerd op schalen genoemd in Ajzen [AJZE02]. Deze schalen bevragen of men "de intentie heeft", of men "van plan is" en of men "wil". Ten opzichte van de pilot-vragenlijst is de schaal of men "verwacht" weggelaten. In de gebruikte schalen in de vragenlijst is alleen gevraagd naar de gedragsintentie als voornemen en niet naar de verwachting dat men tot het gedrag zou overgaan. De reden hiervoor was dat de relatie tussen de attitude toward the behavior, subjective norm en gedragsintentie sterker bleek te zijn wanneer expliciet gevraagd werd naar de gedragsintentie als voornemen, dan wanneer gevraagd werd naar de verwachting dat men tot het gedrag zou overgaan [SHEP88]. Om duidelijk te maken hoe de items met betrekking tot één onderwerp in de vragenlijst gesteld zijn, worden de items met betrekking tot één onderwerp hieronder verder toegelicht. Het werkelijke gedrag is binnen dit onderzoek niet gemeten. De reden hiervoor is dat het meten van het werkelijke gedrag problematisch is, omdat het werkelijke vertoonde gedrag meerdere malen over een bepaalde tijdsperiode gemeten moet worden. Een andere reden is dat medewerkers huiverig zijn met het beantwoorden van items met betrekking tot informatiebeveiliging binnen de organisatie waarin ze actief zijn. Als dit wel gevraagd wordt, bestaat het gevaar dat een sociaal wenselijk antwoord het gevolg is.

- "Mijn intentie is om mijn bedrijfsgegevens te beschermen.": ("zeer onwaarschijnlijk" – … – "zeer waarschijnlijk").
- "Ik wil mijn bedrijfsgegevens beschermen.": ("geheel waar" – … – "geheel niet waar").
- "Ik ben van plan om mijn bedrijfsgegevens te beschermen.": ("zeer mee oneens" – … – "zeer mee eens").

Attitude toward the behavior

De attitude ten opzichte van het hoofdonderwerp uit de "Employee Security-Related Behavior List" is gemeten met schalen die zijn gebaseerd op schalen uit de TpB handleiding van Ajzen [AJZE02]. Binnen dit hoofdonderwerp zijn weer de volgende onderwerpen onderkend: ***B***(eschikbaarheid) ***I***(ntegriteit) ***V***(ertrouwelijkheid) van bedrijfsgegevens, wachtwoordgebruik en back-up. De attitude items zijn onderverdeeld in een *directe* meting en een *indirecte* meting. Bij de directe items is net als bij de pilot-vragenlijst onderscheid gemaakt tussen instrumental items en experiential items. Er is in de vragenlijst gekozen voor drie instrumental items en twee experiential items. Hieronder zijn de items van één onderwerp met betrekking tot de directe meting van attitude toegelicht.

- "Ik vind het beschermen van mijn bedrijfsgegevens tegen onbevoegde kennisname": ("zeer onverstandig" – … – "zeer verstandig"). → instrumental item
- "Ik vind het beschermen van mijn bedrijfsgegevens tegen onbevoegde kennisname voor mij": ("zeer prettig" – … – "zeer vervelend"). → experiential item
- "Ik vind het beschermen van mijn bedrijfsgegevens tegen onbevoegde kennisname voor mij": ("zeer nutteloos" – … – "zeer nuttig"). → instrumental item
- "Ik vind het beschermen van mijn bedrijfsgegevens tegen onbevoegde kennisname": ("zeer gemakkelijk" – … – "zeer moeilijk"). → experiential item
- "Ik vind het beschermen van mijn bedrijfsgegevens tegen onbevoegde kennisname voor anderen": ("zeer nutteloos" – … – "zeer nuttig"). → instrumental item

De indirecte items zijn onderverdeeld in de categorieën *behavioral beliefs* en *outcome evaluations*. Uiteindelijk worden de items uit de twee categorieën die bij elkaar horen samengevoegd. Hieronder staat één set van items die onder de categorie *behavioral beliefs* valt.

- "Als ik een complex wachtwoord verzin, dan zijn mijn bedrijfsgegevens beter beschermd tegen onbevoegde kennisname en ongecontroleerde wijzigingen.": ("zeer onwaarschijnlijk" – … – "zeer waarschijnlijk").
- "Als ik periodiek mijn wachtwoord wijzig, dan zijn mijn bedrijfsgegevens beter beschermd tegen onbevoegde kennisname en ongecontroleerde wijzigingen.": ("zeer onwaarschijnlijk" – … – "zeer waarschijnlijk").
- "Als ik mijn wachtwoord geheimhoud, dan zijn mijn bedrijfsgegevens beter beschermd tegen onbevoegde kennisname en ongecontroleerde wijzigingen.": ("zeer onwaarschijnlijk" – … – "zeer waarschijnlijk").
- "Als ik mijn wachtwoord onthoud, dan zijn mijn bedrijfsgegevens beter beschermd tegen onbevoegde kennisname en ongecontroleerde wijzigingen.": ("zeer onwaarschijnlijk" – … – "zeer waarschijnlijk").

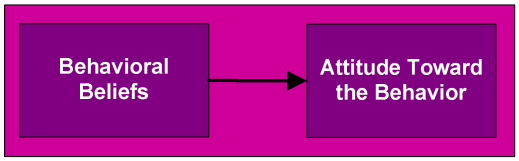
Het volgende item valt onder de categorie *outcome evaluations*. Dit item heeft betrekking op alle bovenstaande items.

- "Dat mijn bedrijfsgegevens beter beschermd zijn tegen onbevoegde kennisname en ongecontroleerde wijzigingen is.": ("zeer ongewenst" – … – "zeer gewenst").

Elk item uit de categorie *behavioral beliefs* wordt apart gekoppeld aan het bijbehorende item uit de categorie *outcome evaluations*. Dit betekent dus dat elk item uit de categorie *behavioral beliefs* vermenigvuldigd wordt met het bijbehorende item uit de categorie *outcome evaluations*.

De te onderzoeken relatie tussen de variabelen attitude toward the behavior en gedragsintentie heeft geresulteerd in de eerste deelvraag: "Wat is de relatie tussen de attitude toward the behavior en de intentie tot gedrag ten aanzien van informatiebeveiliging?"

De relatie van deze deelvraag kan schematisch als volgt weergegeven worden:



Figuur 27: Relatie deelvraag één

Eerst dienen de uiteindelijke scores op de items van de respondenten op de attitude toward the behavior geanalyseerd te worden. Vervolgens zullen al deze scores tegen elkaar afgewogen worden om te beoordelen of de attitude toward the behavior invloed heeft op de gedragsintentie en hoe groot de eventuele invloed is.

Subjective norm

De subjective norm items zijn onderverdeeld in een *directe* meting en in een *indirecte* meting. De items binnen de subjective norm zijn gebaseerd op twee verschillende soorten: descriptive norm en injunctive norm. Dit geldt voor zowel de *directe* meting als de *indirecte* meting. De gebruikte schalen voor de subjective norm zijn gebaseerd op de schalen genoemd in Ajzen en Francis [AJZE02], [FRAN04]. De schaal is op sommige items aangepast, zodat deze aansluit op het gedrag in kwestie. Hieronder zijn de items van één onderwerp met betrekking tot de directe meting van de subjective norm toegelicht.

- "De meeste mensen die belangrijk voor mij zijn vinden dat ik ("altijd" – … – "nooit") mijn bedrijfsgegevens moet beschermen tegen onbevoegde kennisname." → injunctive norm
- "Er wordt van mij verwacht dat ik mijn bedrijfsgegevens bescherm tegen onbevoegde kennisname.": ("zeer mee oneens" – … – "zeer mee eens"). → injunctive norm
- "De meeste mensen die belangrijk voor mij zijn beschermen hun bedrijfsgegevens tegen onbevoegde kennisname.": ("zeer mee oneens" – … – "zeer mee eens"). → descriptive norm

De indirecte items zijn onderverdeeld in de categorieën *normative beliefs* en *motivation to comply*. Uiteindelijk worden de items uit de twee categorieën die bij elkaar horen samengevoegd. Hieronder staat één set van items die onder de categorie *normative beliefs* valt.

- "Naaste collega's, die belangrijk voor mij zijn, vinden dat ik ("nooit" – … – "altijd") mijn bedrijfsgegevens moet beschermen tegen onbevoegde kennisname." → injunctive norm
- "Naaste collega's, die belangrijk voor mij zijn, zorgen er ("nooit" – … – "altijd") voor dat hun bedrijfsgegevens beschermd zijn tegen onbevoegde kennisname." → descriptive norm

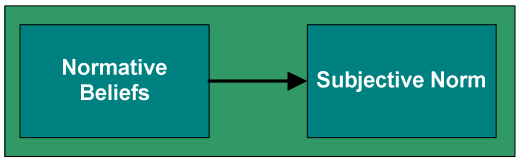
Het volgende item valt onder de categorie *motivation to comply*. Dit item heeft betrekking op alle bovenstaande items (en op alle sets van items die betrekking hebben op *Naaste collega's* welke alleen in bijlage 8.8 "Item lijst" vernoemd zijn).

- "Wat naaste collega's vinden dat ik moet doen is voor mij belangrijk.": ("zeer mee oneens" – … – "zeer mee eens"). → injunctive & descriptive norm

Elk item uit de categorie *normative beliefs* wordt apart gekoppeld aan het bijbehorende item uit de categorie *motivation to comply*. Dit betekent dus dat elk item uit de categorie *normative beliefs* vermenigvuldigd wordt met het bijbehorende item uit de categorie *motivation to comply*.

De te onderzoeken relatie tussen de variabelen subjective norm en gedragsintentie heeft geresulteerd in de tweede deelvraag: "Wat is de relatie tussen de subjective norm en de intentie tot gedrag ten aanzien van informatiebeveiliging?"

De relatie van deze deelvraag kan schematisch als volgt weergegeven worden:



Figuur 28: Relatie deelvraag twee

Eerst dienen de uiteindelijke scores op de items van de respondenten op de subjective norm geanalyseerd te worden. Vervolgens zullen al deze scores tegen elkaar afgewogen worden om te beoordelen of de subjective norm invloed heeft op de gedragsintentie en hoe groot de eventuele invloed is.

Perceived behavioral control

De perceived behavioral control items zijn onderverdeeld in een *directe* meting en een *indirecte* meting. De items binnen de perceived behavioral control zijn gebaseerd op twee verschillende soorten: self-efficacy en controllability. Dit geldt voor zowel de *directe* meting als de *indirecte* meting. De gebruikte schalen voor de perceived behavioral control zijn gebaseerd op de schalen genoemd in Ajzen en Francis [AJZE02], [FRAN04]. De schaal is op sommige items aangepast, zodat deze aansluit op het gedrag in kwestie. Hieronder zijn de items van één onderwerp met betrekking tot de directe meting van de perceived behavioral control toegelicht.

- "Voor mij is het beschermen van mijn bedrijfsgegevens tegen onbevoegde kennisname": ("zeer gemakkelijk" – … – "zeer moeilijk"). → self-efficacy
- "Ik ben ervan overtuigd dat ik mijn bedrijfsgegevens kan beschermen tegen onbevoegde kennisname.": ("zeer mee oneens" – … – "zeer mee eens"). → self-efficacy
- "Ik heb het beschermen van mijn bedrijfsgegevens tegen onbevoegde kennisname volledig onder controle.": ("zeer mee oneens" – … – "zeer mee eens"). → controllability
- "Of ik mijn bedrijfsgegevens bescherm tegen onbevoegde kennisname is volledig aan mij.": ("zeer mee oneens" – … – "zeer mee eens"). → controllability

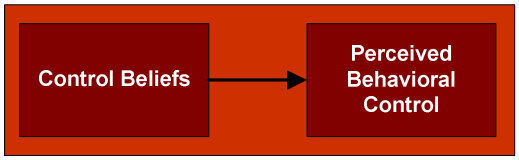
De indirecte items zijn onderverdeeld in de categorieën *control beliefs* en *power to influence*. Uiteindelijk worden de items uit de twee categorieën die bij elkaar horen samengevoegd. Hieronder zijn de items van één onderwerp met betrekking tot de indirecte meting van de perceived behavioral control toegelicht.

- "Ik denk dat ik mijn bedrijfsgegevens kan beschermen tegen onbevoegde kennisname.": ("zeer onwaarschijnlijk" – … – "zeer waarschijnlijk").→ control beliefs
- "Ik vind het ("zeer moeilijk" – … – "zeer gemakkelijk") om mijn bedrijfsgegevens te beschermen tegen onbevoegde kennisname." → power to influence

Elk item uit de categorie *control beliefs* wordt apart gekoppeld aan het bijbehorende item uit de categorie *power to influence*. Dit betekent dus dat het item uit de categorie *control beliefs* vermenigvuldigd wordt met het bijbehorende item uit de categorie *power to influence*.

De te onderzoeken relatie tussen de variabelen perceived behavioral control en gedragsintentie heeft geresulteerd in de derde deelvraag: "Wat is de relatie tussen de perceived behavioral control en de intentie tot gedrag ten aanzien van informatiebeveiliging?"

De relatie van deze deelvraag kan schematisch als volgt weergegeven worden:



Figuur 29: Relatie deelvraag drie

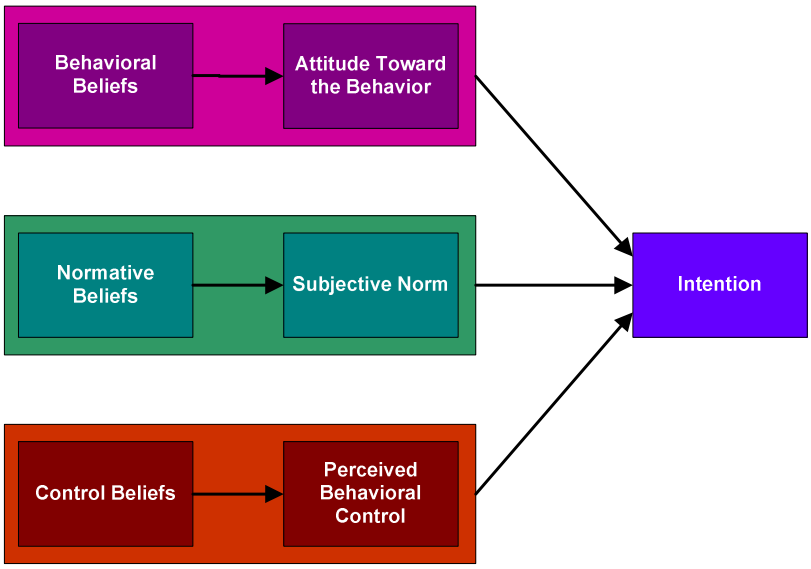
Eerst dienen de uiteindelijke scores op de items van de respondenten op de perceived behavioral control geanalyseerd te worden. Vervolgens zullen al deze scores tegen elkaar afgewogen worden om te beoordelen of de perceived behavioral control invloed heeft op de gedragsintentie en hoe groot de eventuele invloed is.

Feiten- en opinievragen

Er is ten opzichte van de pilot-vragenlijst een tweede opinievraag bijgekomen. Deze ging over het rapportcijfer dat de respondent zichzelf geeft met betrekking tot zijn of haar kennis en vaardigheden ten aanzien van Informatie- en Communicatietechnologie. Deze opinievraag is toegevoegd om de andere opinievraag te controleren. De eerste opinievraag ging over of de respondent zich beschouwt als een IT-specialist.

Deelvraag 4

De te onderzoeken relatie tussen de onafhankelijke variabelen (attitude toward the behavior, subjective norm en perceived behavioral control) en de afhankelijke variabele (gedragsintentie) heeft geresulteerd in de vierde deelvraag: "In hoeverre leveren de attitude toward the behavior, subjective norm en perceived behavioral control een onafhankelijke bijdrage aan het verklaren van de intentie tot gedrag ten aanzien van informatiebeveiliging?"



Figuur 30: Relatie deelvraag vier

Om de vierde deelvraag te kunnen beantwoorden zullen verschillende stappen doorlopen worden. Eerst dient gekeken te worden hoe de uiteindelijke scores op de items van de respondenten op de attitude toward the behavior, subjective norm en perceived behavioral control zich met elkaar verhouden en met elkaar samenhangen. Vervolgens kan gekeken worden of er mogelijke invloeden van de onafhankelijke variabelen (attitude toward the behavior, subjective norm en perceived behavioral control) op de afhankelijke variabele (gedragsintentie) zijn. Uiteindelijk zullen de verschillende relaties (attitude toward the behavior op gedragsintentie, subjective norm op gedragsintentie en perceived behavioral control op gedragsintentie) beoordeeld worden met percentages variërend tussen de 0 en 100. Deze percentages betekenen de hoeveelheid voorspellende waarde van de drie onafhankelijke predictor variabelen (attitude toward the behavior, subjective norm en perceived behavioral control) op de afhankelijke criteriumvariabele gedragsintentie. Bij een percentage van 0 is er geen voorspellende waarde van de onafhankelijke predictor variabele op de afhankelijke criteriumvariabele en bij een percentage van 100 is er heel veel voorspellende waarde van de onafhankelijke predictor variabele op de afhankelijke criteriumvariabele. Dus hoe lager het percentage is, hoe lager de voorspellende waarde van de onafhankelijke predictor variabele op de afhankelijke criteriumvariabele is en vice versa.

4.3.3.1 Interne validiteit

In de pilot-vragenlijst is op de meeste vlakken de interne validiteit gewaarborgd en daarom zijn deze punten ook in de vragenlijst meegenomen. Deze punten zullen in de volgende opsomming nog even kort behandeld worden.

- De TpB handleiding van Ajzen is als leidraad gebruikt om de vragenlijst te construeren met op de achtergrond de beschikbare kennis van de arbeids- en organisatiepsychologie.
- Alle elementen binnen de items zijn compatibel met de TACT elementen.
- De items uit de categorieën zijn door de respondenten ingevuld aan de hand van een 5-punts Likert schaal.
- De meeste itemsets hebben een acceptabele of hoge Cronbach's alpha opgeleverd. Dit betekent dat de verschillende itemsets een hoge interne consistentie met elkaar hebben. De lijst met Cronbach's alphas voor de verschillende itemsets zijn ondergebracht in bijlage 8.9 "Cronbach's alpha hoofdonderzoek".
- De items zijn per blok gesteld; dus eerst *attitude toward the behavior*, dan *subjective norm* en dan *perceived behavioral control*. De gedragsintentie is wel tussen de blokken door gevraagd.
- Items zijn aan het ***T***(topic) ***A***(pplicability) ***P***(erspective) criteria onderworpen.
- De vragenlijst is anoniem en vertrouwelijk afgenomen.
- Voor het online uitzetten van de vragenlijst is gebruik gemaakt van LimeSurvey.
    - Respondenten konden gemakkelijk antwoord geven op de items door de gebruiksvriendelijke interface.
    - De vragenlijst kon op ieder gewenst moment opgeslagen worden om zo na een gewenste tijd weer verder te kunnen gaan.
    - De data staan in de vragenlijst gestructureerd en kan een directe export naar een statistische applicatie maken, waardoor er geen kans bestaat op fouten bij het overtypen of inlezen van de antwoorden.

5. RESULTATEN

De vier deelvragen, die in het eerste hoofdstuk zijn geformuleerd, worden successievelijk in dit hoofdstuk beantwoord in paragraaf 5.1.

De resultaten van de multipele regressieanalyses worden in de gepresenteerde tabellen als volgt weergegeven, tenzij anders aangegeven [KNIP94], [VOET04]: De gedragsintentie vormt de afhankelijke criteriumvariabele. De attitude toward the behavior, subjective norm en perceived behavioral control vormen de drie onafhankelijke predictor variabelen. De waarde R is berekend middels de Pearson's correlatiecoëfficiënt en is de meervoudige correlatiecoëfficiënt. Deze waarde geeft de samenhang weer tussen de afhankelijke en de onafhankelijke variabele. R^2 of R Square is de gekwadrateerde correlatiecoëfficiënt en geeft aan welk percentage van de verklaarde variantie van de criteriumvariabele wordt verklaard door de predictor variabelen. Om het shrinkage-probleem te corrigeren geeft Adjusted R Square de mogelijke ongunstige verhouding in de populatiewaarde. R Square Change geeft aan hoeveel de betreffende predictor variabele toevoegt aan R Square. F Change geeft de F-waarde van de partiële F-toets voor de verandering in R Square, significantie F Change is aangegeven met º ($p > .05$), * ($p < .05$), ** ($p < .01$), *** ($p < .001$), gevolgd door de vrijheidsgraden van F. De partiële regressiecoëfficiënt wordt uitgedrukt met B. Dit is de geschatte waarde van de ruwe of ongestandaardiseerde regressiecoëfficiënt. Hiermee wordt de predictor gewogen en geeft deze aan dat een verandering van één eenheid in de criteriumvariabele gepaard gaat met een verandering van B eenheden in de predictor variabele. Hierbij wordt de standaardfout van B opgenomen. De gestandaardiseerde regressiecoëfficiënt in de populatie bèta (ß) is het regressiegewicht van B dat een indicatie geeft van het relatieve belang van een predictor variabele; het significantieniveau van de t-waarde voor de bèta wordt aangegeven met º ($p > .05$), * ($p < .05$), ** ($p < .01$) en *** ($p < .001$). De t-waarde geeft aan wat de unieke bijdrage van elke predictor is. Hierbij wordt de conventie dat de overschrijdingskans van een gevonden t-waarde kleiner dan alpha (α) = .05 moet zijn om de nulhypothese te kunnen verwerpen, zodat er geconcludeerd kan worden dat het gewicht statistisch significant verschilt van 0. Wanneer er sprake is van een verband tussen de criteriumvariabele en predictor variabele dat R Square = .03, wordt er gesproken over een zwak verband. Correlaties van R Square = .10 worden als matig omschreven en een correlatie van R Square = .30 wordt aanzienlijk genoemd [COHE03].

Als eerste stap van de analyse zijn alle itemscores ingelezen met behulp van het statistische pakket SPSS (Statistical Package for the Social Sciences), versie 15. Hierna zijn alle itemscores gecontroleerd op invoerfouten en waar nodig gecorrigeerd. Het kwam bijvoorbeeld een paar keer voor dat de respondent het geboortejaar in plaats van de leeftijd had ingevoerd. Verder waren *missing values*[39] onmogelijk, aangezien er alleen verplichte velden binnen de vragenlijst bestonden. Uitbijters[40] (outliers) zijn binnen dit onderzoek niet verwijderd omdat de invloed hiervan minimaal is gezien het geringe aantal uitbijters en de omvangrijke steekproef. Alvorens statistische multipele regressieanalyses uitgevoerd konden worden zijn eerst de bivariate correlaties tussen alle items onderzocht op lineariteit en homoscedasticiteit, hierbij is vanuit de puntenwolken geen reden om aan te nemen dat er sprake zou zijn van niet-lineariteit of heteroscedasticiteit. Daarnaast zijn er factoranalyses uitgevoerd op de verschillende componenten. Hierbij zijn er twee componenten toegevoegd die ingaan op *organisatorische verplichtingen* en *bewustwordingscampagnes en trainingen* voor informatiebeveiliging. Vervolgens zijn alle negatieve eindpunten gespiegeld en zijn de samengestelde indirecte variabelen van behavioral beliefs, normative beliefs, en control beliefs middels de scoring key berekend (zie Bijlage 8.10 "Scoring key"). Als laatste zijn de overige items middels de

[39] Missing values zijn specifieke variabelen waarvan geen data is opgeslagen binnen de vragenlijst.

[40] Als er een extreem hoge of lage waarde in een verdeling voorkomt, wordt dat een uitbijter (outlier) genoemd. [MOOR04]

componenten van de factoranalyses gereduceerd naar 33 samengestelde onafhankelijke predictor variabelen en 3 afhankelijke criteriumvariabelen (zie Bijlage 8.8 "Item list"). Voor de 33 samengestelde onafhankelijke predictoren zijn bivariate correlaties berekend om te onderzoeken of de directe en indirecte metingen van hetzelfde component hetzelfde meten. Hieruit is gebleken dat de directe en indirecte metingen van hetzelfde component aanzienlijk met elkaar correleren, maar dat beide metingen iets anders meten omdat ze correleren tussen de .357 en .651 (zie Bijlage 8.11 "Bivariate correlaties"). Vervolgens zijn er voor de drie hoofdonderwerpen *bedrijfsgegevens*, *back-up* en *wachtwoordgebruik* multipele regressieanalyses uitgevoerd op de directe en indirecte variabelen. Deze multipele regressieanalyses zijn onderverdeeld in twee soorten: een compacte analyse en een uitgebreide analyse. Er is gekozen voor deze twee analyses om te valideren of ze dezelfde resultaten opleveren. De compacte analyse is gebaseerd op een beperkt aantal predictor variabelen die het meest passend en waardevol zijn op de criteriumvariabelen en is op de volgende wijze uitgevoerd. Elke gedragsintentie voor de verschillende hoofdonderwerpen zijn als criteriumvariabelen opgenomen. Vervolgens zijn de attitude toward the behavior, de subjective norm en de perceived behavioral control als de onafhankelijke predictor variabelen in het eerste blok opgenomen. Hierna zijn de behavioral beliefs, de normative beliefs, en de control beliefs als de onafhankelijke predictor variabelen in het tweede blok opgenomen. Om de analyse uit te voeren is voor de *stepwise* methode gekozen, waarbij SPSS de beste predictoren kiest. SPSS beantwoordt hierbij impliciet deelvraag één tot en met drie en expliciet deelvraag vier. De uitgebreide analyse is op de volgende wijze uitgevoerd. Eerst is deelvraag één beantwoord door behavioral beliefs en attitude toward the behavior samen te nemen als predictor variabelen op de gedragsintentie als criterium variabele. Er zijn twee deelanalyses uitgevoerd middels de *stepwise* methode. In het eerste deel is de attitude toward the behavior in het eerste blok en de behavioral beliefs in het tweede blok opgenomen. In het tweede deel zijn deze variabelen vice versa in de blokken opgenomen. Hier is voor gekozen om zowel het directe als het indirecte effect apart te onderzoeken. Vervolgens is deelvraag twee beantwoord door normative beliefs en subjective norm samen te nemen als predictor variabelen op de gedragsintentie als criterium variabele. Er zijn twee deelanalyses uitgevoerd middels de *stepwise* methode. In het eerste deel is de subjective norm in het eerste blok en de normative beliefs in het tweede blok opgenomen. In het tweede deel zijn deze variabelen vice versa in de blokken opgenomen. Hierna is deelvraag drie beantwoord door control beliefs en perceived behavioral control samen te nemen als predictor variabelen op de gedragsintentie als criterium variabele. Er zijn twee deelanalyses uitgevoerd middels de *stepwise* methode. In het eerste deel is de perceived behavioral control in het eerste blok en de control beliefs in het tweede blok opgenomen. In het tweede deel zijn deze variabelen vice versa in de blokken opgenomen. Als laatste is deelvraag vier beantwoord door de variabelen met de hoogste voorspellende waarde mee te nemen in de *enter* methode. Hierbij zijn alle directe variabelen in het eerste blok en alle indirecte variabelen in het tweede blok opgenomen. Als laatste is het mediatoreffect onderzocht van de attitude toward the behavior, subjective norm, perceived behavior control. Hierbij is specifiek gekeken of er überhaupt een mediatoreffect aanwezig is en of een aanwezig mediatoreffect gedeeltelijk of volledig is.

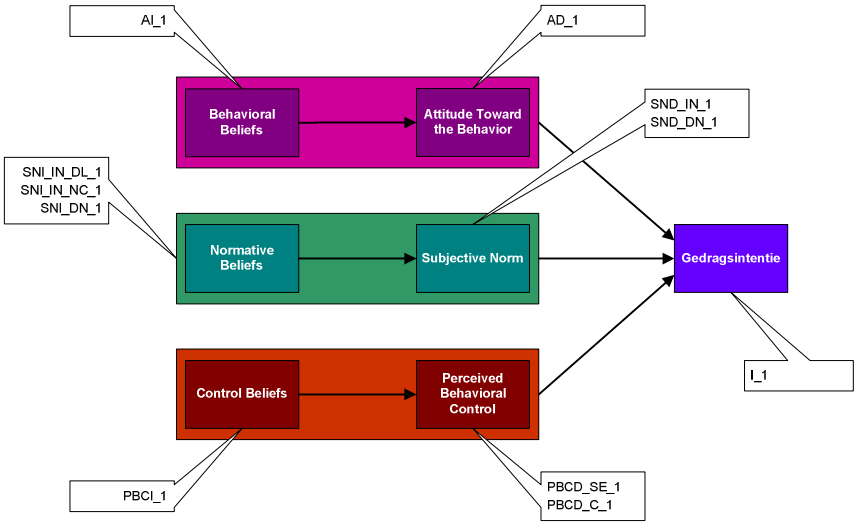
5.1 Compacte analyse & uitgebreide analyse

5.1.1 Compacte analyse

De compacte analyse is op de bovenstaande wijze uitgevoerd. Dit hoofdstuk zal opgedeeld worden in de verschillende hoofdonderwerpen: bedrijfsgegevens, back-up en wachtwoordgebruik.

Bedrijfsgegevens

De samengestelde producten die betrekking hebben op de componenten van bedrijfsgegevens zijn hieronder schematisch weergegeven.



Figuur 31: Samengestelde producten componenten bedrijfsgegevens

Het samengestelde product I_1 voor de gedragsintentie bedrijfsgegevens is ingevoerd als de afhankelijke criteriumvariabele. Vervolgens zijn de samengestelde producten AD_1, SND_IN_1, SND_DN_1, PBCD_SE_1 en PBCD_C_1 als de directe onafhankelijke predictor variabelen in het eerste blok opgenomen. Hierna zijn de samengestelde producten AI_1, SNI_IN_DL_1, SNI_IN_NC_1, SNI_DN_1 en PBCI_1 als de indirecte onafhankelijke predictor variabelen in het tweede blok opgenomen. Vervolgens is voor beide blokken de *stepwise* methode gebruikt. De resultaten van deze analyse zijn in onderstaande tabel weergegeven.

Tabel 11 "Bedrijfsgegevens"
Directe onafhankelijke predictor variabelen en indirecte onafhankelijke predictor variabelen (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,264***	,264	,324***
2[b]	,339***	,075	,194**
3[c]	,357*	,018	,158*
4[d]	,369*	,012	,130*

* (p < .05) en *** (p < .001)

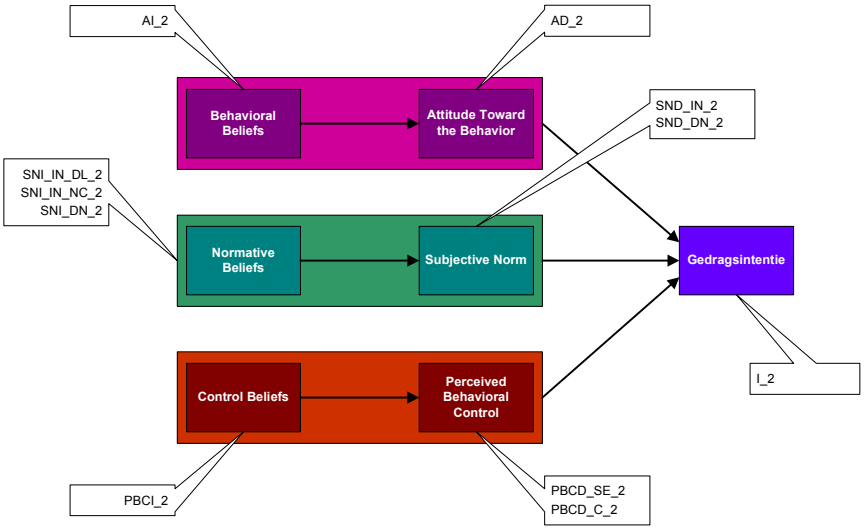
a. AD_1
b. AD_1, SND_IN_1
c. AD_1, SND_IN_1, SNI_IN_NC_1
d. AD_1, SND_IN_1, SNI_IN_NC_1, AI_1

Uit bovenstaande tabel blijkt dat de directe evaluaties of waarderingen van een medewerker om zijn bedrijfsgegevens te beschermen voor 26,4% de intentie om zijn bedrijfsgegevens te beschermen voorspelt. Wat belangrijke mensen van een medewerker vinden dat hij moet doen en wat er van een medewerker verwacht wordt ten aanzien van het beschermen van zijn bedrijfsgegevens, voegen samen een extra voorspellende waarde van 7,5% toe aan de intentie om zijn bedrijfsgegevens te beschermen. Wat naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen

ten aanzien van het beschermen van zijn bedrijfsgegevens, voegt nog eens een extra voorspellende waarde van 1,8% toe aan de intentie om zijn bedrijfsgegevens te beschermen. De indirecte evaluaties of waarderingen van een medewerker om zijn bedrijfsgegevens te beschermen voegt als laatste nog een extra voorspellende waarde van 1,2% toe aan de intentie om zijn bedrijfsgegevens te beschermen. In totaliteit voorspellen *attitude toward the behavior* en *subjective norm* voor 36,9% de intentie van een medewerker om zijn bedrijfsgegevens te beschermen. Hiermee leveren deze twee determinanten een unieke significante bijdrage om de intentie van een medewerker om zijn bedrijfsgegevens te beschermen te voorspellen. Perceived behavioral control levert geen onafhankelijke significante unieke bijdrage aan deze voorspelling.

Back-up

De samengestelde producten die betrekking hebben op de componenten van back-up zijn hieronder schematisch weergegeven.



Figuur 32: Samengestelde producten componenten back-up

Het samengestelde product I_2 voor de gedragsintentie back-up is ingevoerd als de afhankelijke criteriumvariabele. Vervolgens zijn de samengestelde producten AD_2, SND_IN_2, SND_DN_2, PBCD_SE_2 en PBCD_C_2 als de directe onafhankelijke predictor variabelen in het eerste blok opgenomen. Hierna zijn de samengestelde producten AI_2, SNI_IN_DL_2, SNI_IN_NC_2, SNI_DN_2 en PBCI_2 als de indirecte onafhankelijke predictor variabelen in het tweede blok opgenomen. Vervolgens is voor beide blokken de *stepwise* methode gebruikt. De resultaten van deze analyse zijn in onderstaande tabel weergegeven.

Tabel 12 "Back-up"

Directe onafhankelijke predictor variabelen en indirecte onafhankelijke predictor variabelen (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,258***	,258	,190**
2[b]	,344***	,086	,155*
3[c]	,373**	,030	,195**
4[d]	,397**	,024	,191**
5[e]	,418**	,021	,179**

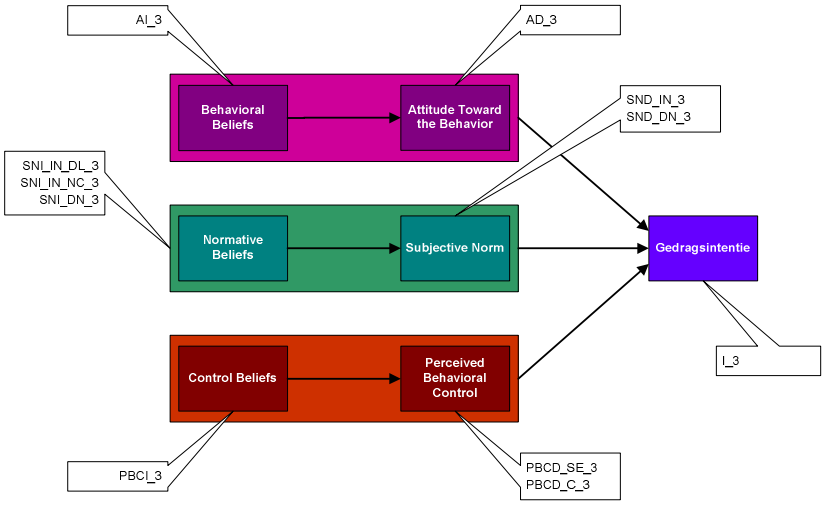
* ($p < .05$), ** ($p < .01$) en *** ($p < .001$)

a. SND_IN_2
b. SND_IN_2, PBCD_SE_2
c. SND_IN_2, PBCD_SE_2, AD_2
d. SND_IN_2, PBCD_SE_2, AD_2, PBCD_C_2
e. SND_IN_2, PBCD_SE_2, AD_2, PBCD_C_2, SNI_IN_NC_2

Uit bovenstaande tabel blijkt dat wat belangrijke mensen van een medewerker vinden dat hij moet doen en wat er van een medewerker verwacht wordt ten aanzien van het zekerstellen van zijn bedrijfsgegevens voor 25,8% de intentie om zijn bedrijfsgegevens zeker te stellen voorspelt. De capaciteit van een medewerker om zijn bedrijfsgegevens zeker te stellen, voegt een extra voorspellende waarde van 8,6% toe aan de intentie om zijn bedrijfsgegevens zeker te stellen. De indirecte evaluaties of waarderingen van een medewerker om zijn bedrijfsgegevens zeker te stellen voegt nog eens een extra voorspellende waarde van 3,0% toe aan de intentie om zijn bedrijfsgegevens zeker te stellen. De controle van een medewerker om zijn bedrijfsgegevens zeker te stellen, voegt nog eens een extra voorspellende waarde van 2,4% toe aan de intentie om zijn bedrijfsgegevens zeker te stellen. Wat naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen ten aanzien van het zekerstellen van zijn bedrijfsgegevens, voegt als laatste nog een extra voorspellende waarde van 2,1% toe aan de intentie om zijn bedrijfsgegevens zeker te stellen. In totaliteit voorspellen *attitude toward the behavior*, *subjective norm* en *perceived behavioral control* voor 41,8% de intentie van een medewerker om zijn bedrijfsgegevens zeker te stellen. Hiermee leveren deze drie determinanten een unieke significante bijdrage om de intentie van een medewerker om zijn bedrijfsgegevens zeker te stellen te voorspellen.

Wachtwoordgebruik

De samengestelde producten die betrekking hebben op de componenten van wachtwoordgebruik zijn hieronder schematisch weergegeven.



Figuur 33: Samengestelde producten componenten wachtwoordgebruik

Het samengestelde product I_3 voor de gedragsintentie wachtwoordgebruik is ingevoerd als de afhankelijke criteriumvariabele. Vervolgens zijn de samengestelde producten AD_3, SND_IN_3, SND_DN_3, PBCD_SE_3 en PBCD_C_3 als de directe onafhankelijke predictor variabelen in het eerste blok opgenomen. Hierna zijn de samengestelde producten AI_3, SNI_IN_DL_3, SNI_IN_NC_3, SNI_DN_3 en PBCI_3 als de indirecte onafhankelijke predictor variabelen in het tweede blok opgenomen. Vervolgens is voor beide blokken de *stepwise* methode gebruikt. De resultaten van deze analyse zijn in onderstaande tabel weergegeven.

Tabel 13 "Wachtwoordgebruik"
Directe onafhankelijke predictor variabelen en indirecte onafhankelijke predictor variabelen (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,297***	,297	,414***
2[b]	,325**	,027	,124*
3[c]	,366***	,042	,228***

* (p < .05), ** (p < .01) en *** (p < .001)

a. AD_3
b. AD_3, SND_IN_3
c. AD_3, SND_IN_3, AI_3

Uit bovenstaande tabel blijkt dat de directe evaluaties of waarderingen van een medewerker om veilig om te gaan met zijn wachtwoord voor 29,7% de intentie om veilig om te gaan met zijn wachtwoord voorspelt. Wat belangrijke mensen van een medewerker vinden dat hij moet doen en wat er van een medewerker verwacht wordt ten aanzien van het veilig omgaan met zijn wachtwoord, voegen samen een extra voorspellende waarde van 2,7% toe aan de intentie om veilig om te gaan met zijn wachtwoord. De indirecte evaluaties of waarderingen van een medewerker om veilig om te gaan met zijn wachtwoord voegt als laatste nog een extra voorspellende waarde van 4,2% toe aan de intentie om veilig om te gaan met zijn wachtwoord. In totaliteit voorspellen *attitude toward the behavior* en *subjective norm* voor 36,6% de intentie van een medewerker om veilig om te gaan met zijn

wachtwoord. Hiermee leveren deze twee determinanten een unieke significante bijdrage om de intentie van een medewerker om veilig om te gaan met zijn wachtwoord te voorspellen. Perceived behavioral control levert geen onafhankelijke significante unieke bijdrage aan deze voorspelling.

5.1.2 Uitgebreide analyse

De uitgebreide analyse is op de wijze uitgevoerd zoals die in de inleiding beschreven is. Dit hoofdstuk is opgedeeld volgens de vier deelvragen. De deelvragen zijn toegespitst op het hoofdonderwerp bedrijfsgegevens waarbij de gedragsintentie ten aanzien van informatiebeveiliging als volgt geoperationaliseerd is: ***B***(eschikbaarheid) ***I***(ntegriteit) ***V***(ertrouwelijkheid) van bedrijfsgegevens, back-up en wachtwoordgebruik.

5.1.2.1 Attitude toward the behavior en de gedragsintentie

Binnen dit hoofdstuk wordt de volgende deelvraag beantwoord: Wat is de voorspellende waarde van attitude toward the behavior ten opzichte van de gedragsintentie ten aanzien van informatiebeveiliging?

Deze deelvraag is beantwoord door behavioral beliefs en attitude toward the behavior samen te nemen als predictor variabelen op de gedragsintenties om bedrijfsgegevens te beschermen, bedrijfsgegevens zeker te stellen en veilig om te gaan met wachtwoordgebruik als criterium variabelen. Er zijn twee deelanalyses uitgevoerd middels de enter methode voor alle drie de hoofdonderwerpen apart. In de eerste deelanalyse is de attitude toward the behavior in het eerste blok en de behavioral beliefs in het tweede blok opgenomen. In de tweede deelanalyse zijn deze variabelen vice versa in de blokken opgenomen. De resultaten voor het hoofdonderwerp bedrijfsgegevens zijn in onderstaande tabel weergegeven.

Tabel 14 "Bedrijfsgegevens"
Attitude toward the behavior en behavioral beliefs (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,264***	,264	,513***
2[b]	,293**	,029	,419*** ,196**
3[c]	,159***	,159	,399***
4[d]	,293***	,134	,196** ,419***

** ($p < .01$) en *** ($p < .001$)

a. AD_1
b. AD_1, AI_1
c. AI_1
d. AI_1, AD_1

Uit bovenstaande tabel blijkt dat de directe evaluaties of waarderingen van een medewerker om zijn bedrijfsgegevens te beschermen voor 26,4% de intentie om zijn bedrijfsgegevens te beschermen voorspelt. De indirecte evaluaties of waarderingen van een medewerker om zijn bedrijfsgegevens te beschermen voorspellen voor 15,9% de intentie om zijn bedrijfsgegevens te beschermen. In totaliteit voorspellen *attitude toward the behavior* en *behavioral beliefs* voor 29,3% de intentie van een medewerker om zijn bedrijfsgegevens te beschermen. Hiermee leveren deze twee predictor variabelen voor alle

modellen een unieke significante bijdrage om deze gedragsintentie als criterium variabele te voorspellen.

De resultaten voor het hoofdonderwerp back-up zijn in onderstaande tabel weergegeven.

Tabel 15 "Back-up"
Attitude toward the behavior en behavioral beliefs (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,223***	,223	,472***
2[b]	,230º	,007	,432*** ,095º
3[c]	,077***	,077	,277***
4[d]	,230***	,153	,095º ,432***

º ($p > .05$) en *** ($p < .001$)

a. AD_2
b. AD_2, AI_2
c. AI_2
d. AI_2, AD_2

Uit bovenstaande tabel blijkt dat de directe evaluaties of waarderingen van een medewerker om zijn bedrijfsgegevens zeker te stellen voor 22,3% de intentie om zijn bedrijfsgegevens zeker te stellen voorspelt. De indirecte evaluaties of waarderingen van een medewerker om zijn bedrijfsgegevens zeker te stellen voorspellen voor 7,7% de intentie om zijn bedrijfsgegevens zeker te stellen. In totaliteit voorspellen *attitude toward the behavior* en *behavioral beliefs* voor 23,0% de intentie van een medewerker om zijn bedrijfsgegevens zeker te stellen. Hiermee leveren deze twee predictor variabelen voor model één, drie en vier een unieke significante bijdrage en voor model twee geen unieke significante bijdrage om deze gedragsintentie als criterium variabele te voorspellen.

De resultaten voor het hoofdonderwerp wachtwoordgebruik zijn in onderstaande tabel weergegeven.

Tabel 16 "Wachtwoordgebruik"
Attitude toward the behavior en behavioral beliefs (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,297***	,297	,545***
2[b]	,353***	,056	,444*** ,258***
3[c]	,187***	,187	,432***
4[d]	,353***	,167	,258*** ,444***

*** ($p < .001$)

a. AD_3
b. AD_3, AI_3
c. AI_3
d. AI_3, AD_3

Uit bovenstaande tabel blijkt dat de directe evaluaties of waarderingen van een medewerker om veilig om te gaan met zijn wachtwoord voor 29,7% de intentie om veilig om te gaan met zijn

wachtwoord voorspelt. De indirecte evaluaties of waarderingen van een medewerker om veilig om te gaan met zijn wachtwoord voorspellen voor 18,7% de intentie om veilig om te gaan met zijn wachtwoord. In totaliteit voorspellen *attitude toward the behavior* en *behavioral beliefs* voor 35,3% de intentie van een medewerker om veilig om te gaan met zijn wachtwoord. Hiermee leveren deze twee predictor variabelen voor alle modellen een unieke significante bijdrage om deze gedragsintentie als criterium variabele te voorspellen.

Uit de tabellen en beschreven resultaten kunnen verschillende conclusies getrokken worden die betrekking hebben op de eerste deelvraag. Deze conclusies zijn in onderstaande opsomming weergegeven:

- Naarmate een medewerker het verstandiger, nuttiger voor zichzelf en nuttiger voor anderen vindt om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoordgebruik, zullen ook de intenties om dit te doen toenemen.
- Naarmate een medewerker het prettiger vindt om zijn bedrijfsgegevens te beschermen, zal ook de intentie om dit te doen toenemen.
- De moeilijkheidsgraad voor een medewerker om zijn bedrijfsgegevens te beschermen heeft geen invloed op de intentie om dit te doen.
- De pleziergraad en de moeilijkheidsgraad voor een medewerker om zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoord hebben geen invloed op de intenties om dit te doen.
- De attitude toward the behavior ten aanzien van de drie gedragsintenties is een sterkere verklarende voorspeller dan de behavioral beliefs ten aanzien van de drie gedragsintenties. Dit wil zeggen dat de directe evaluatie van een medewerker (directe meting), een grotere invloed heeft op de intentie om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoord, dan de evaluatie van de consequenties voor een medewerker (indirecte meting).

5.1.2.2 Subjective norm en de gedragsintentie

Binnen dit hoofdstuk wordt de volgende deelvraag beantwoord: wat is de voorspellende waarde van subjective norm ten opzichte van de gedragsintentie ten aanzien van informatiebeveiliging?

Deze deelvraag is beantwoord door normative beliefs en subjective norm samen te nemen als predictor variabelen op de gedragsintenties om bedrijfsgegevens te beschermen, bedrijfsgegevens zeker te stellen en veilig om te gaan met wachtwoordgebruik als criterium variabelen. Er zijn twee deelanalyses uitgevoerd middels de enter methode. In de eerste deelanalyse is de subjective norm in het eerste blok en de normative beliefs in het tweede blok opgenomen. In de tweede deelanalyse zijn deze variabelen vice versa in de blokken opgenomen. De resultaten voor het hoofdonderwerp bedrijfsgegevens zijn in onderstaande tabel weergegeven.

Tabel 17 "Bedrijfsgegevens"
Subjective norm en normative beliefs (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,209***	,209	,457***
2[b]	,213º	,004	,417*** ,077º
3[c]	,085***	,085	,292***
4[d]	,213***	,128	,077º ,417***

º (p > .05) en *** (p < .001)

a. SND_IN_1
b. SND_IN_1, SNI_IN_DL_1
c. SNI_IN_DL_1
d. SNI_IN_DL_1, SND_IN_1

Uit bovenstaande tabel blijkt dat wat belangrijke mensen van een medewerker vinden dat hij moet doen en wat er van een medewerker verwacht wordt ten aanzien van het beschermen van zijn bedrijfsgegevens, samen een voorspellende waarde van 20,9% hebben op de intentie om zijn bedrijfsgegevens te beschermen. Wat een direct leidinggevende van een medewerker vindt dat hij moet doen ten aanzien van het beschermen van zijn bedrijfsgegevens, heeft een voorspellende waarde van 8,5% op de intentie om zijn bedrijfsgegevens te beschermen. In totaliteit voorspellen *subjective norm* en *normative beliefs* voor 21,3% de intentie van een medewerker om zijn bedrijfsgegevens te beschermen. Hiermee leveren deze twee predictor variabelen voor model één, drie en vier een unieke significante bijdrage en voor model twee geen unieke significante bijdrage om deze gedragsintentie als criterium variabele te voorspellen.

Tabel 18 "Bedrijfsgegevens"
Subjective norm en normative beliefs (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,209***	,209	,457***
2[b]	,240**	,031	,343*** ,211**
3[c]	,157***	,157	,396***
4[d]	,240***	,083	,211** ,343***

** (p < .01) en *** (p < .001)

a. SND_IN_1
b. SND_IN_1, SNI_IN_NC_1
c. SNI_IN_NC_1
d. SNI_IN_NC_1, SND_IN_1

Uit bovenstaande tabel blijkt dat wat belangrijke mensen van een medewerker vinden dat hij moet doen en wat er van een medewerker verwacht wordt ten aanzien van het beschermen van zijn bedrijfsgegevens, samen een voorspellende waarde van 20,9% hebben op de intentie om zijn bedrijfsgegevens te beschermen. Wat naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen ten aanzien van het beschermen van zijn bedrijfsgegevens, heeft een voorspellende waarde van 15,7% op de intentie om zijn bedrijfsgegevens te beschermen. In totaliteit voorspellen *subjective norm* en *normative beliefs* voor 24,0% de intentie van een medewerker om zijn

bedrijfsgegevens te beschermen. Hiermee leveren deze twee predictor variabelen voor alle modellen een unieke significante bijdrage om deze gedragsintentie als criterium variabele te voorspellen.

Tabel 19 "Bedrijfsgegevens"
Subjective norm en normative beliefs (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,048**	,048	,219**
2[b]	,123***	,075	,096º ,300***
3[c]	,115***	,115	,339***
4[d]	,123º	,008	,300*** ,096º

º (p > .05), ** (p < .01) en *** (p < .001)

a. SND_DN_1
b. SND_DN_1, SNI_DN_1
c. SNI_DN_1
d. SNI_DN_1, SND_DN_1

Uit bovenstaande tabel blijkt dat wat belangrijke mensen van een medewerker zelf doen ten aanzien van het beschermen van hun bedrijfsgegevens, een voorspellende waarde van 4,8% heeft op de intentie om zijn bedrijfsgegevens te beschermen. Wat naaste collega's, die belangrijk voor een medewerker zijn, zelf doen ten aanzien van het beschermen van hun bedrijfsgegevens, heeft een voorspellende waarde van 11,5% op de intentie om zijn bedrijfsgegevens te beschermen. In totaliteit voorspellen *subjective norm* en *normative beliefs* voor 12,3% de intentie van een medewerker om zijn bedrijfsgegevens te beschermen. Hiermee leveren deze twee predictor variabelen voor model één, twee en drie een unieke significante bijdrage en voor model vier geen unieke significante bijdrage om deze gedragsintentie als criterium variabele te voorspellen.

De resultaten voor het hoofdonderwerp back-up zijn in onderstaande tabel weergegeven.

Tabel 20 "Back-up"
Subjective norm en normative beliefs (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,258***	,258	,508***
2[b]	,277*	,019	,420*** ,163*
3[c]	,152***	,152	,389***
4[d]	,277***	,125	,163* ,420***

* (p < .05) en *** (p < .001)

a. SND_IN_2
b. SND_IN_2, SNI_IN_DL_2
c. SNI_IN_DL_2
d. SNI_IN_DL_2, SND_IN_2

Uit bovenstaande tabel blijkt dat wat belangrijke mensen van een medewerker vinden dat hij moet doen en wat er van een medewerker verwacht wordt ten aanzien van het zekerstellen van zijn bedrijfsgegevens, samen een voorspellende waarde van 25,8% hebben op de intentie om zijn bedrijfsgegevens zeker te stellen. Wat een direct leidinggevende van een medewerker vindt dat hij

moet doen ten aanzien van het zekerstellen van zijn bedrijfsgegevens, heeft een voorspellende waarde van 15,2% op de intentie om zijn bedrijfsgegevens zeker te stellen. In totaliteit voorspellen *subjective norm* en *normative beliefs* voor 27,7% de intentie van een medewerker om zijn bedrijfsgegevens zeker te stellen. Hiermee leveren deze twee predictor variabelen voor alle modellen een unieke significante bijdrage om deze gedragsintentie als criterium variabele te voorspellen.

Tabel 21 "Back-up"
Subjective norm en normative beliefs (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,258***	,258	,508***
2[b]	,290**	,032	,384*** ,218**
3[c]	,190***	,190	,436***
4[d]	,290***	,100	,218** ,384***

** (p < .01) en *** (p < .001)

a. SND_IN_2
b. SND_IN_2, SNI_IN_NC_2
c. SNI_IN_NC_2
d. SNI_IN_NC_2, SND_IN_2

Uit bovenstaande tabel blijkt dat wat belangrijke mensen van een medewerker vinden dat hij moet doen en wat er van een medewerker verwacht wordt ten aanzien van het zekerstellen van zijn bedrijfsgegevens, samen een voorspellende waarde van 25,8% hebben op de intentie om zijn bedrijfsgegevens zeker te stellen. Wat naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen ten aanzien van het zekerstellen van zijn bedrijfsgegevens, heeft een voorspellende waarde van 19,0% op de intentie om zijn bedrijfsgegevens zeker te stellen. In totaliteit voorspellen *subjective norm* en *normative beliefs* voor 29,0% de intentie van een medewerker om zijn bedrijfsgegevens zeker te stellen. Hiermee leveren deze twee predictor variabelen voor alle modellen een unieke significante bijdrage om deze gedragsintentie als criterium variabele te voorspellen.

Tabel 22 "Back-up"
Subjective norm en normative beliefs (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,055**	,055	,234**
2[b]	,133***	,078	,107º ,308***
3[c]	,124***	,124	,352***
4[d]	,133º	,009	,308*** ,107º

º (p > .05), ** (p < .01) en *** (p < .001)

a. SND_DN_2
b. SND_DN_2, SNI_DN_2
c. SNI_DN_2
d. SNI_DN_2, SND_DN_2

Uit bovenstaande tabel blijkt dat wat belangrijke mensen van een medewerker zelf doen ten aanzien van het zekerstellen van hun bedrijfsgegevens, een voorspellende waarde van 5,5% heeft op de intentie om zijn bedrijfsgegevens zeker te stellen. Wat naaste collega's, die belangrijk voor een

medewerker zijn, zelf doen ten aanzien van het zekerstellen van hun bedrijfsgegevens, heeft een voorspellende waarde van 12,4% op de intentie om zijn bedrijfsgegevens zeker te stellen. In totaliteit voorspellen *subjective norm* en *normative beliefs* voor 13,3% de intentie van een medewerker om zijn bedrijfsgegevens zeker te stellen. Hiermee leveren deze twee predictor variabelen voor model één, twee en drie een unieke significante bijdrage en voor model vier geen unieke significante bijdrage om deze gedragsintentie als criterium variabele te voorspellen.

De resultaten voor het hoofdonderwerp wachtwoordgebruik zijn in onderstaande tabel weergegeven.

Tabel 23 "Wachtwoordgebruik"
Subjective norm en normative beliefs (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,115***	,115	,339***
2[b]	,115º	,000	,351*** -,021º
3[c]	,029*	,029	,169*
4[d]	,115***	,087	-,021º ,351***

º ($p > .05$), * ($p < .05$) en *** ($p < .001$)

a. SND_IN_3
b. SND_IN_3, SNI_IN_DL_3
c. SNI_IN_DL_3
d. SNI_IN_DL_3, SND_IN_3

Uit bovenstaande tabel blijkt dat wat belangrijke mensen van een medewerker vinden dat hij moet doen en wat er van een medewerker verwacht wordt ten aanzien van het veilig omgaan met zijn wachtwoord, samen een voorspellende waarde van 11,5% hebben op de intentie om veilig om te gaan met zijn wachtwoord. Wat een direct leidinggevende van een medewerker vindt dat hij moet doen ten aanzien van het veilig omgaan met zijn wachtwoord, heeft een voorspellende waarde van 2,9% op de intentie om veilig om te gaan met zijn wachtwoord. In totaliteit voorspellen *subjective norm* en *normative beliefs* voor 11,5% de intentie van een medewerker om veilig met zijn wachtwoord om te gaan. Hiermee leveren deze twee predictor variabelen voor model één, drie en vier een unieke significante bijdrage en voor model twee geen unieke significante bijdrage om deze gedragsintentie als criterium variabele te voorspellen.

Tabel 24 "Wachtwoordgebruik"
Subjective norm en normative beliefs (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,115***	,115	,339***
2[b]	,117º	,002	,305*** ,058º
3[c]	,057***	,057	,240***
4[d]	,117***	,060	,058º ,305***

º (p > .05) en *** (p < .001)

a. SND_IN_3
b. SND_IN_3, SNI_IN_NC_3
c. SNI_IN_NC_3
d. SNI_IN_NC_3, SND_IN_3

Uit bovenstaande tabel blijkt dat wat belangrijke mensen van een medewerker vinden dat hij moet doen en wat er van een medewerker verwacht wordt ten aanzien van het veilig omgaan met zijn wachtwoord, samen een voorspellende waarde van 11,5% hebben op de intentie om veilig om te gaan met zijn wachtwoord. Wat naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen ten aanzien van het veilig omgaan met zijn wachtwoord, heeft een voorspellende waarde van 5,7% op de intentie om veilig om te gaan met zijn wachtwoord. In totaliteit voorspellen *subjective norm* en *normative beliefs* voor 11,7% de intentie van een medewerker om veilig om te gaan met zijn wachtwoord. Hiermee leveren deze twee predictor variabelen voor model één, drie en vier een unieke significante bijdrage en voor model twee geen unieke significante bijdrage om deze gedragsintentie als criterium variabele te voorspellen.

Tabel 25 "Wachtwoordgebruik"
Subjective norm en normative beliefs (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,021*	,021	,144*
2[b]	,064**	,043	,052º ,228**
3[c]	,062***	,062	,249***
4[d]	,064º	,002	,228** ,052º

º (p > .05), * (p < .05), ** (p < .01) en *** (p < .001)

a. SND_DN_3
b. SND_DN_3, SNI_DN_3
c. SNI_DN_3
d. SNI_DN_3, SND_DN_3

Uit bovenstaande tabel blijkt dat wat belangrijke mensen van een medewerker zelf doen ten aanzien van het veilig omgaan met hun wachtwoord, een voorspellende waarde van 2,1% heeft op de intentie om veilig om te gaan met zijn wachtwoord. Wat naaste collega's, die belangrijk voor een medewerker zijn, zelf doen ten aanzien van het veilig omgaan met hun wachtwoord, heeft een voorspellende waarde van 6,2% op de intentie om veilig om te gaan met zijn wachtwoord. In totaliteit voorspellen *subjective norm* en *normative beliefs* voor 6,4% de intentie van een medewerker om veilig om te gaan met zijn wachtwoord. Hiermee leveren deze twee predictor variabelen voor model

één, twee en drie een unieke significante bijdrage en voor model vier geen unieke significante bijdrage om deze gedragsintentie als criterium variabele te voorspellen.

Uit de tabellen en beschreven resultaten kunnen verschillende conclusies getrokken worden die betrekking hebben op de tweede deelvraag. Deze conclusies zijn in onderstaande opsomming weergegeven:

- Wat belangrijke mensen van een medewerker vinden dat hij moet doen en wat er van een medewerker verwacht wordt ten aanzien van alle drie de gedragsintenties, is de sterkst verklarende voorspeller vanuit de subjective norm ten aanzien van alle drie de gedragsintenties. Dit wil zeggen dat wat belangrijke mensen van een medewerker vinden dat hij moet doen en wat er van een medewerker verwacht wordt, de meeste invloed heeft op de intentie om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoord. Naarmate de invloed van wat belangrijke mensen van een medewerker vinden dat hij moet doen en wat er van een medewerker verwacht wordt toeneemt om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoordgebruik, zullen ook de intenties om dit te doen toenemen.
- Wat naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen ten aanzien van alle drie de gedragsintenties, is een sterkere verklarende voorspeller, dan wat een direct leidinggevende van een medewerker vindt dat hij moet doen ten aanzien van alle drie de gedragsintenties. Dit wil zeggen dat wat naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen een grotere invloed heeft op de intentie om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoord, dan wat een direct leidinggevende van een medewerker vindt dat hij moet doen. Naarmate de invloed van wat naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen toeneemt om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoordgebruik, zullen ook de intenties om dit te doen groter zijn dan de invloed van wat een direct leidinggevende van een medewerker vindt dat hij moet doen.
- Wat naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen ten aanzien van alle drie de gedragsintenties, is een sterkere verklarende voorspeller, dan wat naaste collega's, die belangrijk voor een medewerker zijn, zelf doen ten aanzien van alle drie de gedragsintenties. Dit wil zeggen dat wat naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen, een grotere invloed heeft op de intentie om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoord, dan wat naaste collega's, die belangrijk voor een medewerker zijn, zelf doen. Naarmate de invloed van wat naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen toeneemt om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoordgebruik, zullen ook de intenties om dit te doen groter zijn dan de invloed van wat naaste collega's, die belangrijk voor een medewerker zijn, zelf doen.
- Wat belangrijke mensen van een medewerker zelf doen ten aanzien van alle drie de gedragsintenties, is de zwakst verklarende voorspeller voor alle drie de gedragsintenties. Dit wil zeggen dat wat belangrijke mensen van een medewerker zelf doen, de minste invloed heeft op de intentie om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoord. Naarmate de invloed van wat belangrijke mensen van een medewerker zelf doen toeneemt om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoordgebruik, zullen de intenties om dit te doen *minimaal* toenemen.

- Wat belangrijke mensen van een medewerker vinden dat hij moet doen en wat er van een medewerker verwacht wordt ten aanzien van alle drie de gedragsintenties, is een sterkere verklarende voorspeller dan wat direct leidinggevende(n?) en naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen ten aanzien van alle drie de gedragsintenties. Dit wil zeggen dat wat belangrijke mensen van een medewerker vinden dat hij moet doen en wat er van een medewerker verwacht wordt, een grotere invloed heeft op de intentie om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoord, dan wat direct leidinggevende en naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen. Naarmate de invloed van wat belangrijke mensen van een medewerker vinden dat hij moet doen en wat er van een medewerker verwacht wordt toeneemt om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoordgebruik, zullen ook de intenties om dit te doen groter zijn dan de invloed van wat direct leidinggevende en naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen.
- Wat naaste collega's, die belangrijk voor een medewerker zijn, zelf doen ten aanzien van alle drie de gedragsintenties, is een sterkere verklarende voorspeller dan wat belangrijke mensen van een medewerker zelf doen ten aanzien van alle drie de gedragsintenties. Dit wil zeggen dat wat naaste collega's, die belangrijk voor een medewerker zijn, zelf doen, een grotere invloed heeft op de intentie om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoord, dan wat belangrijke mensen van een medewerker zelf doen. Naarmate de invloed van wat naaste collega's, die belangrijk voor een medewerker zijn, zelf doen toeneemt om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoordgebruik, zullen ook de intenties om dit te doen groter zijn dan de invloed van wat belangrijke mensen van een medewerker zelf doen.

5.1.2.3 Perceived behavioral control en de gedragsintentie

Binnen dit hoofdstuk wordt de volgende deelvraag beantwoord: wat is de voorspellende waarde van perceived behavioral control ten opzichte van de gedragsintentie ten aanzien van informatiebeveiliging?

Deze deelvraag is beantwoord door control beliefs en perceived behavioral control samen te nemen als predictor variabelen op de gedragsintentie om bedrijfsgegevens te beschermen, bedrijfsgegevens zeker te stellen en veilig om te gaan met wachtwoordgebruik als criterium variabelen. Er zijn twee deelanalyses uitgevoerd middels de enter methode. In de eerste deelanalyse is de perceived behavioral control in het eerste blok en de control beliefs in het tweede blok opgenomen. In de tweede deelanalyse zijn deze variabelen vice versa in de blokken opgenomen. De resultaten voor het hoofdonderwerp bedrijfsgegevens zijn in onderstaande tabel weergegeven.

Tabel 26 "Bedrijfsgegevens"
Perceived behavioral control en control beliefs (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,066***	,066	,257***
2[b]	,068º	,001	,231** ,045º
3[c]	,032**	,032	,180**
4[d]	,068**	,035	,045º ,231**

º (p > .05), ** (p < .01) en *** (p < .001)

a. PBCD_SE_1
b. PBCD_SE_1, PBCI_1
c. PBCI_1
d. PBCI_1, PBCD_SE_1

Uit bovenstaande tabel blijkt dat de capaciteit van een medewerker om zijn bedrijfsgegevens te beschermen, een voorspellende waarde van 6,6% heeft op de intentie om zijn bedrijfsgegevens te beschermen. Wat een medewerker zelf denkt dat hij kan doen ten aanzien van het beschermen van zijn bedrijfsgegevens, heeft een voorspellende waarde van 3,2% op de intentie om zijn bedrijfsgegevens te beschermen. In totaliteit voorspellen *perceived behavioral control* en *control beliefs* voor 6,8% de intentie van een medewerker om zijn bedrijfsgegevens te beschermen. Hiermee leveren deze twee predictor variabelen voor model één, drie en vier een unieke significante bijdrage en voor model twee geen unieke significante bijdrage om deze gedragsintentie als criterium variabele te voorspellen.

Tabel 27 "Bedrijfsgegevens"
Perceived behavioral control en control beliefs (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,018º	,018	,132º
2[b]	,038*	,020	,077º ,152*
3[c]	,032**	,032	,180**
4[d]	,038º	,005	,152* ,077º

º (p > .05), * (p < .05) en ** (p < .01)

a. PBCD_C_1
b. PBCD_C_1, PBCI_1
c. PBCI_1
d. PBCI_1, PBCD_C_1

Uit bovenstaande tabel blijkt dat de controle van een medewerker om zijn bedrijfsgegevens te beschermen, een voorspellende waarde van 1,8% heeft op de intentie om zijn bedrijfsgegevens te beschermen. Wat een medewerker zelf denkt dat hij kan doen ten aanzien van het beschermen van zijn bedrijfsgegevens, heeft een voorspellende waarde van 3,2% op de intentie om zijn bedrijfsgegevens te beschermen. In totaliteit voorspellen *perceived behavioral control* en *control beliefs* voor 3,8% de intentie van een medewerker om zijn bedrijfsgegevens te beschermen. Hiermee leveren deze twee predictor variabelen voor model twee en drie een unieke significante bijdrage en voor model één en vier geen unieke significante bijdrage om deze gedragsintentie als criterium variabele te voorspellen.

De resultaten voor het hoofdonderwerp back-up zijn in onderstaande tabel weergegeven.

Tabel 28 "Back-up"
Perceived behavioral control en control beliefs (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,222***	,222	,472***
2[b]	,255**	,033	,317*** ,238**
3[c]	,197***	,197	,444***
4[d]	,255***	,058	,238** ,317***

** (p < .01) en *** (p < .001)

a. PBCD_SE_2
b. PBCD_SE_2, PBCI_2
c. PBCI_2
d. PBCI_2, PBCD_SE_2

Uit bovenstaande tabel blijkt dat de capaciteit van een medewerker om zijn bedrijfsgegevens zeker te stellen, een voorspellende waarde van 22,2% heeft op de intentie om zijn bedrijfsgegevens zeker te stellen. Wat een medewerker zelf denkt dat hij kan doen ten aanzien van het zekerstellen van zijn bedrijfsgegevens, heeft een voorspellende waarde van 19,7% op de intentie om zijn bedrijfsgegevens zeker te stellen. In totaliteit voorspellen *perceived behavioral control* en *control beliefs* voor 25,5% de intentie van een medewerker om zijn bedrijfsgegevens zeker te stellen. Hiermee leveren deze twee predictor variabelen voor alle modellen een unieke significante bijdrage om deze gedragsintentie als criterium variabele te voorspellen.

Tabel 29 "Back-up"
Perceived behavioral control en control beliefs (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,169***	,169	,411***
2[b]	,249***	,080	,258*** ,322***
3[c]	,197***	,197	,444***
4[d]	,249***	,052	,322*** ,258***

*** (p < .001)

a. PBCD_C_2
b. PBCD_C_2, PBCI_2
c. PBCI_2
d. PBCI_2, PBCD_C_2

Uit bovenstaande tabel blijkt dat de controle van een medewerker om zijn bedrijfsgegevens zeker te stellen, een voorspellende waarde van 16,9% heeft op de intentie om zijn bedrijfsgegevens zeker te stellen. Wat een medewerker zelf denkt dat hij kan doen ten aanzien van het zekerstellen van zijn bedrijfsgegevens, heeft een voorspellende waarde van 19,7% op de intentie om zijn bedrijfsgegevens zeker te stellen. In totaliteit voorspellen *perceived behavioral control* en *control beliefs* voor 24,9% de intentie van een medewerker om zijn bedrijfsgegevens zeker te stellen. Hiermee leveren deze twee predictor variabelen voor alle modellen een unieke significante bijdrage om deze gedragsintentie als criterium variabele te voorspellen.

De resultaten voor het hoofdonderwerp wachtwoordgebruik zijn in onderstaande tabel weergegeven.

Tabel 30 "Wachtwoordgebruik"
Perceived behavioral control en control beliefs (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,163***	,163	,404***
2[b]	,192**	,029	,258** ,224**
3[c]	,153***	,153	,392***
4[d]	,192**	,039	,224** ,258**

** (p < .01) en *** (p < .001)

a. PBCD_SE_3
b. PBCD_SE_3, PBCI_3
c. PBCI_3
d. PBCI_3, PBCD_SE_3

Uit bovenstaande tabel blijkt dat de capaciteit van een medewerker om veilig om te gaan met zijn wachtwoord, een voorspellende waarde van 16,3% heeft op de intentie om veilig om te gaan met zijn wachtwoord. Wat een medewerker zelf denkt dat hij kan doen ten aanzien van het veilig omgaan met zijn wachtwoord, heeft een voorspellende waarde van 15,3% op de intentie om veilig om te gaan met zijn wachtwoord. In totaliteit voorspellen *perceived behavioral control* en *control beliefs* voor 19,2% de intentie van een medewerker om veilig om te gaan met zijn wachtwoord. Hiermee leveren deze twee predictor variabelen voor alle modellen een unieke significante bijdrage om deze gedragsintentie als criterium variabele te voorspellen.

Tabel 31 "Wachtwoordgebruik"
Perceived behavioral control en control beliefs (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,037**	,037	,192**
2[b]	,156***	,120	,060º ,370***
3[c]	,153***	,153	,392***
4[d]	,156º	,003	,370*** ,060º

º (p > .05), ** (p < .01) en *** (p < .001)

a. PBCD_C_3
b. PBCD_C_3, PBCI_3
c. PBCI_3
d. PBCI_3, PBCD_C_3

Uit bovenstaande tabel blijkt dat de controle van een medewerker om veilig om te gaan met zijn wachtwoord, een voorspellende waarde van 3,7% heeft op de intentie om veilig om te gaan met zijn wachtwoord. Wat een medewerker zelf denkt dat hij kan doen ten aanzien van het veilig omgaan met zijn wachtwoord, heeft een voorspellende waarde van 15,3% op de intentie om veilig om te gaan met zijn wachtwoord. In totaliteit voorspellen *perceived behavioral control* en *control beliefs* voor 15,6% de intentie van een medewerker om veilig om te gaan met zijn wachtwoord. Hiermee leveren deze twee

predictor variabelen voor model één, twee en drie een unieke significante bijdrage en voor model vier geen unieke significante bijdrage om deze gedragsintentie als criterium variabele te voorspellen.

Uit de tabellen en beschreven resultaten kunnen verschillende conclusies getrokken worden die betrekking hebben op de derde deelvraag. Deze conclusies zijn in onderstaande opsomming weergegeven:

- De capaciteit van een medewerker ten aanzien van alle drie de gedragsintenties, is de sterkst verklarende voorspeller vanuit de perceived behavioral control ten aanzien van alle drie de gedragsintenties. Dit wil zeggen dat wat een medewerkers zelf kan, de meeste invloed heeft op de intentie om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoord. Naarmate een medewerker zelf meer kan ten aanzien van het beschermen van zijn bedrijfsgegevens, het zekerstellen van zijn bedrijfsgegevens en het veilig omgaan met zijn wachtwoord, zullen ook de intenties om dit te doen toenemen.
- De capaciteit van een medewerker ten aanzien van de drie gedragsintenties, is een sterkere verklarende voorspeller, dan de controle van een medewerker ten aanzien van de drie gedragsintenties. Dit wil zeggen dat wat een medewerker zelf kan, een grotere invloed heeft op de intentie om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoord, dan wat een medewerker denkt zelf te kunnen. Naarmate een medewerker zelf meer kan ten aanzien van het beschermen van zijn bedrijfsgegevens, het zekerstellen van zijn bedrijfsgegevens en het veilig omgaan met zijn wachtwoord, zullen ook de intenties om dit te doen groter zijn dan wat een medewerker denkt zelf te kunnen.
- De controle van een medewerker ten aanzien van het beschermen van zijn bedrijfsgegevens en het veilig omgaan met zijn wachtwoord, is de zwakst verklarende voorspeller voor de intentie van een medewerker om zijn bedrijfsgegevens te beschermen en veilig om te gaan met zijn wachtwoordgebruik. Dit wil zeggen dat wat een medewerker zelf denkt dat hij kan doen, de minste invloed heeft op de intentie om zijn bedrijfsgegevens te beschermen en veilig om te gaan met zijn wachtwoord. Naarmate een medewerker denkt zelf meer te kunnen ten aanzien van het beschermen van zijn bedrijfsgegevens en het veilig omgaan met zijn wachtwoord, zullen de intenties om dit te doen *minimaal* toenemen.
- De capaciteit van een medewerker ten aanzien van de drie gedragsintenties, is een sterkere verklarende voorspeller dan wat een medewerker zelf denkt dat hij kan doen ten aanzien van de drie gedragsintenties. Dit wil zeggen dat wat een medewerker zelf kan (directe meting), een grotere invloed heeft op de intentie om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoord, dan wat een medewerker zelf denkt dat hij kan doen (indirecte meting). Naarmate een medewerker zelf meer kan (directe meting) ten aanzien van het beschermen van zijn bedrijfsgegevens, het zekerstellen van zijn bedrijfsgegevens en het veilig omgaan met zijn wachtwoord, zullen ook de intenties om dit te doen groter zijn dan wat een medewerker zelf denkt dat hij kan doen (indirecte meting).
- Wat een medewerker zelf denkt dat hij kan doen ten aanzien van de drie gedragsintenties, is een sterkere verklarende voorspeller dan de controle van een medewerker ten aanzien van de drie gedragsintenties. Dit wil zeggen dat wat een medewerker zelf denkt dat hij kan doen (indirecte meting), een grotere invloed heeft op de intentie om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoord, dan wat een medewerker zelf denkt dat hij kan doen (directe meting). Naarmate een medewerker zelf denkt dat hij meer kan doen (indirecte meting) ten aanzien van het beschermen van zijn bedrijfsgegevens, het zekerstellen van zijn bedrijfsgegevens en het veilig

omgaan met zijn wachtwoord, zullen ook de intenties om dit te doen groter zijn dan wat een medewerker zelf denkt dat hij kan doen (directe meting).

5.1.2.4 Attitude toward the behavior, subjective norm, perceived behavioral control en de gedragsintentie

Binnen dit hoofdstuk wordt de volgende deelvraag beantwoord: wat is de voorspellende waarde van de samenhang tussen de attitude toward the behavior, subjective norm en perceived behavioral control ten opzichte van de gedragsintentie ten aanzien van informatiebeveiliging?

Deze deelvraag is beantwoord door de beste voorspellers van alle determinanten samen te nemen als predictor variabelen op de gedragsintentie om bedrijfsgegevens te beschermen, bedrijfsgegevens zeker te stellen en veilig om te gaan met wachtwoordgebruik als criterium variabelen. Er is voor elk hoofdonderwerp één analyse uitgevoerd middels de enter methode. De resultaten van deze analyse zijn voor alle hoofdonderwerpen apart in onderstaande tabellen weergegeven.

De beste voorspellers voor het hoofdonderwerp bedrijfsgegevens zijn in onderstaande tabel weergegeven. De beste voorspeller staat bovenaan en de slechtste voorspeller staat onderaan

Tabel 32 "Bedrijfsgegevens"
Percentages voorspellers (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,264***	,264	,513***
2[b]	,209***	,209	,457***
3[c]	,159***	,159	,399***
4[d]	,157***	,157	,396***
5[e]	,115***	,115	,339***
6[f]	,085***	,085	,292***
7[g]	,066***	,066	,257***
8[h]	,048**	,048	,219**
9[i]	,032**	,032	,180**
10[j]	,018º	,018	,132º

º ($p > .05$), ** ($p < .01$) en *** ($p < .001$)

a. AD_1
b. SND_IN_1
c. AI_1
d. SNI_IN_NC_1
e. SNI_DN_1
f. SNI_IN_DL_1
g. PBCD_SE_1
h. SND_DN_1
i. PBCI_1
j. PBCD_C_1

Aan de hand van deze tabel zullen de beste voorspellers ten opzichte van de intentie om bedrijfsgegevens te beschermen gekozen worden. Dit is op een trial and error wijze gedaan. Deze wijze moet als volgt geïnterpreteerd worden: eerst worden de op het oog de beste voorspellers gekozen en daarna wordt gekeken wat een voorspeller aan voorspellende waarde vergroot of verkleint. Wanneer de voorspeller meer dan 1% voorspellende waarde toevoegt zal deze meegenomen worden en wanneer de voorspeller minder dan 1% voorspellende waarde toevoegt zal

deze niet meegenomen worden. In onderstaande tabel zijn de beste voorspellers samengevoegd voor het hoofdonderwerp bedrijfsgegevens.

Tabel 33 "Bedrijfsgegevens"
Beste voorspellers (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,369***	,369	,324*** ,194** ,130* ,158*

* (p < .05), ** (p < .01) en *** (p < .001)

a. AD_1, SND_IN_1, AI_1, SNI_IN_NC_1

Uit bovenstaande tabel blijkt dat precies dezelfde voorspellers gekozen zijn als bij het hoofdonderwerp bedrijfsgegevens in de compacte analyse. De voorspellers: AD_1, SND_IN_1, AI_1 en SNI_IN_NC_1 hebben een voorspellende waarde van 36,9% op de intentie om bedrijfsgegevens te beschermen. Hiermee leveren alle predictor variabelen voor het model een unieke significante bijdrage om deze gedragsintentie als criterium variabele te voorspellen.

De beste voorspellers voor het hoofdonderwerp back-up zijn in onderstaande tabel weergegeven. De beste voorspeller staat bovenaan en de slechtste voorspeller staat onderaan

Tabel 34 "Back-up"
Percentages voorspellers (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,258***	,258	,508***
2[b]	,223***	,223	,472***
3[c]	,222***	,222	,472***
4[d]	,197***	,197	,444***
5[e]	,190***	,190	,436***
6[f]	,169***	,169	,411***
7[g]	,152***	,152	,389***
8[h]	,124***	,124	,352***
9[i]	,077***	,077	,277***
10[j]	,055**	,055	,234**

** (p < .01) en *** (p < .001)

a. SND_IN_2
b. AD_2
c. PBCD_SE_2
d. PBCI_2
e. SNI_IN_NC_2
f. PBCD_C_2
g. SNI_IN_DL_2
h. SNI_DN_2
i. AI_2
j. SND_DN_2

Aan de hand van deze tabel zullen de beste voorspellers ten opzichte van de intentie om bedrijfsgegevens zeker te stellen gekozen worden. Dit is op een trial and error wijze gedaan. Deze wijze moet als volgt geïnterpreteerd worden: eerst worden de op het oog beste voorspellers gekozen

en daarna wordt gekeken wat een voorspeller aan voorspellende waarde vergroot of verkleint. Wanneer de voorspeller meer dan 1% voorspellende waarde toevoegt zal deze meegenomen worden en wanneer de voorspeller minder dan 1% voorspellende waarde toevoegt zal deze niet meegenomen worden. In onderstaande tabel zijn de beste voorspellers samengevoegd voor het hoofdonderwerp back-up.

Tabel 35 "Back-up"
Beste voorspellers (n = 216)

Model	R Square	R Square Change	Beta
			,191**
			,179**
1[a]	,369***	,369	,195**
			,155*
			,190**

* (p < .05), ** (p < .01) en *** (p < .001)

a. PBCD_C_2, SNI_IN_NC_2, AD_2, PBCD_SE_2, SND_IN_2

Uit bovenstaande tabel blijkt dat precies dezelfde voorspellers gekozen zijn als bij het hoofdonderwerp back-up in de compacte analyse. De voorspellers: SND_IN_2 , AD_2, PBCD_SE_2, SNI_IN_NC_2 en PBCD_C_2 hebben een voorspellende waarde van 41,8% op de intentie om bedrijfsgegevens zeker te stellen. Hiermee leveren alle predictor variabelen voor het model een unieke significante bijdrage om deze gedragsintentie als criterium variabele te voorspellen.

De beste voorspellers voor het hoofdonderwerp wachtwoordgebruik zijn in onderstaande tabel weergegeven. De beste voorspeller staat bovenaan en de slechtste voorspeller staat onderaan

Tabel 36 "Wachtwoordgebruik"
Percentages voorspellers (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,297***	,297	,545***
2[b]	,187***	,187	,432***
3[c]	,163***	,163	,404***
4[d]	,153***	,153	,392***
5[e]	,115***	,115	,339***
6[f]	,062***	,062	,249***
7[g]	,057***	,057	,240***
8[h]	,037**	,037	,192**
9[i]	,029*	,029	,169*
10[j]	,021*	,021	,144*

* (p < .05), ** (p < .01) en *** (p < .001)

a. AD_3
b. AI_3
c. PBCD_SE_3
d. PBCI_3
e. SND_IN_3
f. SNI_DN_3
g. SNI_IN_NC_3
h. PBCD_C_3
i. SNI_IN_DL_3
j. SND_DN_3

Aan de hand van deze tabel zullen de beste voorspellers ten opzichte van de intentie om veilig om te gaan met wachtwoordgebruik gekozen worden. Dit is op een trial and error wijze gedaan. Deze wijze moet als volgt geïnterpreteerd worden: eerst worden de op het oog beste voorspellers gekozen en daarna wordt gekeken wat een voorspeller aan voorspellende waarde vergroot of verkleint. Wanneer de voorspeller meer dan 1% voorspellende waarde toevoegt zal deze meegenomen worden en wanneer de voorspeller minder dan 1% voorspellende waarde toevoegt zal deze niet meegenomen worden. In onderstaande tabel zijn de beste voorspellers samengevoegd voor het hoofdonderwerp wachtwoordgebruik.

Tabel 37 "Wachtwoordgebruik"
Beste voorspellers (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,366***	,366	,414*** ,228*** ,124*

* (p < .05) en *** (p < .001)

a. AD_3, AI_3, SND_IN_3

Uit bovenstaande tabel blijkt dat precies dezelfde voorspellers gekozen zijn als bij het hoofdonderwerp wachtwoordgebruik in de compacte analyse. De voorspellers: AD_3, AI_3 en SND_IN_3 hebben een voorspellende waarde van 36,6% op de intentie om veilig om te gaan met wachtwoordgebruik. Hiermee leveren alle predictor variabelen voor het model een unieke significante bijdrage om deze gedragsintentie als criterium variabele te voorspellen.

Uit de tabellen en beschreven resultaten kunnen verschillende conclusies getrokken worden die betrekking hebben op de vierde deelvraag. Deze conclusies zijn in onderstaande opsomming weergegeven:

- De houding van een medewerker ten aanzien van de drie gedragsintenties is de sterkst verklarende voorspeller van de drie determinanten (attitude toward the behavior, subjective norm en perceived behavioral control). Dit wil zeggen dat de houding van een medewerker de meeste invloed heeft op de intentie om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoord.
- Attitude toward the behavior en subjective norm zijn de sterkst verklarende voorspellers voor de intentie van een medewerker om zijn bedrijfsgegevens te beschermen en veilig om te gaan met zijn wachtwoord. Dit wil zeggen dat de houding en de norm vanuit de sociale omgeving van een medewerker de meeste invloed hebben op de intentie om zijn bedrijfsgegevens te beschermen en veilig om te gaan met zijn wachtwoord.
- Attitude toward the behavior, subjective norm en perceived behavioral control zijn alle drie sterke verklarende voorspellers voor de intentie van een medewerker om zijn bedrijfsgegevens zeker te stellen. Dit wil zeggen dat de houding, de norm vanuit de sociale omgeving, de capaciteit en de controle van een medewerker de meeste invloed hebben op de intentie om zijn bedrijfsgegevens zeker te stellen.

5.2 Het mediatoreffect

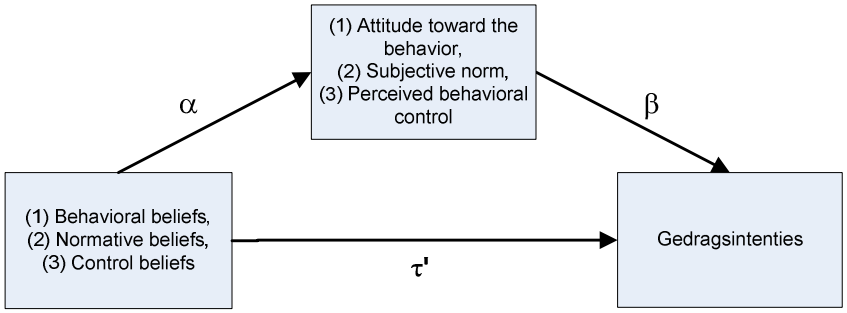
Als laatste is het mediatoreffect voor de behavioral beliefs, normative beliefs en control beliefs ten opzichte van de onderliggende cognitieve fundamenten attitude toward the behavior, subjective norm en perceived behavioral control onderzocht. Hierbij is gekeken of er sprake is van een

mediatoreffect voor de drie interveniërende variabelen of dat er vanuit de belief variabelen ook een directe relatie bestaat met de gedragsintentie. De mediatorvariabelen of interveniërende variabelen worden gevormd door de attitude toward the behavior, subjective norm en perceived behavioral control die medieert of intervenieert tussen de onafhankelijke variabelen behavioral beliefs, normative beliefs, en control beliefs en de afhankelijke variabele gedragsintentie. De mediatorvariabelen attitude toward the behavior, subjective norm en perceived behavioral control spelen twee rollen: ten eerste vormen zij de afhankelijke variabelen ten opzichte van de behavioral beliefs, normative beliefs en control beliefs. Ten tweede vormen zij de onafhankelijke variabelen ten opzichte van de gedragsintentie. Om aan te kunnen tonen dat er sprake is van een mediatoreffect moet worden voldaan aan een viertal eisen [BARO86], [JUDD81], [MACK93]:

- Er bestaat een samenhang tussen de behavioral beliefs, normative beliefs en control beliefs en de gedragsintentie. Hierbij moet worden aangetoond dat de behavioral beliefs, normative beliefs en control beliefs een statistisch significant effect hebben op de gedragsintentie.
- De attitude toward the behavior, subjective norm en perceived behavioral control kunnen deze samenhang tussen de behavioral beliefs, normative beliefs, en control beliefs en gedragsintentie alleen dan verklaren, als de attitude toward the behavior, subjective norm en perceived behavioral control samenhangen met de behavioral beliefs, normative beliefs en control beliefs. Hierbij moet worden aangetoond dat de behavioral beliefs, normative beliefs en control beliefs een statistisch significant effect hebben op de attitude toward the behavior, subjective norm en perceived behavioral control.
- De attitude toward the behavior, subjective norm en perceived behavioral control kunnen deze samenhang tussen de behavioral beliefs, normative beliefs, en control beliefs en de gedragsintentie alleen dan verklaren, als de attitude toward the behavior, subjective norm en perceived behavioral control ook samenhangen met de gedragsintentie. Hierbij moet worden aangetoond dat de attitude toward the behavior, subjective norm en perceived behavioral control een statistisch significant effect hebben op de gedragsintentie.
- Als de attitude toward the behavior, subjective norm en perceived behavioral control de samenhang tussen de behavioral beliefs, normative beliefs, en control beliefs en de gedragsintentie kunnen verklaren dan impliceert dit, ten slotte, dat de gedragsintentie niet langer samenhangt met de behavioral beliefs, normative beliefs en control beliefs, zodra de attitude toward the behavior, subjective norm en perceived behavioral control constant worden gehouden. Hierbij moet worden aangetoond dat de partiële regressiecoëfficiënten van de behavioral beliefs, normative beliefs en control beliefs onder constant houden van de attitude toward the behavior, subjective norm en perceived behavioral control niet statistisch significant zijn.

Bij de vierde eis kan onderscheid worden gemaakt tussen volledige en gedeeltelijke mediatie. Van volledige mediatie is sprake als het effect van de behavioral beliefs, normative beliefs en control beliefs op de gedragsintentie volledig verklaard kan worden door de mediatorvariabele van de attitude toward the behavior, subjective norm en perceived behavioral control. Het effect van de behavioral beliefs, normative beliefs en control beliefs op de gedragsintentie verdwijnt geheel, zodra de attitude toward the behavior, subjective norm en perceived behavioral control constant worden gehouden. Van gedeeltelijke mediatie is sprake wanneer het effect van de behavioral beliefs, normative beliefs en control beliefs op gedragsintentie zwakker wordt, maar niet geheel verdwijnt als de attitude toward the behavior, subjective norm en perceived behavioral control constant worden gehouden. Er is geen sprake van mediatie als de partiële regressiecoëfficiënten van de behavioral beliefs, normative beliefs en control beliefs bij de vierde eis even groot of zelfs groter zijn dan de regressiecoëfficiënten van de behavioral beliefs, normative beliefs en control beliefs bij de eerste eis, waarbij de attitude toward the behavior, subjective norm en perceived behavioral control niet constant zijn gehouden.

Naast de volledige en gedeeltelijke mediatie, kan de relatie tussen de behavioral beliefs, normative beliefs, control beliefs, de attitude toward the behavior, subjective norm, perceived behavioral control en de gedragsintentie ook geformuleerd worden in termen van directe effecten, mediator effecten en totale effecten. Het directe effect (in figuur 34: τ') van de behavioral beliefs, normative beliefs en control beliefs op de gedragsintentie is het effect dat niet verloopt via de attitude toward the behavior, subjective norm en perceived behavioral control, maar rechtstreeks gaat. Dit komt overeen met de partiële regressiegewichten van de behavioral beliefs, normative beliefs en control beliefs bij de vierde eis, waar de attitude toward the behavior, subjective norm en perceived behavioral control constant zijn gehouden. Het mediatoreffect (in figuur 34: $\alpha\beta$) van de behavioral beliefs, normative beliefs en control beliefs op de gedragsintentie is het effect van de behavioral beliefs, normative beliefs en control beliefs op de gedragsintentie wat verloopt via de attitude toward the behavior, subjective norm en perceived behavioral control. Dit zijn de regressiecoëfficiënten van de behavioral beliefs, normative beliefs en control beliefs bij de tweede eis. Hierbij wordt nagegaan of de behavioral beliefs, normative beliefs en control beliefs effect hebben op de attitude toward the behavior, subjective norm en perceived behavioral control, maal de regressiecoëfficiënten van de attitude toward the behavior, subjective norm en perceived behavioral control bij de derde eis. Hierbij wordt immers nagegaan of de attitude toward the behavior, subjective norm en perceived behavioral control een effect hebben op de gedragsintentie. Het totale effect (in figuur 34: $\tau' + \alpha\beta$) van de behavioral beliefs, normative beliefs en control beliefs op de gedragsintentie is de som van de directe en de mediator effecten. Het bestaan van dit totale effect wordt vastgesteld bij de eerste eis. Hieronder zijn de verschillende relaties voor het mediatoreffect schematisch weergegeven:



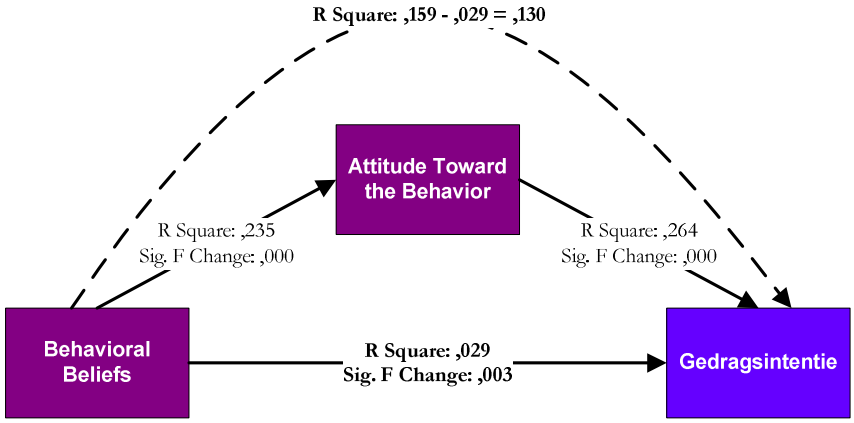
Figuur 34: Het mediatoreffect

Om vast te stellen of er sprake is van een mediatoreffect zijn er twee regressieanalyses uitgevoerd:

- Regressieanalyse A: effect van de onafhankelijke variabelen behavioral beliefs, normative beliefs en control beliefs op de mediatorvariabelen attitude toward the behavior, subjective norm en perceived behavioral control.
- Regressieanalyse B: de effecten van de onafhankelijke variabelen behavioral beliefs, normative beliefs, en control beliefs en de mediatorvariabelen attitude toward the behavior, subjective norm en perceived behavioral control op de afhankelijke variabele gedragsintentie.

Hierbij is getoetst of de mediator effecten van de behavioral beliefs, normative beliefs en control beliefs op de gedragsintentie statistisch significant zijn en voor welk percentage het totale effect van de behavioral beliefs, normative beliefs en control beliefs op de gedragsintentie voor rekening komt van het mediator effect (via de attitude toward the behavior, subjective norm en perceived behavioral control), dus voor welk percentage de attitude toward the behavior, subjective norm en perceived behavioral control het effect van de behavioral beliefs, normative beliefs en control beliefs op de gedragsintentie medieert. Hieronder is schematisch bovenstaande theorie in praktijk omgezet om een

beeld te geven van het mediatoreffect. Voor de onafhankelijke variabele is de behavioral beliefs gekozen, voor de mediatorvariabele is de attitude toward the behavior gekozen en voor de afhankelijke variabele is de gedragsintentie gekozen. Al deze variabelen hebben betrekking op het hoofdonderwerp *bedrijfsgegevens*.



Figuur 35: Mediatoreffect voorbeeld

In de onderstaande tabel zijn de verschillende onderzochte relaties weergegeven:

Tabel 38 "Bedrijfsgegevens, back-up en wachtwoordgebruik"
Mediatoreffect attitude toward the behavior en behavioral beliefs

Model	R Square	Mediatoreffect?
1	,159 - ,029 = ,130[a]	Gedeeltelijk
2	,077 - ,007 = ,070[b]	Volledig
3	,187 - ,056 = ,131[c]	Gedeeltelijk

a. AI_1, AD_1 en I_1
b. AI_2, AD_2 en I_2
c. AI_3, AD_3 en I_3

In model 1 en 3 is er een gedeeltelijk mediatoreffect, omdat de relatie tussen de behavioral beliefs en de gedragsintentie significant is. In model 2 is er een volledig mediatoreffect, omdat de relatie tussen de behavioral beliefs en de gedragsintentie niet significant is. Het effect in model 1 van de behavioral beliefs rechtstreeks op de gedragsintentie is 2,9%, in model 2 is dit effect 0,7% en in model 3 is dit effect 5,6%. Het effect in model 1 van de behavioral beliefs op de gedragsintentie via de attitude toward the behavior is 13,0%, in model 2 is dit effect 7,7% en in model 3 is dit effect 13,1%. Er kan geconcludeerd worden dat er in deze modellen een veel groter effect is dat via de mediatorvariabele loopt, dan het effect van de behavioral beliefs rechtstreeks op de gedragsintentie.

Tabel 39 "Bedrijfsgegevens, back-up en wachtwoordgebruik"
Mediatoreffect subjective norm en normative beliefs

Model	R Square	Mediatoreffect?
1	,085 - ,004 = ,081[a]	Volledig
2	,157 - ,031 = ,126[b]	Gedeeltelijk
3	,115 - ,075 = ,040[c]	Gedeeltelijk
4	,152 - ,019 = ,133[d]	Gedeeltelijk
5	,190 - ,032 = ,158[e]	Gedeeltelijk
6	,124 - ,078 = ,046[f]	Gedeeltelijk
7	,029 - ,000 = ,029[g]	Volledig
8	,057 - ,002 = ,055[h]	Volledig
9	,062 - ,043 = ,019[i]	Gedeeltelijk

a. SNI_IN_DL_1, SND_IN_1 en I_1
b. SNI_IN_NC_1, SND_IN_1 en I_1
c. SNI_DN_1, SND_DN_1 en I_1
d. SNI_IN_DL_2, SND_IN_2 en I_2
e. SNI_IN_NC_2, SND_IN_2 en I_2
f. SNI_DN_2, SND_DN_2 en I_2
g. SNI_IN_DL_3, SND_IN_3 en I_3
h. SNI_IN_NC_3, SND_IN_3 en I_3
i. SNI_DN_3, SND_DN_3 en I_3

In model 2, 3, 4, 5, 6 en 9 is er een gedeeltelijk mediatoreffect, omdat de relatie tussen de normative beliefs en de gedragsintentie significant is. In model 1, 7 en 8 is er een volledig mediatoreffect, omdat de relatie tussen de normative beliefs en de gedragsintentie niet significant is. Het effect in model 1 van de normative beliefs rechtstreeks op de gedragsintentie is 0,4%, in model 2 is dit effect 3,1%, in model 3 is dit effect 7,5%, in model 4 is dit effect 1,9%, in model 5 is dit effect 3,2%, in model 6 is dit effect 7,8%, in model 7 is dit effect 0,0%, in model 8 is dit effect 0,2% en in model 9 is dit effect 4,3%. Het effect in model 1 van de normative beliefs op de gedragsintentie via de subjective norm is 8,1%, in model 2 is dit effect 12,6%, in model 3 is dit effect 4,0%, in model 4 is dit effect 13,3%, in model 5 is dit effect 15,8%, in model 6 is dit effect 4,6%, in model 7 is dit effect 2,9%, in model 8 is dit effect 5,5% en in model 9 is dit effect 1,9%. Er kan geconcludeerd worden dat er in de meeste modellen een veel groter effect is dat via de mediatorvariabele loopt, dan het effect van de normative beliefs rechtstreeks op de gedragsintentie. Alleen in de modellen 3, 6 en 9 (die ingaan op wat naaste collega's, die belangrijk voor een medewerker zijn, zelf doen ten aanzien van de drie gedragsintenties) is het effect van de normative beliefs op de gedragsintentie groter dan het effect van de normative beliefs op de gedragsintentie via de subjective norm.

Tabel 40 "Bedrijfsgegevens, back-up en wachtwoordgebruik"
Mediatoreffect perceived behavioral control en control beliefs

Model	R Square	Mediatoreffect?
1	,032 - ,001 = ,031[a]	Volledig
2	,032 - ,020 = ,012[b]	Gedeeltelijk
3	,197 - ,033 = ,164[c]	Gedeeltelijk
4	,197 - ,080 = ,117[d]	Gedeeltelijk
5	,153 - ,029 = ,124[e]	Gedeeltelijk
6	,153 - ,120 = ,033[f]	Gedeeltelijk

a. PBCI_1, PBCD_SE_1 en I_1
b. PBCI_1, PBCD_C_1 en I_1
c. PBCI_2, PBCD_SE_2 en I_2
d. PBCI_2, PBCD_C_2 en I_2
e. PBCI_3, PBCD_SE_3 en I_3
f. PBCI_3, PBCD_C_3 en I_3

In model 2 tot en met 6 is er een gedeeltelijk mediatoreffect, omdat de relatie tussen de control beliefs en de gedragsintentie significant is. In model 1 is er een volledig mediatoreffect, omdat de relatie tussen de control beliefs en de gedragsintentie niet significant is. Het effect in model 1 van de control beliefs rechtstreeks op de gedragsintentie is 0,1%, in model 2 is dit effect 2,0%, in model 3 is dit effect 3,3%, in model 4 is dit effect 8,0%, in model 5 is dit effect 2,9% en in model 6 is dit effect 12,0%. Het effect in model 1 van de control beliefs op de gedragsintentie via de perceived behavioral control is 3,1%, in model 2 is dit effect 1,2%, in model 3 is dit effect 16,4%, in model 4 is dit effect 11,7%, in model 5 is dit effect 12,4% en in model 6 is dit effect 3,3%. Er kan geconcludeerd worden dat er in de meeste modellen een veel groter effect is dat via de mediatorvariabele loopt, dan het effect van de control beliefs rechtstreeks op de gedragsintentie. Alleen in de modellen 2 en 6 is het effect van de control beliefs op de gedragsintentie groter dan het effect van de control beliefs op de gedragsintentie via de perceived behavioral control.

5.3 Trainings- en bewustwordingscampagnes analyse

Binnen dit onderzoek is regelmatig gerefereerd naar trainings- en bewustwordingscampagnes voor informatiebeveiliging. Stanton heeft in zijn vragenlijst gekeken naar de overwegingen die medewerkers hadden op basis van een raamwerk dat onder andere bestond uit *training and awareness* om te voorspellen hoe succesvol de informatiebeveiliging van de organisatie zou zijn. Zijn conclusie was dat er een sterke relatie bestaat tussen de overwegingen die medewerkers hebben in de mate van "training and awareness" binnen de organisatie en de mate van succes van de informatiebeveiliging. Om dit te toetsen zijn hiervoor een viertal items opgenomen met betrekking tot het veiliger om kunnen gaan met bedrijfsgegevens door trainings- en bewustwordingscampagnes. Deze zijn samengevoegd tot PBCI_5. De analyse is uitgevoerd middels de gedragsintenties I_1, I_2 en I_3 als criteriumvariabelen en PBCI_5 als predictor variabele. In onderstaande tabel zijn de resultaten voor de verschillende hoofdonderwerpen: bedrijfsgegevens, back-up en wachtwoordgebruik te zien.

Tabel 41 "Trainings- en bewustwordingscampagnes"

Trainings- en bewustwordingscampagnes als voorspeller voor bedrijfsgegevens, back-up en wachtwoordgebruik (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,021*	,021	,143*
2[b]	,017º	,017	,129º
3[c]	,040**	,040	,199**

º ($p > .05$), * ($p < .05$) en ** ($p < .01$)

a. PBCI_5 op I_1
b. PBCI_5 op I_2
c. PBCI_5 op I_3

Uit bovenstaande tabel blijkt dat wat een medewerker zelf denkt dat hij door trainings- en bewustwordingscampagnes kan doen ten aanzien van het beschermen van zijn bedrijfsgegevens, een voorspellende waarde van 2,1% heeft op de intentie om zijn bedrijfsgegevens te beschermen. Wat een medewerker zelf denkt dat hij door trainings- en bewustwordingscampagnes kan doen ten aanzien van het zekerstellen van zijn bedrijfsgegevens, heeft geen unieke significante bijdrage. En wat een medewerker zelf denkt dat hij door trainings- en bewustwordingscampagnes kan doen ten aanzien van het veilig omgaan met zijn wachtwoord, heeft een voorspellende waarde van 4,0% op de intentie om veilig om te gaan zijn wachtwoord. Deze voorspellende waarde zijn voor alle gedragsintenties van de hoofdonderwerpen zwak te noemen. Dit wil dus zeggen dat de kans klein is dat de intentie van een medewerker om veilig met zijn bedrijfsgegevens om te gaan door trainings- en bewustwordingscampagnes beter zal worden.

5.4 Organisatorische verplichtingen analyse

Uit het onderzoek Stanton e.a. komt naar voren dat de organisatorische verplichting van een medewerker een belangrijke gedragsvoorspeller is voor gedrag ten aanzien van informatiebeveiliging. Om dit te toetsen zijn hiervoor een viertal items opgenomen die ingaan op de organisatorische verplichtingen die samengevoegd zijn tot SNI_IN_4. De analyse is uitgevoerd middels de gedragsintenties I_1, I_2 en I_3 als criteriumvariabelen en SNI_IN_4 als predictor variabele. In onderstaande tabel zijn de resultaten voor de verschillende hoofdonderwerpen: bedrijfsgegevens, back-up en wachtwoordgebruik te zien.

Tabel 42 "Organisatorische verplichtingen"

Organisatorische verplichtingen als voorspeller voor bedrijfsgegevens, back-up en wachtwoordgebruik (n = 216)

Model	R Square	R Square Change	Beta
1[a]	,099***	,099	,315***
2[b]	,018º	,018	,133º
3[c]	,070***	,070	,264***

º ($p > .05$) en *** ($p < .001$)

a. SNI_IN_4 op I_1
b. SNI_IN_4 op I_2
c. SNI_IN_4 op I_3

Uit bovenstaande tabel blijkt dat wat de organisatie vindt dat een medewerker moet doen met zijn bedrijfsgegevens en of hier voorschriften voor opgesteld zijn waarnaar hij moet handelen, een voorspellende waarde van 9,9% hebben op de intentie om zijn bedrijfsgegevens te beschermen. Ten aanzien van het zekerstellen van zijn bedrijfsgegevens, heeft het een voorspellende waarde van 1,8%.

Voor het veilig omgaan met zijn wachtwoord, heeft het een voorspellende waarde van 7,0%. Deze voorspellende waarden zijn voor het beschermen van bedrijfsgegevens en het veilig omgaan met het wachtwoord zwak tot matig te noemen en voor het zekertellen van bedrijfsgegevens zwak te noemen. Dit wil zeggen dat er een matige kans bestaat dat de intenties van een medewerker om zijn bedrijfsgegevens te beschermen en veilig met zijn wachtwoord om te gaan, worden beïnvloed door organisatorische procedures en voorschriften die zowel actief als passief door de organisatie worden uitgedragen. Voor de intenties van een medewerker om zijn bedrijfsgegevens zeker te stellen bestaat een kleine kans dat deze worden beïnvloed door organisatorische procedures en voorschriften die zowel actief als passief door de organisatie worden uitgedragen.

6. CONCLUSIES EN DISCUSSIE

In dit onderzoek is middels de theorie van gepland gedrag getracht voorspellende verklaringen te vinden voor het proces bij medewerkers binnen organisaties dat leidt tot gedragsintenties ten aanzien van informatiebeveiliging. In dit afsluitend hoofdstuk komen achtereenvolgens de volgende onderwerpen aan bod: wat zijn de belangrijkste bevindingen uit het hoofdonderzoek, welke conclusies kunnen op grond van dit onderzoek worden getrokken met betrekking tot de waarde van de theorie van gepland gedrag voor het verklaren van gedrag ten aanzien van informatiebeveiliging (paragraaf 6.1), wat zijn de mogelijke andere verklarende variabelen naast de onderzochte attitude toward the behavior, subjective norm en perceived behavioral control vanuit het literatuuronderzoek (paragraaf 6.2), wat is de maatschappelijke relevantie van dit onderzoek (paragraaf 6.3), met welke kanttekeningen moet er bij de interpretatie van dit onderzoek rekening gehouden worden (paragraaf 6.4) en wat zijn de mogelijke suggesties voor vervolgonderzoeken (paragraaf 6.5).

6.1 De conclusies op een rij

In hoeverre kunnen vanuit de theorie van gepland gedrag mogelijke voorspellende verklaringen voor de gedragsintenties van medewerkers binnen organisaties in Nederland ten aanzien van informatiebeveiliging gedaan worden, vanuit de attitude toward the behavior, subjective norm en perceived behavioral control? Deze paragraaf geeft een overzicht van de conclusies die kunnen worden getrokken met betrekking tot deze vraag, vanuit de resultaten van dit onderzoek.

Geconcludeerd wordt met betrekking tot de attitude toward the behavior dat een positieve of negatieve houding van een medewerker ten opzichte van de gedragsintentie om bedrijfsgegevens te beschermen, bedrijfsgegevens zeker te stellen en veilig om te gaan met wachtwoordgebruik de sterkst verklarende voorspeller is van de drie determinanten (attitude toward the behavior, subjective norm en perceived behavioral control). Hierbij zijn de volgende relaties gevonden. Naarmate een medewerker het verstandiger, nuttiger voor zichzelf en nuttiger voor anderen vindt om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoordgebruik, zullen ook de intenties om dit te doen toenemen. Naarmate een medewerker het prettiger vindt om zijn bedrijfsgegevens te beschermen, zal ook de intentie om dit te doen toenemen. Daarentegen heeft de moeilijkheidsgraad voor een medewerker om zijn bedrijfsgegevens te beschermen geen invloed op de intentie om dit te doen. Als laatste hebben de pleziergraad en de moeilijkheidsgraad voor een medewerker om zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoord ook geen invloed op de intenties om dit te doen. De bovenstaande relaties zijn in onderstaande tabel samengevat weergegeven.

Tabel 43
Samenvatting relaties attitude

	Beschermen bedrijfsgegevens	Zekerstellen bedrijfsgegevens	Veilig omgaan wachtwoordgebruik
Wijsheidsgraad	+	+	+
Pleziergraad	+		
Nuttigheidsgraad voor zichzelf	+	+	+
Moeilijkheidsgraad			
Nuttigheidsgraad voor anderen	+	+	+

Geconcludeerd wordt met betrekking tot de subjective norm dat de volgende relaties bestaan. Naarmate de invloed van wat belangrijke mensen[41] van een medewerker vinden dat hij moet doen en wat er van een medewerker verwacht wordt toeneemt om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoordgebruik, zullen ook de intenties om dit te doen toenemen. Naarmate de invloed van wat naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen toeneemt om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoordgebruik, zullen ook de intenties om dit te doen groter zijn dan de invloed van wat een direct leidinggevende van een medewerker vindt dat hij moet doen. Naarmate de invloed van wat naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen toeneemt om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoordgebruik, zullen ook de intenties om dit te doen groter zijn dan de invloed van wat naaste collega's, die belangrijk voor een medewerker zijn, zelf doen. Naarmate de invloed van wat belangrijke mensen van een medewerker zelf doen toeneemt om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoordgebruik, zullen de intenties om dit te doen *minimaal* toenemen. Naarmate de invloed van wat belangrijke mensen van een medewerker vinden dat hij moet doen en wat er van een medewerker verwacht wordt toeneemt om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoordgebruik, zullen ook de intenties om dit te doen groter zijn dan de invloed van wat direct leidinggevende en naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen. Naarmate de invloed van wat naaste collega's, die belangrijk voor een medewerker zijn, zelf doen toeneemt om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoordgebruik, zullen ook de intenties om dit te doen groter zijn dan de invloed van wat belangrijke mensen van een medewerker zelf doen. De bovenstaande relaties zijn in onderstaande tabel samengevat weergegeven.

Tabel 44
Samenvatting relaties subjective norm

	Beschermen bedrijfsgegevens	Zekerstellen bedrijfsgegevens	Veilig omgaan wachtwoordgebruik
Wat belangrijke mensen van een medewerker vinden dat hij moet doen	+++	+++	+++
Wat er van een medewerker verwacht wordt	+++	+++	+++
Wat belangrijke mensen van een medewerker zelf doen			
Wat een direct leidinggevende van een medewerker vindt dat hij moet doen	+	+	+
Wat naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen	++	++	++
Wat naaste collega's, die belangrijk voor een medewerker zijn, zelf doen	+	+	++

[41] Dit zijn referentiepersonen uit de omgeving van de medewerker, die voor hem of haar belangrijk zijn.

Geconcludeerd wordt met betrekking tot de perceived behavioral control dat de volgende relaties bestaan. Naarmate een medewerker zelf meer kan ten aanzien van het beschermen van zijn bedrijfsgegevens, het zekerstellen van zijn bedrijfsgegevens en het veilig omgaan met zijn wachtwoord, zullen ook de intenties om dit te doen toenemen. Naarmate een medewerker zelf meer kan ten aanzien van het beschermen van zijn bedrijfsgegevens, het zekerstellen van zijn bedrijfsgegevens en het veilig omgaan met zijn wachtwoord, zullen ook de intenties om dit te doen groter zijn dan wat een medewerker denkt zelf te kunnen. Naarmate een medewerker denkt zelf meer te kunnen ten aanzien van het beschermen van zijn bedrijfsgegevens en het veilig omgaan met zijn wachtwoord, zullen de intenties om dit te doen *minimaal* toenemen. De bovenstaande relaties zijn in onderstaande tabel samengevat weergegeven.

Tabel 45
Samenvatting relaties perceived behavioral control

	Beschermen bedrijfsgegevens	Zekerstellen bedrijfsgegevens	Veilig omgaan wachtwoordgebruik
Wat een medewerker zelf meer kan	++	++	++
Wat een medewerker denkt zelf te kunnen	+	+	+

Geconcludeerd kan worden met betrekking tot de relatie tussen de attitude toward the behavior, subjective norm en perceived behavioral control ten aanzien van de drie gedragsintenties, dat met name de houding van een medewerker ten aanzien van de drie gedragsintenties de sterkst verklarende voorspeller van de drie determinanten (attitude toward the behavior, subjective norm en perceived behavioral control) is. Dit wil zeggen dat de houding van een medewerker de meeste invloed heeft op de intentie om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoord. Daarnaast zijn attitude toward the behavior en subjective norm de sterkst verklarende voorspellers voor de intentie van een medewerker om zijn bedrijfsgegevens te beschermen en veilig om te gaan met zijn wachtwoord. Dit wil zeggen dat de houding en de norm vanuit de sociale omgeving van een medewerker de meeste invloed hebben op de intentie om zijn bedrijfsgegevens te beschermen en veilig om te gaan met zijn wachtwoord. Als laatste zijn de attitude toward the behavior, subjective norm en perceived behavioral control alle drie sterke verklarende voorspellers voor de intentie van een medewerker om zijn bedrijfsgegevens zeker te stellen. Dit wil zeggen dat de houding, de norm vanuit de sociale omgeving, de capaciteit en de controle van een medewerker de meeste invloed hebben op de intentie om zijn bedrijfsgegevens zeker te stellen. De bovenstaande relaties zijn in onderstaande tabel samengevat weergegeven.

Tabel 46
Samenvatting relaties tussen attitude, subjective norm en perceived behavioral control

	Beschermen bedrijfsgegevens	Zekerstellen bedrijfsgegevens	Veilig omgaan wachtwoordgebruik
Attitude	+++	++	+++
Subjective norm	++	++	++
Perceived behavioral control	+	++	+

Ajzen stelt dat de *behavioral beliefs* gemedieerd worden middels de *attitude toward the behavior*, de *normative beliefs* gemedieerd worden middels de *subjective norm* en de *control beliefs* gemedieerd worden middels de *perceived behavioral control*. Uit de resultaten van dit onderzoek kan geconcludeerd worden dat er voor de drie determinanten: *attitude toward the behavior*, *subjective norm* en *perceived behavioral control* een gedeeltelijk of volledig mediatoreffect bestaat. Dit wil zeggen dat de theoretische relaties worden bevestigd door de empirische gegevens uit dit onderzoek.

Uit onderzoek van Stanton e.a. zou er een sterke relatie moeten bestaan tussen de beliefs die medewerkers hebben in de mate van "training and awareness" binnen de organisatie en de mate van succes van de informatiebeveiliging. Uit de resultaten van dit onderzoek komt naar voren dat de kans klein is dat de intentie van een medewerker om veilig met zijn bedrijfsgegevens om te gaan door trainings- en bewustwordingscampagnes beter zal worden. Daarnaast zouden de resultaten uit het onderzoek van Stanton e.a. aantonen dat de organisatorische verplichting van medewerkers een belangrijke gedragsvoorspeller is voor informatiebeveiligingsgerelateerd gedrag. Uit de resultaten van dit onderzoek komt naar voren dat er een matige kans bestaat dat de intenties van een medewerker om zijn bedrijfsgegevens te beschermen en veilig met zijn wachtwoord om te gaan, worden beïnvloed door organisatorische procedures en voorschriften die zowel actief als passief door de organisatie worden uitgedragen. Voor de intenties van een medewerker om zijn bedrijfsgegevens zeker te stellen bestaat een kleine kans dat deze worden beïnvloed door organisatorische procedures en voorschriften die zowel actief als passief door de organisatie worden uitgedragen. Geconcludeerd kan worden met betrekking tot de "training and awareness" en de organisatorische verplichting, dat deze een lage voorspellende waarde hebben voor de gedragsintenties van een medewerker om zijn bedrijfsgegevens te beschermen, zijn bedrijfsgegevens zeker te stellen en veilig om te gaan met zijn wachtwoord.

6.2 Theoretische reflectie

In dit onderzoek is op basis van de theorie van gepland gedrag getracht inzicht te krijgen in de gedragsintentie van medewerkers binnen organisaties in Nederland bij het beveiligen van en veilig omgaan met de informatievoorziening van zijn of haar organisatie. Hierbij bevestigen de empirische gegevens de theoretische veronderstellingen vanuit de theorie van gepland gedrag. Er is alleen gekeken naar de gedragsintentie ten aanzien van informatiebeveiliging. Het daadwerkelijk gedrag en de actual behavioral control zijn buiten beschouwing gelaten. Met andere woorden, er is alleen gekeken naar verklarende invloeden en voorspellingen die de gedragsintentie vormgeven ten aanzien van informatiebeveiliging. Of de gedragsintentie vervolgens ook daadwerkelijk in gedrag zou kunnen worden omgezet en hoeveel actual behavioral control daarbij aanwezig is, is buiten beschouwing gelaten. Er is verder ook niet ingegaan op het automatisch gedrag ten aanzien van informatiebeveiliging, wat wordt gevormd door routines en gewoontes. Het volgende wordt verondersteld: hoe positiever de attitude toward the behavior, de subjective norm en de perceived behavioral control samenhangen, des te sterker de intentie van de persoon zal zijn om het gedrag in kwestie uit te voeren. Als laatste wordt verwacht dat een persoon zijn intentie tot werkelijk gedrag zal omzetten, als de situatie zich voordoet en als er voldoende werkelijke controle is over het desbetreffende gedrag. Dit alles bij elkaar genomen, kan de theorie van gepland gedrag gezien worden als een allesomvattende theorie voor het verklaren van gedrag. Gesteld wordt dat de gedragsintentie gevormd wordt door de variabelen attitude toward the behavior, de subjective norm en de perceived behavioral control. Dit wil zeggen dat alle andere invloeden interveniëren middels deze drie variabelen en zo indirect invloed hebben op de gedragsintentie. Ajzen sluit het toevoegen van additionele voorspellende variabelen niet uit [AJZE08c], maar geeft aan dat het raadzaam is hier spaarzaam mee om te gaan en slechts na empirische verkenning een eventuele additionele voorspeller toe te voegen. Hierbij moet wel worden voldaan aan een viertal criteria:

- De voorgestelde additionele voorspeller moet gedragsspecifiek zijn.
- Het moet in overeenstemming zijn met het principe van de TACT elementen.
- Het moet toepasbaar zijn voor uiteenlopende soorten gedrag die bestudeerd worden door sociale wetenschappers.
- De additionele voorspeller moet conceptueel onafhankelijk zijn van de theorie van gepland gedrag.

6.3 Relevantie voor de praktijk

In dit onderzoek is er gekeken vanuit de theorie van gepland gedrag, om een verklarende en voorspellende uitspraak te kunnen doen over de gedragsintentie ten aanzien van informatiebeveiliging. Hierbij is uitgegaan van de drie determinanten attitude toward the behavior, subjective norm en perceived behavioral control die individueel en samen de gedragsintentie beïnvloeden. In de vorige paragraaf is geconcludeerd dat de attitude van een medewerker ten aanzien van de drie gedragsintenties de sterkst verklarende voorspeller is van de drie determinanten (attitude toward the behavior, subjective norm en perceived behavioral control). Attitude toward the behavior en subjective norm zijn de sterkst verklarende voorspellers voor de intentie van een medewerker om zijn bedrijfsgegevens te beschermen en om veilig om te gaan met zijn wachtwoord. Alle drie de determinanten zijn sterke verklarende voorspellers voor de intentie van een medewerker om zijn bedrijfsgegevens zeker te stellen. Middels de behavioral beliefs, normative beliefs, en control beliefs is er een beeld gevormd van de onderliggende cognitieve fundamenten van attitude toward the behavior, subjective norm en perceived behavioral control. Vanuit hier zou een programma ontwikkeld kunnen worden voor gedragsinterventie. Hierbij moet opgemerkt worden dat het alleen gaat om salient beliefs die direct opvraagbaar zijn in het geheugen van een respondent [AJZE06]. In het algemeen geldt dat hoe zwaarder het gewicht is van een belieffactor des te meer dit de gedragsintentie en mogelijk het werkelijke gedrag beïnvloedt [AJZE71]. Het is aanvaardbaar om een gedragsinterventie op elk van de drie determinanten van de theorie van gepland gedrag uit te voeren, zolang er ruimte is voor verandering. Maar het is veiliger om alleen die determinanten te nemen die een significante bijdrage leveren aan de voorspelling van de gedragsintentie. Het uitgangspunt is dat door een gedragsinterventie uit te voeren op de beliefs er daardoor een verandering zal plaatsvinden bij het corresponderende attitude toward the behavior, subjective norm en perceived behavioral control. Als laatste kan het zijn dat de nieuw gevormde gedragsintentie niet wordt omgezet in werkelijk gedrag, waardoor de gedragsinterventie alsnog niet succesvol is. Daarom stelt Ajzen dat het van belang is dat er een sterke verbinding tussen de gedragsintentie en het werkelijke gedrag is [AJZE06].

Uit de resultaten van dit onderzoek kan aangenomen worden dat er een gedragsinterventie op de behavioral beliefs, normative beliefs, en control beliefs en het onderliggende cognitieve fundament attitude toward the behavior, subjective norm en perceived behavioral control uitgevoerd kan worden. Hierbij is gekeken welke belieffactoren de sterkste significante bijdrage leveren aan de voorspelling van de drie gedragsintenties. Vanuit de behavioral beliefs kan gesteld worden dat de attitude van een medewerker ten opzichte van de gedragsintentie om bedrijfsgegevens te beschermen, bedrijfsgegevens zeker te stellen en veilig om te gaan met wachtwoordgebruik de sterkst significante verklarende voorspeller is van de drie determinanten. Hierdoor zal een gedragsinterventie op de behavioral beliefs het hoogste rendement hebben. Vanuit de normative beliefs kan aangenomen worden dat wat naaste collega's, die belangrijk voor een medewerker zijn, vinden dat hij moet doen en wat zij zelf doen ten aanzien van de drie gedragsintenties, een sterke significante verklarende voorspeller is. Hierbij wordt er vanuit gegaan dat belangrijke naaste collega's een voorbeeldfunctie hebben voor de medewerker. Dit rechtvaardigt een gedragsinterventie waarbij naaste collega's, die belangrijk zijn voor een medewerker een prominente rol krijgen. Vanuit de control beliefs kan gesteld worden dat de capaciteit en controle van een medewerker ten aanzien van de drie gedragsintenties en wat een medewerker zelf denkt dat hij kan doen ten aanzien van de drie gedragsintenties de zwakste significante verklarende voorspeller is van de drie determinanten. Hiermee heeft een gedragsinterventie op de control beliefs mogelijk het minste rendement voor een mogelijke gedragsverandering. Voor het ontwikkelen van een mogelijke gedragsinterventie geeft de TpB interventiehandleiding alleen maar algemene richtlijnen [AJZE06]. Hierbij wordt vooral gesteund op de ervaring en creativiteit van een onderzoeker. Het is onduidelijk welke soort van interventie het meest efficiënt zal zijn.

6.4 Enkele kanttekeningen

Bij het interpreteren van de resultaten uit dit onderzoek moet er rekening gehouden worden met enkele beperkingen. Op de eerste plaats is het belangrijk op te merken dat door de cross-sectionele onderzoeksopzet het alleen mogelijk is om verbanden aan te tonen. Daarnaast zijn er nog een aantal beperkingen die hieronder besproken worden.

Op het onderzoek van Stanton e.a. na is dit het eerste onderzoek binnen het vakgebied van de informatiebeveiliging, waarbij de theorie van gepland gedrag tracht het gedrag ten aanzien van informatiebeveiliging te verklaren. Hierbij gaat het dus om resultaten die verdere validatie vereist.

Binnen het onderzoek is het daadwerkelijk gedrag en de actual behavioral control buiten beschouwing gelaten, omdat de gehanteerde onderzoeksopzet en de beschikbare tijd zich niet leende om zowel het daadwerkelijk gedrag als de actual behavioral control te onderzoeken. Aangezien het zeer moeilijk is om de actual behavioral control te meten is in dit onderzoek, net zoals in vele andere onderzoeken, gebruik gemaakt van perceived behavioral control als een proxy voor actual behavioral control [AJZE08].

Bij de analyse is voorbij gegaan aan de onderlinge verklarende variatie tussen attitude toward the behavior, subjective norm en perceived behavioral control. Hierdoor is het mogelijk dat een deel van de verklarende en voorspellende waarde toegeschreven wordt aan de onderlinge relaties tussen attitude toward the behavior, subjective norm en perceived behavioral control.

Het gedrag ten aanzien van informatiebeveiliging is, vanwege de complexiteit, in zeer beperkte maat geoperationaliseerd. Slechts drie specifieke gedragsintenties ten aanzien van informatiebeveiliging zijn onderzocht. Hierbij is maar een klein stuk van de informatievoorziening als geheel onderzocht, waarop een betrekkelijk aantal gedragingen van toepassing zijn. Daartegenover staat dat het betrekkelijk aantal gedragingen middels een omvangrijk hoeveelheid items, betrouwbaar en gedetailleerd gemeten is.

De interne consistentie van de indirecte metingen zijn niet gevalideerd middels Test-Retest Reliability. Hiervoor zouden meerdere metingen moeten plaatsvinden, waarbij dezelfde vragenlijst door dezelfde respondenten op verschillende tijdsintervallen beantwoord zouden moeten worden [AJZE06]. Om de interne consistentie van de indirecte metingen toch te valideren zijn er bivariate correlaties berekend tussen de directe en indirecte metingen van hetzelfde component. Hierbij is vastgesteld dat alle interne directe en indirecte metingen correleren tussen de .357 en .651. Dit betekent dat de directe en indirecte metingen op elkaar lijken maar toch op bepaalde punten van elkaar verschillen.

Er is voor het ontwikkelen van de vragenlijst uitgegaan van een theoretische en pragmatische veronderstelling vanuit het vakgebied van de informatiebeveiliging. Er is bij deze meta-analyse voorbij gegaan aan het inventariseren van personal salient beliefs of modal salient beliefs. Het effect dat hierdoor zou kunnen optreden is dat respondenten antwoorden gaan geven op vragen waarvoor geen antwoord beschikbaar is. Maar uit de resultaten blijkt dat iets meer dan 50% van de potentiële respondenten zijn gestopt na minimaal 11 en maximaal 70 vragen. Dus mensen hebben uit vrije wil de vragen beantwoord, zonder dat hiervoor een straf of beloning tegenover stond. Het gevolg hiervan zou kunnen zijn dat er een selectieve groep van respondenten ontstaat die betrokken is bij het onderwerp. Dit zijn maar speculaties die niet zijn bewezen.

De generalisatie van de resultaten naar de vier onderscheiden branches stuit op problemen. De onderzoeksgroep is waarschijnlijk selectief samengesteld en de verdeling ervan is scheef: hightech industrie 4,81%, overige industrie 4,33%, kennisintensieve dienstverlening 57,21% en overige

dienstverlening 33,65%. Een mogelijke verklaring voor deze verdeling is dat het onderwerp van dit onderzoek meer aandacht krijgt binnen de dienstverlening, dan binnen de industrie.

6.5 Suggesties voor toekomstig onderzoek

Suggesties voor toekomstig onderzoek worden opgesplitst in twee soorten. Enerzijds zullen er suggesties gedaan worden voor mogelijk onderzoek aan de hand van de verzamelde gegevens uit dit onderzoek, aangezien de dataset maar gedeeltelijk is gebruikt. Anderzijds zullen een aantal ideeën omtrent nieuwe dataverzameling gedaan worden. Aan de hand van de verzamelde gegevens kan onderzocht worden wat de invloed is van het wel of niet zijn van een manager. Hierbij zou sprake kunnen zijn van een hogere of lagere risicotolerantie en risicoperceptie voor de gedragsintentie ten aanzien van informatiebeveiliging. Daarnaast zouden geslacht, leeftijd, branche, werkervaring en IT-ervaring onderzocht kunnen worden, als verstorende variabelen tussen de afhankelijke en onafhankelijke variabelen uit de theorie van gepland gedrag. Als laatste zouden de onderlinge invloeden van de drie determinanten (attitude toward the behavior, subjective norm en perceived behavioral control) onderzocht kunnen worden.

De gebruikte dataset heeft echter ook beperkingen waarvoor enkele suggesties voor vervolgonderzoek worden gedaan aan de hand van nieuwe dataverzameling. Er zou bijvoorbeeld onderzocht kunnen worden wat de invloed is van de gedragsintentie op het daadwerkelijk gedrag en welke rol actual behavioral control daarbij speelt. Dit is relevant om te weten aangezien het zo kan zijn dat een persoon de intentie heeft om bijvoorbeeld back-ups te maken, maar dat dit niet gedaan wordt, omdat bepaalde factoren (bijvoorbeeld werkdruk, het ontbreken van procedures, enzovoorts) dit niet toelaten. Wanneer er in longitudinaal onderzoek zowel het daadwerkelijk gedrag en de actual behavioral control worden onderzocht, zal de voorspellende betrouwbaarheid van het gedrag ten aanzien van informatiebeveiliging waarschijnlijk toenemen. De potentiële additionele voorspellende variabele motivatie zou onderzocht kunnen worden met de vraag of er bij gedrag ten aanzien van informatiebeveiliging sprake is van werkintrinsieke- en werkextrinsieke motieven. Daarnaast zou gekeken kunnen worden of de waarde van de opbrengsten die men wil bereiken en de verwachtingen dat die opbrengsten het gevolg zullen zijn van de inspanning die men levert, aanwezig zijn bij gedrag ten aanzien van informatiebeveiliging. Hierdoor zou duidelijk moeten worden welke rol werkmotivatie speelt ten opzichte van gedragsintentie ten aanzien van informatiebeveiliging. Het Pareto optimum zou mogelijk toepasbaar kunnen zijn voor alle soorten van gedrag ten aanzien van informatiebeveiliging, waarbij 20% van de gedragingen ten aanzien van informatiebeveiliging 80% van de informatiebeveiligingsincidenten veroorzaken. Van de 93 gedragingen van Stanton zouden de 20% cruciale gedragingen geabstraheerd kunnen worden middels een incidentenonderzoek. Hierbij zouden vervolgens de personal salient beliefs of modal salient beliefs geïnventariseerd kunnen worden. Hierbij kunnen deze aan de hand van de theorie van gepland gedrag worden onderzocht. Hierdoor kan een compleet beeld van voorspellende waarde gegeven worden voor de gedragingen ten aanzien van informatiebeveiliging. Voor de drie verschillende gedragsintenties beschreven in dit onderzoek, zouden de personal salient beliefs of modal salient beliefs geïnventariseerd kunnen worden. Door vervolgens dit onderzoek te herhalen met hetzelfde steekproefkader maar met een operationalisatie op basis van de personal salient beliefs of modal salient beliefs, zouden de resultaten van dit onderzoek gevalideerd kunnen worden. Daarnaast zou er onderzocht kunnen worden wat de invloed is van de emotionele aspecten ten aanzien van de theorie van gepland gedrag. Als laatste geeft Verplanken aan dat routines en gewoontes opgevat kunnen worden als een mentaal construct dat ingaat op het automatisch gedrag [VERP06]. Het effect van routines en gewoontes zouden als een mentaal construct onderzocht kunnen worden om na te gaan wat de invloed hiervan is op de voorspelbaarheid van de theorie van gepland gedrag voor gedrag ten aanzien van informatiebeveiliging.

7. LITERATUURLIJST

[AART98] Aarts, H., Verplanken, B., van, Knippenberg, A., Predicting behavior from actions in the past: Repeated decision making or a matter of habit?, *Journal of Applied Social Psycholog*, vol. 28, pp. 1355-1374, 1998.

[AJZE71] Ajzen, I., Attitudinal vs. normative messages: An investigation of the differential effects of persuasive communications on behavior. Sociometry, vol. 34, pp. 263-280, 1971.

[AJZE85] Ajzen, I., *From intentions to actions: A theory of planned behavior*, Springer, Berlin/ New York, 1985.

[AJZE88] Ajzen, I., Attitudes, personality, and behavior*,* Open University Press, Milton Keynes, 1988.

[AJZE91] Ajzen, I., The theory of planned behavior, *Organizational Behavior and Human Decision Processes*, vol. 50, pp. 179-211, 1991.

[AJZE02] Ajzen, I., Constructing a TpB Questionnaire: Conceptual and Methodological Considerations, TpB Guide, University of Massachusetts, 2002.

[AJZE06] Ajzen, I., Designing a TpB Intervention, TpB Guide, University of Massachusetts, 2006.

[AJZE08] Ajzen, I., Theory of Planned Behavior, Home page – 08-10-2008: http://people.umass.edu/aizen/faq.html, 2008.

[AJZE70] Ajzen, I., & Fishbein, M., The prediction of behavior from attitudinal and normative variables, *Journal of Experimental Social Psychology*, vol. 6, pp. 466-487, 1970.

[AJZE73] Ajzen, I., & Fishbein, M., Attitudinal and normative variables as predictors of specific behaviors, *Journal of Personality and Social Psychology*, vol. 27, pp. 27, 41-57, 1973.

[AJZE77] Ajzen, I., & Fishbein, M., Attitude-behavior relationships: a theoretical analysis and review of empirical research, *Psychological Bulletin*, vol. 84, pp. 888-918, 1977.

[AJZE80] Ajzen, I., & Fishbein, M., *Understanding attitudes and predicting social behavior*, Prentice Hall, Englewood Cliffs, 1980.

[AJZE08a] Ajzen, I., & Fishbein, M., Scaling and testing multiplicative combinations in the expectancy-value model of attitudes, *Journal of Applied Social Psychology*, vol. 38, pp. 2222-2247, 2008.

[AJZE08b] Ajzen, I., & Gilbert Cote, N., Attitudes and the prediction of behavior. In W. D. Crano & R. Prislin (Eds.), *Attitudes and attitude change*, pp. 289-311, Psychology Press, New York, 2008

[ALBA01] Albarracin, D., Johnson, B.T., Fishbein, M., & Muellerleile, P.A. Theories of reasoned action and planned behavior as models of condom use: A meta-analysis, *Psychological Bulletin*, vol. 127, pp. 142-161, 2001.

[ALBL05] Alblas, G., & Wijsman, E., *Gedrag in organisaties*, Wolters Noordhoff, Groningen, 2005.

[ALDE72] Alderfer, C.P., *Existence, relatedness and growth: Human needs in organizational setting*, The Free Press, New York, 1972.

[ARMI01] Armitage, C.J., & Conner, M., Efficacy of the theory of planned behavior: A meta-analytic review, *British Journal of Social Psychology*, vol. 40, pp. 471-499, 2001.

[BAND77] Bandura, A., *Social learning theory*, Prentice Hall, Englewood Cliffs, 1977.

[BAND86] Bandura, A., *Social foundations of thought and action: A social cognitive theory*, Englewood Cliffs, Prentice-Hall, New York, 1986.

[BAND99] Bandura, A., *Social cognitive theory of personality,* In: L. Pervin & O. John (Eds.), Handbook of personality, Guilford Publications, New York, 1999.

[BARO86] Baron, R.M., Kenny, D.A., The moderator-mediator variable distinction in social psychological research: Conceptual, strategic and statistical considerations, *Journal of Personality and Social Psychology*, vol. 51, pp. 1173-1182, 1986.

[BAST03] Basten, N.F.H., *Security awareness*, Informatiebeveiligingsjaarboek 2003/2004, ten Hage & Stam uitgevers, Den Haag, 2003.

[BERN94] Bernstein, D.A., Clarke-Stewart, A., Roy, E.J., Srull T.K., & Wickens, C.D., *Psychology*, Houghton Mifflin Company, Boston, 1994.

[BIBE07] Biber-Klever, L.G., Informatieverwerking, *Informatiebeveiliging*, Juni, 2007.

[BOSC04] Bosch, L. van den,. Hofman, A., & Hoogenboom, M.C., *Onbewust maakt onbeken*, Informatiebeveiligingsjaarboek 2004/2005, ten Hage & Stam uitgevers, Den Haag, 2004.

[BRAT07] Bratton, J., Callinan, M., Forshaw, C., & Sawchuk., P., *Work and organizational behaviour: understanding the workplace*, Palgrave Macmillan, Basingstoke, 2007.

[COHE03] Cohen, J., Cohen, P., West, S.G., Aiken, L.S., *Applied multiple regression / correlation analysis for the behavioral sciences*, New York: Erlbaum, Mahwah, 2003.

[CVIB02] Nederlands Normalisatie-instituut, *Code voor informatiebeveiliging*, Delft, 2002.

[DAVI89] Davis, F. D., Perceived usefulness, perceived ease of use, and user acceptance of information technology, *MIS Quarterly*, 319-339, 1989.

[DIGM90] Digman. J.M, Personality structure: Emergence of the five factor model, *Annual Review of Psychology,* vol. 41, pp. 417-440, 1990.

[FEST57] Festinger, L., *Theory of cognitive dissonace*, Stanford University Press, Stanford, 1957.

[FISH67] Fishbein, M. *Attitude and the prediction of behavior* In: M. Fishbein (Ed.) Readings in attitude theory and measurement, Wiley, New York, 1967.

[FISH75] Fishbein, M., & Ajzen, I. *Belief, attitude, intention, and behavior: An introduction to theory and research,* MA: Addison - Wesley, Reading, 1975.

[FISH76] Fishbein, M., *The prediction of behaviors from attitudinal variables*, Harper & Row, New York, 1976.

[FRAN04] Francis, J., Eccles, M., Johnston, M., Walker, A., Grimshaw, J., Foy, R., Kaner, E., Smith, L., Bonetti, D., CONSTRUCTING QUESTIONNAIRES BASED ON THE THEORY OF PLANNED BEHAVIOUR: *A MANUAL for HEALTH SERVICES RESEARCHERS*, University of Newcastle, Newcastle, 2004.

[FRIJ93] Frijda, N., Moods, *Emotion episodes and Emotions*, In: Lewis, M., Haviland, J.M. (Eds.), Handbook of emotions, Guilford press, pp. 381-403, New York, 1993.

[GEOR96] George, J., *Trait ans State affect*, In: K. Murphy (Ed.), Individual differences and behavior in organizations, vol. 16, pp. 145, Jossey-Bass, San Francisco, 1996.

[GIGE99] Gigerenzer, G., Todd, P., *Simple Heuristics that Make us Smart*, Oxford University Press, New York, 1999.

[GRUM90] Grumbkow, J. von, Arbeids- en organisatieprychologie, Open Universiteit, Heerlen, 1990.

[HAGG02] Hagger, M.S., Chatzisarantis, N.L.D., & Biddle, S.J.H., A meta-analytic review of the theories of reasoned action and planned behavior in physical activity: Predictive validity and the contribution of additional variables, *Journal of Sport and Exercise Psychology*, vol. 24, pp. 3-32, 2002.

[HARD94] Hardonk, M., Controle van gedrag, *Nederlands tijdschrift voor de psycholgie*, vol. 49, pp. 193-207, 1994.

[HAVE00] Have, S., *Binding en motivatie. Acht adviezen voor employment marketing*, Nieuwezijds: Amsterdam, 2000.

[HEID82] Heider, F., *The Psychology Of Interpersonal Relations*, Wiley, New York, 1982.

[HERZ59] Herzberg, F., Mausner, B., & Snyderman, B., *The motivation to work*, John Wiley & Sons, New York, 1959.

[HITT05] Hitt, M., Black, J., & Porter, L., *Management*, Pearson Prentice Hall, New Jersey, 2005.

[HOCH79] Hochschild, A.R., Emotions Work, Feeling Rules, and Social Stracture, *American journal of Sociology*, vol. 85, pp. 551-575, 1979.

[HOFL05] Hofland, V.L., Bewust van informatiebeveiliging, Master Thesis, TU Delft, 2005.

[INFO91] Information Security Forum, Security Status Survey 1991: IT Security Awareness, Information Security Forum, Londen, 1991.

[INFO93] Information Security Forum, Implementation Guide: How To Make Your Organisation Aware Of IT Security, Information Security Forum, Londen, 1993.

[INFO00] Information Security Forum, Information Security Culture: A preliminary investigation, Information Security Forum, Londen, 2000.

[INFO02] Information Security Forum, Effective Security Awareness, Information Security Forum, Londen, 2002.

[INTE05] International Standards Organization, Information technology — Security techniques — Code of practice for information security management, Geneva, 2005.

[ISMH04] Tipton, H., & Krause, M., *Information Security Management Handbook*, Auerbach publications, Florida, 2004.

[JACO07] Jacobs, B.P.F., *De Menselijke Maat in ICT*, Home page – 16-02-2008: http://www.cs.ru.nl/B.Jacobs, Nijmegen, 2007.

[JANS02] Jansen, P.G.W., *Organisatie en mensen : inleiding in de bedrijfspsychologie voor economen en bedrijfskundigen*, Nelissen, Soest, 2002.

[JENT04] Jentjens, V.L.M., & Graaf, M.C. de, *Geïntegreerde informatiebeveiliging : de sleutel tot succesvolle implementatie*, Lemma, Utrecht, 2004.

[JUDD81] Judd, C. M., Kenny, D. A., Process analysis: Estimating mediation in treatment evaluations, *Evaluation Review*, vol. 5, pp. 602-615, 1981.

[KAHN73] Kahnemann, D., *Attention and effort*, Englewood Cliffs, Prentice Hall, New York, 1973.

[KATZ78] Katz, D., & Kahn, R. L., *The social Psychology of organizations*, Wiley, New York, 1978.

[KELL72] Kelley H., *Causal schemata and attribution process*, General learning press, Morristow, 1972.

[KEUN91] Keuning, D., & Eppink, D. J., *Management en organisatie: Theorie en toepassing*, Stenfert Kroese, Leiden, 1991.

[KILL06] Killmeyer, J., *Information security architecture: an integrated approach to security in the organization*, Auerbach Publ, London, 2006.

[KNIP94] Knippenberg, A. van, & Siero, F., W., *Multivariate analyse: Beknopte inleiding en toepassingen*, Bohn Stafleu Van Loghum, Houten, 1994.

[KOMP04] Kompier, M.A.J., & Houtman, I.L.D., *Mentale werkbelasting.* In P., Voskamp, P.A.M., van Scheijndel, K.J., Peereboom, Handboek Ergonomie, Kluwer, Alphen aan den Rijn, 2004.

[KOOT06] Koot, A., & Haas, J. de, Organisaties overschatten niveau van awareness, *Informatiebeveiliging*, Juli, pp. 30-33, 2005.

[KRUG06] Krugera, H.A., & Kearney, W.D., A prototype for assessing information security awareness, Elsevier Ltd., *computers & security*, vol. 25, pp. 289-296, 2006.

[LAZA84] Lazarus, R.S., On the primacy of cognition, *American Psycologist*, vol. 39, pp. 222-223, 1984.

[LEAC03] Leach, J., Improving user security behaviour, Elsevier Ltd., *Computers & Security*, vol. 22, pp. 685-692, 2003.

[LIKE32] Likert, R., A Technique for the Measurement of Attitudes, *Archives of Psychology*, vol. 140, pp. 1-55, 1932.

[LOCK84] Locke, E., A., & Latham G., P., *Gole setting: Amotivational technique that works*, Prentice-Hall, Englewood-Cliffs, 1984.

[LOOI04] Looijen, M., *Beheer van informatiesystemen*, Ten HageStam, Den Haag, 2004.

[LUTH84] Luthans, F., & Kreitner, R., *Organizational Behavior Modification and Beyond*, Foresman, Glenview, 1984.

[MACK93] Mac Kinnon, D. P., Dwyer, J. H., Estimating mediated effects in prevention studies, *Evaluation Review*, vol. 17, pp. 144 - 158, 1993.

[MADD92] Madden, T.J., Ellen, P.S., & Ajzen, I., A comparison of the theory of planned behavior and the theory of reasoned action, *Personality and Social Psychology Bulletin*, vol. 18, pp. 3-9, 1992.

[MAGN04] Magnée E., & Schippers, H., De strategische betekenis van informatiebeveiliging, *de EDP-Auditor*, vol. 2, pp. 11-23, 2004.

[MASL54] Maslow, A., *Motivation and personality*, Harper & Row, New York, 1954.

[MATH04] Mathisen, J., Measuring Information Security Awareness, Master Thesis, Gjøvik University College Oslo, 2004.

[MCCL61] McClelland, D., *The achieving society*, Van Nostrand, Princeton, 1961.

[MCGR60] McGregor, D., *The Human Side of Enterprise*, McGraw- Hill, New York, 1960.

[MITN02] Mitnick, K., Simon, W., Wozniak, S., *The art of deception,* Wiley, 2002.

[MOOR04] Moore, D.S. & McCabe, G.P., *Introduction to the practice of statistics*, Freeman, New York, 2004.

[NEN7510] Algemeen Nederlands normalisatie-instituut, *NEN 7510 Medische informatica – Informatiebeveiliging in de zorg De code voor informatiebeveiliging voor de zorgsector*, Delft, 2004.

[NEYS03] Neys, C., IT'ers, regels en Security Awareness, Referaat postdoctorale opleiding MSIT, TU Eindhoven, 2003.

[NEYS04] Neys, C., & Schaaf, T. van der, Grip op de factor mens, *Informatiebeveiliging*, December, pp. 8-12, 2004.

[NGI92] Nederlands Genootschap voor Informatica Afdeling Beveiliging, *Risico-analyse en risicomanagement*, Kluwer Bedrijfswetenschappen, Amsterdam, 1992.

[NIST98] Wilson, M., et al., Information Technology Security Training Requirements: A Role- and Performance-Based Model, National Institute of Standards and Technology, Gaithersburg, 1998.

[NIST03] Wilson M., & Hash, J., *Building an Information Technology Security Awareness and Training Program*, National Institute of Standards and Technology, Gaithersburg, 2003.

[OSGO57] Osgood, C.E., Suci, G.J., & Tannenbaum, P.H., *The measurement of meaning*, University of Illinois Press, Urbana, 1957.

[OVER05] Overbeek, P.L., Roos Lindgreen, E., Spruit, M.E.M., *Informatiebeveiliging onder controle*, Pearson Education: Financial Times / Prentice Hall, Amsterdam, 2005.

[PRAA02] Praat J. van, & Suerink, H., *Inleiding EDP-auditing*, Ten Hagen Stam, Den Haag, 2002.

[RASM83] Rasmussen, J., Skills, rules, knowledge; signals, signs, and symbols, and other distinctions in human performance models, *IEEE Transactions on Systems*, Man and Cybernetics, vol. 13, pp. 257-266, 1983.

[RASM86] Rasmussen, J., *Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering*, North-Holland Series in System Science and Engineering, Elsevier Science Ltd, Amsterdam, 1986.

[RASM97] Rasmussen, J., Risk management in a dynamic society: a modeling problem, *Safety Science*, vol. 27, pp. 183-213, 1997.

[REAS90] Reason, J.T., *Human error*, Cambridge University Press, Cambridge, 1990.

[ROBB02] Robbins, S.P.*, Gedrag in organisaties*, Prentice Hall, Amsterdam, 2002.

[ROBB08] Robbins, S.P., & Judge, T. A., *Essentials of organizational behavior*, Pearson/Prentice Hall, Upper Saddle River, 2008.

[ROE91] Roe, R.A., & Zijlstra, F.H.R, *Arbeidsanalyse ten behoeve van (her)ontwerp van functies: een handelingstheoretische invalshoek*, In: Algera, J.A., Analyse van arbeid vanuit verschillende perspectieven, Swets & Zeitlinger, Amsterdam / Lisse, 1991.

[ROED98] H.L. Roediger, E. Deutsch Capaldi, S.G. Paris, J. Polivy, C.P. Herman, *Inleiding psychologie*, Academia Press, 1998.

[SCHO99] Schomaker, P., Wie bindt, die wint. Een onderzoek naar de mate van commitment (binding) van werknemers van Writers & Rogers Accountants, Proefschrift, Radboud Universiteit Nijmegen, 1999.

[SCHN08] Schneier, B., The Psychology of Security, Home page – 18-03-2008: http://www.schneier.com/essay-155.html, 2008.

[SHAI06] Shaikh, A.A., An Investigation into the Corporate Security Awareness and Training Program, Master Thesis, HANKEN-Swedish School of Economics and Business Administration Helsinki, 2006.

[SHEE02] Sheeran, P. Intention-behavior relations: A conceptual and empirical review. In W. Stroebe & M. Hewstone (Eds.), *European review of social psychology*, vol. 12, pp. 1-36, 2002.

[SHEE99] Sheeran, P., & Taylor, S. Predicting intentions to use condoms: A meta-analysis and comparison of the theories of reasoned action and planned behavior, *Journal of Applied Social Psychology*, vol. 29, pp. 1624-1675, 1999.

[SHEP88] Sheppard, B.L., Hartwick, J. & Warshaw, P.R., The theory of reasoned action: a metaanalysis of past research with recommendations for modifications and future research, *Journal of Consumer Research*, vol. 15, pp. 325-343, 1988.

[SKIN71] Skinner B.F., *Contingencies of Reinforcement*, Appleton Century Crofts, East Norwalk, 1971.

[SPEE04] Spee, A.J.A.M., Insider threat in IT (de factor mens beschouwd), Referaat postdoctorale opleiding IT auditing, Erasmus Universiteit Rotterdam, 2004.

[SPRU04] Spruit, M.E.M., *Informatiebeveiliging en bewustzijn*, Informatiebeveiliging Jaarboek 2004/2005, Ten Hagen en Stam, Den Haag, 2004.

[STAN03a] Stanton, J.M., Caldera, C., Isaac, A., Stam, K. R., & Marcinkowski, S.J., Behavioral Information Security: Defining the Criterion Space, Research paper, Syracuse University: School of Information Studies, New York, 2003.

[STAN03b] Stanton, J.M., Behavioral Information Security - Brief Overview, Symposium presentation, Syracuse University: School of Information Studies, New York, 2003.

[STAN03c] Stanton, J.M., Stam, K.R., Guzman, I., & Caldera, C., Examining the linkage between organizational commitment and information security. Proceedings of the IEEE Systems, Man, and Cybernetics Conference, Washington, 2003.

[STAN04] Stanton, J.M., Stam, K.R., Jolton, J., & Mastrangelo, P.R., Behavioral Information Security: Two End User Survey Studies of Motivation and Security Practices, Proceedings of the Tenth Americas Conference on Information Systems, New York, 2004.

[STAN05a] Stanton, J.M., Stam, K.R., Mastrangelo, & Jolton, J., An analysis of end user security behaviors. *Computers & Security*, vol. 24, pp. 124-133, 2005.

[STAN05b] Stanton, J.M., Stam, K.R., & Yamodo-Fagnot, I., The Madness of Crowds: Employees Beliefs about Information Security in Relation to Security Outcomes, Submitted for consideration to the 2005 Security Conference, Syracuse University: School of Information Studies, Las Vegas, 2005.

[STAN06] Stanton, J.M., *The visible employee : using workplace monitoring and surveillance to protect information assets - without compromising employee privacy or trust,* Information Today, Medford, 2006.

[STAR02] Starreveld, R.W., van Leeuwen, O.C., en van Nimwegen, H., *Bestuurlijke informatieverzorging, deel 1: Algemene grondslagen*, Stenfert Kroese, Groningen/Houten, 2002.

[SUTT03] Sutton, S., French, D.P., Hennings, S.J., Mitchell, J., Wareham, N.J., Griffin, S., Hardeman, W., Kinmonth, A.L., Eliciting salient beliefs in research on the theory of planned behavior: the effect of question world, *Current Psychology: Developmental, Learning, Personality, Social*, vol. 22, pp. 234-251, 2003.

[TETT95] Tettero, O., & Out, D.J., Gesloten of gestolen: Informatiebeveiliging van nu tot 2000, Telematica Research Centrum, Enschede, 1995.

[THAN06] Thangarajan, S.A., IT security awareness in the Indian ICT sector, Master Thesis, Stockholm University / Royal Institute of Technology, 2006.

[THOM06] Thomson, K., & Solms, R. von, *Towards an Information Security Competence Maturity Model*, Elsevier Ltd., Computer Fraud & Security, vol. 25, pp. 11-15, 2006.

[TVER81] Tversky A., & Kahneman D., The Framing of Decisions and the Psychology of Choice, *Science*, vol. 211, pp. 453-458, 1981.

[VECC84] Vecchio, R.P., Mode of Psygological Inequity, *Organizational Behavior and Human Performance*, 266-282, 1984.

[VEEN94] Veerman, M., Intelligentie en probleemaanpak, *De psycholoog*, vol. 29, pp. 223-228, 1994.

[VENK03] Venkatesh, V., Morris, M.G., Davis, G.B., & Davis, F.D., User acceptance of information technology: Toward a unified view. *MIS Quarterly*, vol. 2, pp. 425-478, 2003.

[VERP06] Verplanken, B., Beyond frequency: Habit as mental construct, *British Journal of Social Psychology*, vol. 45, pp. 639-656, 2006.

[VERP98] Verplanken, B., Aarts, H., Knippenberg, A., Moonen, A., Habit versus planned behavior: A field experiment, *British Journal of Social Psychology*, vol. 37, pp. 111-128, 1998.

[VOET04] Voeten, M.J.M., Bercken, J.H.L. van den, Regressieanalyse met SPSS: Een handleiding voor lineaire regressieanalyse met SPSS, Radboud Universiteit Nijmegen, 2004.

[VOGE90] Vogelaar, A.L.W., Arbeidssatisfactie, een gevolg van behoeftenstructuur en kenmerken van werk en werksituatie, Proefschrift, Rijksuniversiteit Leiden, 1990.

[VRIE88] Vries, H. de, Dijkstra, M., Kuhlman, P., Self-efficacy: the third factor besides attitude and subjective norm as a predictor of behavioural intentions, *Health education research*, vol. 3, pp. 273-282, 1988.

[VROO64] Vroom, V.H., *Work and Motivation*, Wiley, New York, 1964.

[WAGE89] Wagenaar, W.A., *Vergissen*. In: J. van der Leijden Sr., Psychologische functieleer, Bohn Stafleu Van Loghum, Houten, 1989.

[WEIS96] Weiss, H.M., & Cropanzano, R., Affective Events Theory, *Research in Organizational Behavior*, vol. 18, pp. 17-19 en pp. 20-22, JAI Press, Greenwich, 1996.

[WYLD04] Wylder J., *Strategic Information Security*, Auerbach Publications, New York, 2004.

8. BIJLAGEN

8.1 Bijlage Employee Security-Related Behavior List

Tabel 47
Employee Security-Related Behavior List

Employee Security-Related Behavior List		
Employee Security-Related Behavior	*Expertise Needed*	*Likely Intentions*
1. Employee transmitted a harassing message using the company's e-mail	Lower	Negative
2. Employee harassed a colleague by sending many, lengthy pager messages	Lower	Negative
3. Someone pretending to be a systems administrator called and said there was a problem with his account and asked for his password, which employee gave with no verification of the caller's credentials	Lower	Negative
4. Employee provided information or a list of staff members to someone outside the organization	Lower	Negative
5. Employee sent an obscene joke using company e-mail	Lower	Negative
6. Employee copied and distributed copyrighted material including digitizing photographs from magazines and books	Lower	Negative
7. Employee sent a harassing e-mail to someone in her company from an anonymous outside e-mail account	Lower	Negative
8. Employee sold cosmetics with the use of the company e-mail system	Lower	Negative
9. Employee used the Internet for activities that interfered with her work-related productivity	Lower	Negative
10. Employee forwarded a chain letter that contained a "pyramid" (get rich quick) scheme	Lower	Negative
11. Employee chose a password that was "1234".	Lower	Negative
12. Employee transferred a lot of files to a personal notebook computer that got stolen	Lower	Negative
13. Employee left confidential data out on his desk at night	Lower	Negative
14. Employee shared her company access codes with others in her family so that they could use her high speed Internet connection	Lower	Negative
15. Employee played network games on the company's computers	Lower	Negative
16. Employee sent e-mail from someone else's account	Lower	Negative
17. Employee sent unsolicited e-mail messages in the form of "junk mail" advertising material to individuals who did not specifically request such material	Lower	Negative
18. Employee did not change her password for over two years	Lower	Negative
19. Employee shared her account information with a friend	Lower	Negative
20. Employee wrote her password on a sticky tape and put it on her monitor	Lower	Negative
21. Employee taped his password to the bottom of his keyboard	Lower	Negative

22. Employee used his social security number as a password	Lower	Negative
23. Employee transmitted her personal opinions about politics on the company's group collaboration tool	Lower	Hard to tell
24. Employee sent out e-mails in order to compile a list of others' e-mail addresses.	Lower	Hard to tell
25. Employee chose an easily guessable password.	Lower	Hard to tell
26. Employee questioned the need and applicability of organizational security policies.	Lower	Hard to tell
27. Employee complained about the inconvenience of organizational security policies to his boss.	Lower	Hard to tell
28. Employee told customers over the phone that they could rest assured that hackers would not steal their customer information.	Lower	Hard to tell
29. Employee followed the terms of a software license.	Lower	Positive
30. Employee signed compliance statements after review of information security policies.	Lower	Positive
31. Employee changed her password every six months.	Lower	Positive
32. Employee signed all the way out to the sign-out screen whenever he left his desk.	Lower	Positive
33. Employee notified an appropriate administrator when she copied organizational information resources for use in off-site work (e.g., at client site, business trip).	Lower	Positive
34. Employee logged off whenever he left his cubicle.	Lower	Positive
35. Employee shredded her old paper documents.	Lower	Positive
36. Employee locked her tapes, disks, and documents in a file cabinet when she was away from her desk.	Lower	Positive
37. Employee refused to release non-public company data/information to a reporter.	Lower	Positive
38. Employee accessed files that she should not have had access to by using a colleague's user ID because she wanted to avoid filling out the paperwork to increase her access level.	Middle	Negative
39. Employee accessed data for which she was not an intended recipient.	Middle	Negative
40. Employee mailed an encryption software CD to a foreign country in violation of international or regional export control laws.	Middle	Negative
41. Employee posted a cartoon containing an ethnic slur on the company's internal Web site.	Middle	Negative
42. Employee used the company's information resources for personal commercial profit.	Middle	Negative
43. Employee distributed someone else's copyrighted materials using the company's network.	Middle	Negative
44. Employee used an unauthorized file-sharing program on a company computer without written consent from the relevant authority.	Middle	Negative
45. Employee installed pirated software.	Middle	Negative
46. Employee loaded an unauthorized application onto her PC.	Middle	Negative
47. Employee created and mailed a chain letter containing a "pyramid" (get rich quick) scheme.	Middle	Negative

48. Employee installed some software from a CD and didn't know where the CD came from or who wrote the software.	Middle	Negative
49. Employee installed shareware with a restricted license agreement on her company PC and did not pay the shareware fee.	Middle	Negative
50. Employee installed some software on his PC for which the company did not have a license.	Middle	Negative
51. Employee exchanged digital movies and songs (peer-to-peer sharing of files) using company equipment.	Middle	Negative
52. Employee mistakenly introduced a malicious worm program into the network.	Middle	Negative
53. Employee used unsolicited e-mail to advertise a service offered by the organization.	Middle	Hard to tell
54. Employee used her company PC to post non-business-related messages to large numbers of Usenet newsgroups.	Middle	Hard to tell
55. Employee used a modem to dial out to the Internet from a computer connected to a secure LAN.	Middle	Hard to tell
56. Employee constructively criticized organizational security policies to her boss.	Middle	Positive
57. Employee obtained authorization for the connection of his portable computer with an appropriate system administrator.	Middle	Positive
58. Employee released sensitive data to other staff only on a need-to-know basis.	Middle	Positive
59. Employee activated his screensavers with password protection to protect his data when left unattended.	Middle	Positive
60. Employee backed up her data on a regular basis.	Middle	Positive
61. Employee used excellent access codes (passwords and usernames) and changed them periodically.	Middle	Positive
62. Employee reported a discovered security vulnerability to the appropriate authorities.	Middle	Positive
63. Employee intentionally introduced a Trojan horse program into the network.	Higher	Negative
64. Employee used a file decryption program to discover the contents of a file containing trade secrets.	Higher	Negative
65. Employee forged routing information to make it seem like someone else had sent some packets.	Higher	Negative
66. Employee forged her e-mail header information to make it look like her boss had sent a message.	Higher	Negative
67. Employee logged into a server account he was not expressly authorized to access.	Higher	Negative
68. Employee deleted a colleague's account information so that he would not be able to access his files.	Higher	Negative
69. Employee intentionally put a logic bomb in her code.	Higher	Negative
70. Employee built a special script that disabled another user's terminal session.	Higher	Negative
71. Employee used the company's information resources to help a colleague erase her performance reviews.	Higher	Negative
72. Employee created a denial of service attack on a competitor's Web site using the company's computers.	Higher	Negative
73. Employee created a security breach by disrupting network communications.	Higher	Negative

74. Employee used a "ping flood" attack to see what would happen to the company's network.	Higher	Negative
75. Employee turned off the user authentication function on the console of a Web host system.	Higher	Negative
76. Employee found and saved trade secret information about other companies using the Internet.	Higher	Negative
77. Employee brought a wire1ess gateway device into his office and installed it on the network without authorization.	Higher	Negative
78. Employee encrypted some of her files even though this was against company policy.	Higher	Negative
79. Employee set up a network monitoring device, which intercepted data not intended for his system, to asses show well the network was running.	Higher	Hard to tell
80. Employee set up a packet spoofing application just to test out her programming ability.	Higher	Hard to tell
81. Employee used a "steganography" software tool to store organizational information in a JPEG file.	Higher	Hard to tell
82. Employee attached a modem to her office computer so that she could dial in from home and do work.	Higher	Hard to tell
83. Employee used an intrusion detection program on the company's network even though that was not part of his job.	Higher	Hard to tell
84. Employee used a password-cracking program to unlock a file for which a colleague had lost the password.	Higher	Hard to tell
85. Employee used a port-scanning program to look for vulnerabilities on company computers even though this was not part of her job.	Higher	Hard to tell
86. Employee used a network sniffer to diagnose a problem with the company's network.	Higher	Positive
87. Employee removed access rights data from a user who was leaving the company.	Higher	Positive
88. Employee scanned his files and software for malicious code prior to execution.	Higher	Positive
89. Employee taught others about appropriate and acceptable user policies within the organization.	Higher	Positive
90. Employee participated in advanced security training designated by the organization.	Higher	Positive
91. Employee conducted random/periodic auditing of different departments' security status.	Higher	Positive
92. Employee attended a training program to become familiar with indicators of virus infection and learn how to report operational anomalies to resource administrators.	Higher	Positive
93. Employee attended a training program to learn about the sensitivity/criticality of special company files so that he could apply appropriate protective measures when handling the information.	Higher	Positive

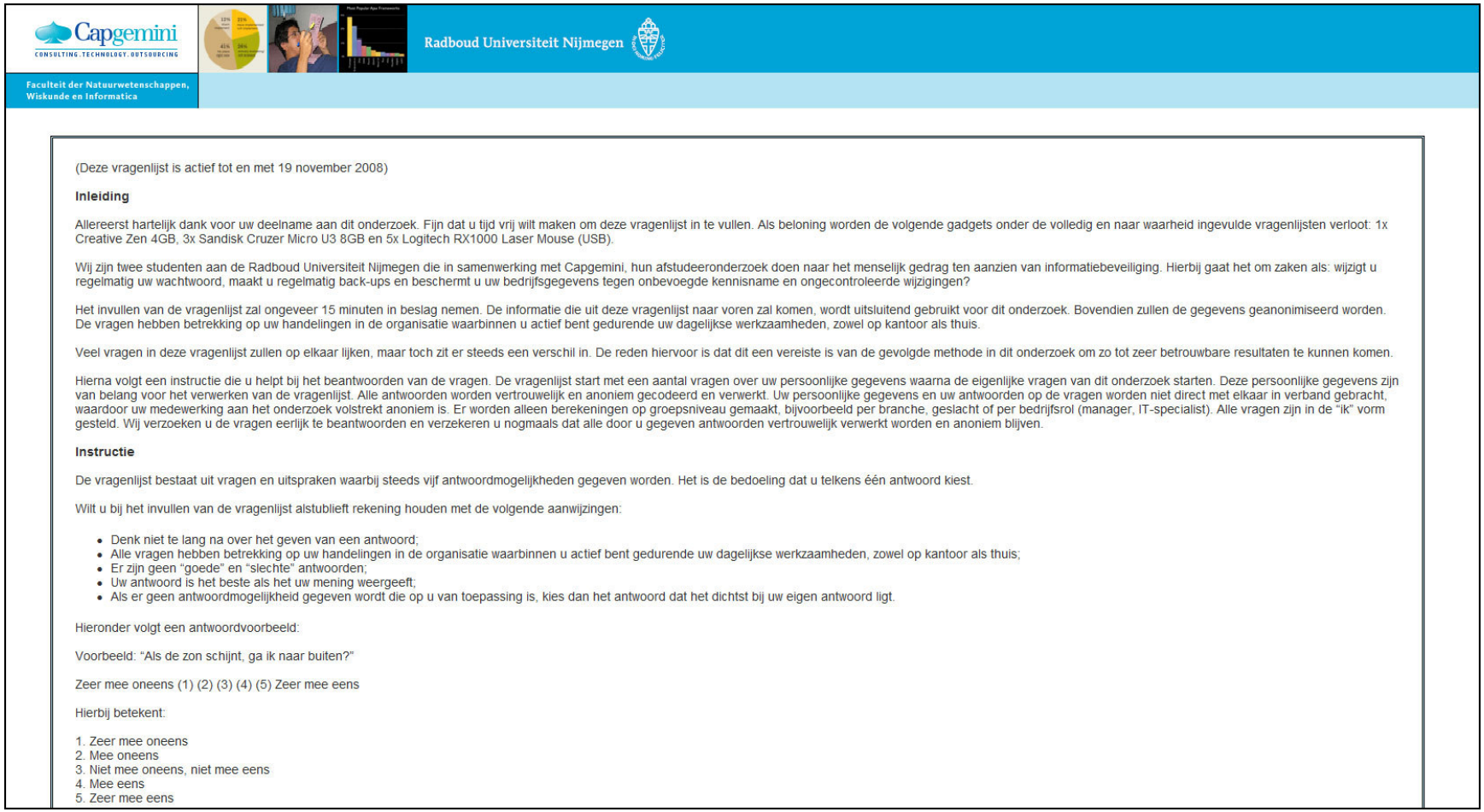
8.2 Bijlage Two factor taxonomy of security behaviors

Table 1 Two factor taxonomy of security behaviors

Expertise	Intentions	Title	Description
High	Malicious	Intentional destruction	Behavior requires technical expertise together with a strong intention to do harm to the organization's IT and resources. Example: employee breaks into an employer's protected files in order to steal a trade secret.2
Low	Malicious	Detrimental misuse	Behavior requires minimal technical expertise but nonetheless includes intention to do harm through annoyance, harassment, rule breaking, etc. Example: using company email for SPAM messages marketing a sideline business.
High	Neutral	Dangerous tinkering	Behavior requires technical expertise but no clear intention to do harm to the organization's IT and resources. Example: employee configures a wireless gateway that inadvertently allows wireless access to the company's network by people in passing cars.
Low	Neutral	Naïve mistakes	Behavior requires minimal technical expertise and no clear intention to do harm to the organization's information technology and resources. Example: choosing a bad password such as "password."
High	Beneficial	Aware assurance	Behavior requires technical expertise together with a strong intention to do good by preserving and protecting the organization's information technology and resources. Example: recognizing the presence of a backdoor program through careful observation of own PC.
Low	Beneficial	Basic hygiene	Behavior requires no technical expertise but includes clear intention to preserve and protect the organization's IT and resources. Example: a trained and aware employee resists an attempt at social engineering by refusing to reveal her password to a caller claiming to be from computer services.

Figuur 36: Two factor taxonomy of security behaviors [STAN05a]

8.3 Bijlage Introductiepagina vragenlijst



Capgemini
CONSULTING. TECHNOLOGY. OUTSOURCING

Radboud Universiteit Nijmegen

Faculteit der Natuurwetenschappen, Wiskunde en Informatica

(Deze vragenlijst is actief tot en met 19 november 2008)

Inleiding

Allereerst hartelijk dank voor uw deelname aan dit onderzoek. Fijn dat u tijd vrij wilt maken om deze vragenlijst in te vullen. Als beloning worden de volgende gadgets onder de volledig en naar waarheid ingevulde vragenlijsten verloot: 1x Creative Zen 4GB, 3x Sandisk Cruzer Micro U3 8GB en 5x Logitech RX1000 Laser Mouse (USB).

Wij zijn twee studenten aan de Radboud Universiteit Nijmegen die in samenwerking met Capgemini, hun afstudeeronderzoek doen naar het menselijk gedrag ten aanzien van informatiebeveiliging. Hierbij gaat het om zaken als: wijzigt u regelmatig uw wachtwoord, maakt u regelmatig back-ups en beschermt u uw bedrijfsgegevens tegen onbevoegde kennisname en ongecontroleerde wijzigingen?

Het invullen van de vragenlijst zal ongeveer 15 minuten in beslag nemen. De informatie die uit deze vragenlijst naar voren zal komen, wordt uitsluitend gebruikt voor dit onderzoek. Bovendien zullen de gegevens geanonimiseerd worden. De vragen hebben betrekking op uw handelingen in de organisatie waarbinnen u actief bent gedurende uw dagelijkse werkzaamheden, zowel op kantoor als thuis.

Veel vragen in deze vragenlijst zullen op elkaar lijken, maar toch zit er steeds een verschil in. De reden hiervoor is dat dit een vereiste is van de gevolgde methode in dit onderzoek om zo tot zeer betrouwbare resultaten te kunnen komen.

Hierna volgt een instructie die u helpt bij het beantwoorden van de vragen. De vragenlijst start met een aantal vragen over uw persoonlijke gegevens waarna de eigenlijke vragen van dit onderzoek starten. Deze persoonlijke gegevens zijn van belang voor het verwerken van de vragenlijst. Alle antwoorden worden vertrouwelijk en anoniem gecodeerd en verwerkt. Uw persoonlijke gegevens en uw antwoorden op de vragen worden niet direct met elkaar in verband gebracht, waardoor uw medewerking aan het onderzoek volstrekt anoniem is. Er worden alleen berekeningen op groepsniveau gemaakt, bijvoorbeeld per branche, geslacht of per bedrijfsrol (manager, IT-specialist). Alle vragen zijn in de "ik" vorm gesteld. Wij verzoeken u de vragen eerlijk te beantwoorden en verzekeren u nogmaals dat alle door u gegeven antwoorden vertrouwelijk verwerkt worden en anoniem blijven.

Instructie

De vragenlijst bestaat uit vragen en uitspraken waarbij steeds vijf antwoordmogelijkheden gegeven worden. Het is de bedoeling dat u telkens één antwoord kiest.

Wilt u bij het invullen van de vragenlijst alstublieft rekening houden met de volgende aanwijzingen:

- Denk niet te lang na over het geven van een antwoord;
- Alle vragen hebben betrekking op uw handelingen in de organisatie waarbinnen u actief bent gedurende uw dagelijkse werkzaamheden, zowel op kantoor als thuis;
- Er zijn geen "goede" en "slechte" antwoorden;
- Uw antwoord is het beste als het uw mening weergeeft;
- Als er geen antwoordmogelijkheid gegeven wordt die op u van toepassing is, kies dan het antwoord dat het dichtst bij uw eigen antwoord ligt.

Hieronder volgt een antwoordvoorbeeld:

Voorbeeld: "Als de zon schijnt, ga ik naar buiten?"

Zeer mee oneens (1) (2) (3) (4) (5) Zeer mee eens

Hierbij betekent:

1. Zeer mee oneens
2. Mee oneens
3. Niet mee oneens, niet mee eens
4. Mee eens
5. Zeer mee eens

Figuur 37: Screenshot introductiepagina vragenlijst

8.4 Bijlage Uitzetbrief

Beste heer/mevrouw,

Wij zijn twee studenten aan de Radboud Universiteit Nijmegen die in samenwerking met Capgemini, hun afstudeeronderzoek doen naar het menselijk gedrag ten aanzien van informatiebeveiliging. Hierbij gaat het om zaken als: wijzigt u regelmatig uw wachtwoord, maakt u regelmatig back-ups en beschermt u uw bedrijfsgegevens tegen onbevoegde kennisname en ongecontroleerde wijzigingen?

Het onderzoek heeft als doel om meer inzicht te verkrijgen in de oorzaken en oorsprong van het gedrag van medewerkers ten aanzien van informatiebeveiliging. Om dit inzicht te verkrijgen zetten wij een vragenlijst uit naar organisaties binnen verschillende branches. Tijdens ons onderzoek en dus ook tijdens het opstellen van deze vragenlijst houden we vast aan de theorie van gepland gedrag (een methode uit de sociale wetenschappen) en toetsen we of deze theorie toepasbaar is op het gedrag ten aanzien van informatiebeveiliging. Als dit positief is kunnen hierop maatwerk vragenlijsten worden ontwikkeld die direct kunnen leiden tot gedragsinterventies. Uw medewerking is hiervoor van essentieel belang. Door het geven van uw mening kan dit inzicht verkregen worden en maakt u kans om een Creative Zen 4GB (1x), een Sandisk Cruzer Micro U3 8GB (3x) of een Logitech RX1000 Laser Mouse (USB) (5x) te winnen. Bij deze willen wij u vriendelijk vragen om een vragenlijst in te vullen. Het invullen van deze vragenlijst kost u ongeveer 15 minuten. Vanzelfsprekend worden uw antwoorden volledig anoniem verwerkt en alleen voor dit onderzoek gebruikt. De resultaten van het onderzoek worden gepubliceerd in november 2008.

In onderstaande link is de vragenlijst te vinden:

https://survey.science.ru.nl/index.php?sid=67164&lang=nl

Alvast hartelijk dank voor uw medewerking. Heeft u nog vragen, dan kunt u ons bereiken via m.dam@student.ru.nl of kjgwessels@student.ru.nl.

Met vriendelijke groet,

Michiel Dam
Kevin Wessels

8.5 Bijlage Employee Security-Related Behavior List gerelateerd aan informatiebeveiliging

In deze bijlage zijn de 93 gedragingen van Stanton vertaalt naar de componenten voor de informatievoorziening. Deze componenten zijn op hoog niveau onderverdeeld. De 93 gedragingen zijn onder deze componenten gehangen naar een steeds meer gespecialiseerd niveau. Dit gespecialiseerd niveau is steeds meer terug te vertalen naar de gedragingen die Stanton heeft opgenomen in zijn "Employee Security-Related Behavior List". Verder zijn er ook een paar gedragingen die niet onder één van de componenten voor de informatievoorziening geplaatst konden worden. Deze gedragingen zijn wel opgenomen in deze lijst omdat ze gerelateerd kunnen worden aan informatiebeveiliging, maar ze vallen niet onder één van de componenten.

Gedrag ten aanzien van informatiebeveiliging

1. Het betrouwbaar omgaan met computerhardware, -software en -gegevens.

1.1 Beschikbaarheid, vertrouwelijkheid en integriteit van wachtwoordgebruik: 3, 11, 18, 22, 25, 31
1.2 Beschikbaarheid, vertrouwelijkheid en integriteit wachtwoordgebruik: 19, 20, 21, 38, 61, 67, 68
1.3 Positief / negatief ten aanzien van beschikbaarheid, vertrouwelijkheid en integriteit van gegevens: 4, 6, 10, 12, 13, 14, 28, 33, 35, 37, 39, 42, 58, 63, 64, 71, 72, 81
1.4 Beschikbaarheid gegevens via backup: 60
1.5 Oneigenlijk softwaregebruik (internet/intranet, filesharing, illegaal ongeautoriseerd): 9, 41, 44, 45, 46, 48, 49, 50, 69, 70
1.6 Via e-mail: 1, 2, 5, 7, 8, 11, 16, 17, 24, 40, 47, 53
1.7 Oneigenlijk hardwaregebruik (gamen, netwerk): 15, 43, 51, 82
1.8 Eigenlijk hardwaregebruik: 57

2. Policy gerelateerd gedrag: 23, 26, 27, 29, 30, 56

2.1 Clear screen clear desk: 32, 34, 36, 59

Informatiebeveiligingsbewustzijn

3. Actief of passief vermijden, ontdekken en melden van (mogelijke) zwakheden in de informatiebeveiliging: 62, 83, 84, 86, 87, 88

4. Training en bewustwording ten aanzien van informatiebeveiliging: 91, 92, 93

4.1 Het overdragen van kennis ten aanzien van informatiebeveiliging aan collega's: 89

Vragenlijst indeling

Tabel 48
Vragenlijst indeling

Vragenlijst item	Onderwerp	Vraagnummer
	Attitude toward the behavior	
1	Wachtwoordgebruk	1.1, 1.2, 1.3
2	Bedrijfsgegevens	1.4, 1.5
3	Bedrijfssoftware	1.6, 1.7
4	Bedrijfshardware	1.8, 1.9
5	Policy	2
6	Actief of passief informatiebeveiliging	3
7	Training en bewustwording	4
	Subjective norm	
1	Wachtwoordgebruk	1.1, 1.2, 1.3
2	Bedrijfsgegevens	1.4, 1.5
3	Bedrijfssoftware	1.6, 1.7
4	Bedrijfshardware	1.8, 1.9
5	Policy	2
6	Actief of passief informatiebeveiliging	3
7	Training en bewustwording	4
	Perceived behavioral control	
1	Wachtwoord	1.1, 1.2, 1.3
2	Wachtwoordgebruk	1.4, 1.5
3	Bedrijfssoftware	1.6, 1.7
4	Bedrijfshardware	1.8, 1.9
5	Policy	2
6	Actief of passief informatiebeveiliging	3
7	Training en bewustwording	4

8.6 Bijlage Cronbach's alpha vooronderzoek

Tabel 49

Beschrijvende statistieken schaalgegevens van het vooronderzoek (n = 16): aantal items, gemiddelde schaal frequentie, standaarddeviatie van schaalscores en de Cronbach's α

Construct	Aantal items	Gemiddelde schaal frequentie	Standaarddeviatie schaalscores	Cronbach's α
Attitude toward the behavior				
Bedrijfsgegevens	14	54,463	7,380	,785
Back-up	10	35,129	5,927	,746
Wachtwoordgebruik	25	159,850	12,643	,762
Subjective norm				
Injunctive norm				
Bedrijfsgegevens	6	7,583	2,754	,655
Back-up	4	5,629	2,373	,598
Wachtwoordgebruik	10	67,429	8,212	,865
Descriptive norm				
Bedrijfsgegevens	3	2,563	1,601	,922
Back-up	2	2,363	1,537	,550
Wachtwoordgebruik	5	17,800	4,219	,833
Perceived behavioral control				
Self-efficacy				
Bedrijfsgegevens	6	12,200	3,493	,853
Back-up	4	6,796	2,607	,683
Wachtwoordgebruik	10	27,529	5,247	,677
Controllability				
Bedrijfsgegevens	6	15,963	3,995	,847
Back-up	4	5,400	2,324	,424
Wachtwoordgebruik	10	19,267	4,389	,566

8.7 Bijlage Demografische gegevens

Tabel 50
Mijn geslacht is

Antwoord	Telling	Percentage
Vrouwelijk (F)	41	18,3%
Mannelijk (M)	183	81,7%

Tabel 51
Mijn leeftijd is

Berekening	Resultaat
Minimum	20
Maximum	64
Gemiddelde	37,8

Tabel 52
Ik heb (een) … management functie

Antwoord	Telling	Percentage
Geen (1)	126	56,25%
Operationele (2)	52	23,21%
Tactische (3)	25	11,16%
Strategische (4)	21	9,38%

Tabel 53
Ik beschouw mezelf als een IT-specialist

Antwoord	Telling	Percentage
zeer mee oneens (1)	10	4,46%
mee oneens (2)	25	11,16%
gedeeltelijk mee oneens (3)	13	5,80%
noch mee oneens, noch mee eens (4)	14	6,25%
gedeeltelijk mee eens (5)	42	18,75%
mee eens (6)	78	34,82%

Tabel 54
Ik ben … jaar werkzaam als professional op de arbeidsmarkt.

Berekening	Resultaat
Minimum	0
Maximum	41
Gemiddelde	13,7

Tabel 55

Binnen welke branche is de organisatie actie?

Antwoord	Telling	Percentage
Hightech industrie (1)	10	4,46%
Overige industrie (2)	9	4,02%
Kennisintensieve dienstverlening (3)	125	55,80%
Overige dienstverlening (4)	80	35,71%

Tabel 56

Ik ben … uur per week binnen de organisatie werkzaam met automatiseringsmiddelen en progamma's.

Antwoord	Telling	Percentage
0 tot 2 uur (1)	8	3,57%
3 tot 5 uur (2)	9	4,02%
6 tot 9 uur (3)	6	2,68%
10 tot 19 uur (4)	23	10,27%
20 of meer uur (5)	178	79,46%

Tabel 57

Ik ben … uur per week privé werkzaam met automatiseringsmiddelen en programma's.

Antwoord	Telling	Percentage
0 tot 2 uur (1)	42	18,75%
3 tot 5 uur (2)	52	23,21%
6 tot 9 uur (3)	65	29,02%
10 tot 19 uur (4)	44	19,64%
20 of meer uur (5)	21	9,38%

Tabel 58

Mijn kennis en vaardigheden ten aanzien van Informatie- en Communicatietechnologie beoordeel ik met het rapportcijfer

Antwoord	Telling	Percentage
1 (1)	0	0%
2 (2)	4	1,79%
3 (3)	6	2,68%
4 (4)	2	0,89%
5 (5)	6	2,68%
6 (6)	16	7,14%
7 (7)	74	33,04%
8 (8)	82	36,61%
9 (9)	30	13,39%
10 (10)	4	1,79%

8.8 Bijlage Item lijst

Tabel 59
Item lijst

TpB construct onderdeel	Itemcode	Itemomschrijving	Schaalscore	Schaalnaam
Gedragsintentie				
Bedrijfsgegevens	AI1 - 1	Mijn intentie is om mijn bedrijfsgegevens te beschermen.	1 tot en met 5	onwaarschijnlijk/ waarschijnlijk | positief
	AI2 - 1	Mijn intentie is om periodiek back-ups te maken van mijn bedrijfsgegevens.		
	AI3 - 1	Mijn intentie is om veilig om te gaan met mijn wachtwoord.		
Back-up	AI1 - 2	Ik wil mijn bedrijfsgegevens beschermen.	1 tot en met 5	waar/niet waar | positief
	AI2 - 2	Ik wil periodiek back-ups maken van mijn bedrijfsgegevens.		
	AI3 - 2	Ik wil veilig omgaan met mijn wachtwoord.		
Wachtwoordgebruik	AI1 - 3	Ik ben van plan om mijn bedrijfsgegevens te beschermen.	1 tot en met 5	oneens/eens | positief
	AI2 - 3	Ik ben van plan om periodiek back-ups te maken van mijn bedrijfsgegevens.		
	AI3 - 3	Ik ben van plan om veilig om te gaan met mijn wachtwoord.		
Attitude toward the behavior				
Bedrijfsgegevens	AD 1 - 1	Ik vind het beschermen van mijn bedrijfsgegevens tegen onbevoegde kennisname bedrijfsgegevens	1 tot en met 5	onverstandig/verstandig | positief
Bedrijfsgegevens	AD 1 - 2	Ik vind het beschermen van mijn bedrijfsgegevens tegen ongecontroleerde wijzigingen	1 tot en met 5	onverstandig/verstandig | positief
Bedrijfsgegevens Back-up	AD 1 - 3	Ik vind het zekerstellen van mijn bedrijfsgegevens, zodat deze op ieder gewenst moment beschikbaar zijn voor mij	1 tot en met 5	onverstandig/verstandig | positief

Back-up	AD 1 - 4	Ik vind het maken van back-ups van mijn bedrijfsgegevens	1 tot en met 5	onverstandig/verstandig | positief
Wachtwoordgebruik	AD 1 - 5	Ik vind het verzinnen van een complex wachtwoord dat bijvoorbeeld bestaat uit minimaal 8 karakters, waarvan er minimaal 4 cijfers, 1 hoofdletter en 1 vreemd teken zijn,	1 tot en met 5	onverstandig/verstandig | positief
Wachtwoordgebruik	AD 1 - 6	Ik vind het periodiek wijzigen van mijn wachtwoord	1 tot en met 5	onverstandig/verstandig | positief
Wachtwoordgebruik	AD 1 - 7	Ik vind het geheimhouden van mijn wachtwoord	1 tot en met 5	onverstandig/verstandig | positief
Wachtwoordgebruik	AD 1 - 8	Ik vind het onthouden van mijn wachtwoord	1 tot en met 5	onverstandig/verstandig | positief
Bedrijfsgegevens	AD 2 - 1	Ik vind het beschermen van mijn bedrijfsgegevens tegen onbevoegde kennisname voor mij	1 tot en met 5	prettig/vervelend | positief
Bedrijfsgegevens	AD 2 - 2	Ik vind het beschermen van mijn bedrijfsgegevens tegen ongecontroleerde wijzigingen voor mij	1 tot en met 5	prettig/vervelend | positief
Bedrijfsgegevens Back-up	AD 2 - 3	Ik vind het zekerstellen van mijn bedrijfsgegevens, zodat deze op ieder gewenst moment beschikbaar zijn voor mij	1 tot en met 5	prettig/vervelend | positief
Back-up	AD 2 - 4	Ik vind het maken van back-ups van mijn bedrijfsgegevens voor mij	1 tot en met 5	prettig/vervelend | positief
Wachtwoordgebruik	AD 2 - 5	Ik vind het verzinnen van een complex wachtwoord dat bijvoorbeeld bestaat uit minimaal 8 karakters, waarvan er minimaal 4 cijfers, 1 hoofdletter en 1 vreemd teken zijn, voor mij	1 tot en met 5	prettig/vervelend | positief
Wachtwoordgebruik	AD 2 - 6	Ik vind het periodiek wijzigen van mijn wachtwoord voor mij	1 tot en met 5	prettig/vervelend | positief
Wachtwoordgebruik	AD 2 - 7	Ik vind het geheimhouden van mijn wachtwoord voor mij	1 tot en met 5	prettig/vervelend | positief
Wachtwoordgebruik	AD 2 - 8	Ik vind het onthouden van mijn wachtwoord voor mij	1 tot en met 5	prettig/vervelend | positief
Bedrijfsgegevens	AD 3 - 1	Ik vind het beschermen van mijn bedrijfsgegevens tegen onbevoegde kennisname voor mij	1 tot en met 5	nutteloos/nuttig | positief
Bedrijfsgegevens	AD 3 - 2	Ik vind het beschermen van mijn bedrijfsgegevens tegen ongecontroleerde wijzigingen voor mij.	1 tot en met 5	nutteloos/nuttig | positief

Bedrijfsgegevens Back-up	AD 3 - 3	Ik vind het zekerstellen van mijn bedrijfsgegevens, zodat deze op ieder gewenst moment beschikbaar zijn voor mij.	1 tot en met 5	nutteloos/nuttig | positief
Back-up	AD 3 - 4	Ik vind het maken van back-ups van mijn bedrijfsgegevens voor mij.	1 tot en met 5	nutteloos/nuttig | positief
Wachtwoordgebruik	AD 3 - 5	Ik vind het verzinnen van een complex wachtwoord dat bijvoorbeeld bestaat uit minimaal 8 karakters, waarvan er minimaal 4 cijfers, 1 hoofdletter en 1 vreemd teken zijn, voor mij.	1 tot en met 5	nutteloos/nuttig | positief
Wachtwoordgebruik	AD 3 - 6	Ik vind het periodiek wijzigen van mijn wachtwoord voor mij.	1 tot en met 5	nutteloos/nuttig | positief
Wachtwoordgebruik	AD 3 - 7	Ik vind het geheimhouden van mijn wachtwoord voor mij.	1 tot en met 5	nutteloos/nuttig | positief
Wachtwoordgebruik	AD 3 - 8	Ik vind het onthouden van mijn wachtwoord voor mij.	1 tot en met 5	nutteloos/nuttig | positief
Bedrijfsgegevens	AD 4 - 1	Ik vind het beschermen van mijn bedrijfsgegevens tegen onbevoegde kennisname.	1 tot en met 5	gemakkelijk/moeilijk | positief
Bedrijfsgegevens	AD 4 - 2	Ik vind het beschermen van mijn bedrijfsgegevens tegen ongecontroleerde wijzigingen.	1 tot en met 5	gemakkelijk/moeilijk | positief
Bedrijfsgegevens Back-up	AD 4 - 3	Ik vind het zekerstellen van mijn bedrijfsgegevens, zodat deze op ieder gewenst moment beschikbaar zijn voor mij.	1 tot en met 5	gemakkelijk/moeilijk | positief
Back-up	AD 4 - 4	Ik vind het maken van back-ups van mijn bedrijfsgegevens.	1 tot en met 5	gemakkelijk/moeilijk | positief
Wachtwoordgebruik	AD 4 - 5	Ik vind het verzinnen van een complex wachtwoord dat bijvoorbeeld bestaat uit minimaal 8 karakters, waarvan er minimaal 4 cijfers, 1 hoofdletter en 1 vreemd teken zijn,	1 tot en met 5	gemakkelijk/moeilijk | positief
Wachtwoordgebruik	AD 4 - 6	Ik vind het periodiek wijzigen van mijn wachtwoord.	1 tot en met 5	gemakkelijk/moeilijk | positief
Wachtwoordgebruik	AD 4 - 7	Ik vind het geheimhouden van mijn wachtwoord.	1 tot en met 5	gemakkelijk/moeilijk | positief
Wachtwoordgebruik	AD 4 - 8	Ik vind het onthouden van mijn wachtwoord.	1 tot en met 5	gemakkelijk/moeilijk | positief
Bedrijfsgegevens	AD 5 - 1	Ik vind het beschermen van mijn bedrijfsgegevens tegen onbevoegde kennisname voor anderen.	1 tot en met 5	nutteloos/nuttig | positief
Bedrijfsgegevens	AD 5 - 2	Ik vind het beschermen van mijn bedrijfsgegevens tegen ongecontroleerde wijzigingen voor anderen.	1 tot en met 5	nutteloos/nuttig | positief

Bedrijfsgegevens Back-up	AD 5 - 3	Ik vind het zekerstellen van mijn bedrijfsgegevens, zodat deze op ieder gewenst moment beschikbaar zijn voor mij, voor anderen.	1 tot en met 5	nutteloos/nuttig | positief
Back-up	AD 5 - 4	Ik vind het maken van back-ups van mijn bedrijfsgegevens voor anderen.	1 tot en met 5	nutteloos/nuttig | positief
Wachtwoordgebruik	AD 5 - 5	Ik vind het verzinnen van een complex wachtwoord dat bijvoorbeeld bestaat uit minimaal 8 karakters, waarvan er minimaal 4 cijfers, 1 hoofdletter en 1 vreemd teken zijn, voor anderen.	1 tot en met 5	nutteloos/nuttig | positief
Wachtwoordgebruik	AD 5 - 6	Ik vind het periodiek wijzigen van mijn wachtwoord voor anderen.	1 tot en met 5	nutteloos/nuttig | positief
Wachtwoordgebruik	AD 5 - 7	Ik vind het geheimhouden van mijn wachtwoord voor anderen.	1 tot en met 5	nutteloos/nuttig | positief
Wachtwoordgebruik	AD 5 - 8	Ik vind het onthouden van mijn wachtwoord voor anderen.	1 tot en met 5	nutteloos/nuttig | positief

Behavioral beliefs

Back-up Bedrijfsgegevens	AIBB - 1	Als ik back-ups maak van mijn bedrijfsgegevens, dan zijn deze op ieder gewenst moment beschikbaar voor mij.	1 tot en met 5	onwaarschijnlijk/ waarschijnlijk | positief
Wachtwoordgebruik Bedrijfsgegevens	AIBB - 2	Als ik een complex wachtwoord verzin, dan zijn mijn bedrijfsgegevens beter beschermd tegen onbevoegde kennisname en ongecontroleerde wijzigingen.	1 tot en met 5	onwaarschijnlijk/ waarschijnlijk | positief
Wachtwoordgebruik Bedrijfsgegevens	AIBB - 3	Als ik periodiek mijn wachtwoord wijzig, dan zijn mijn bedrijfsgegevens beter beschermd tegen onbevoegde kennisname en ongecontroleerde wijzigingen.	1 tot en met 5	onwaarschijnlijk/ waarschijnlijk | positief
Wachtwoordgebruik Bedrijfsgegevens	AIBB - 4	Als ik mijn wachtwoord geheimhoud, dan zijn mijn bedrijfsgegevens beter beschermd tegen onbevoegde kennisname en ongecontroleerde wijzigingen.	1 tot en met 5	onwaarschijnlijk/ waarschijnlijk | positief
Wachtwoordgebruik Bedrijfsgegevens	AIBB - 5	Als ik mijn wachtwoord onthoud, dan zijn mijn bedrijfsgegevens beter beschermd tegen onbevoegde. kennisname en ongecontroleerde wijzigingen.	1 tot en met 5	onwaarschijnlijk/ waarschijnlijk | positief

Outcome evaluations

Back-up Bedrijfsgegevens	AIOE - 1	Dat op ieder gewenst moment mijn bedrijfsgegevens beschikbaar zijn voor mij is.	-2 tot en met +2	ongewenst/ gewenst | negatief
Wachtwoordgebruik Bedrijfsgegevens	AIOE - 2	Dat mijn bedrijfsgegevens beter beschermd zijn tegen onbevoegde kennisname en ongecontroleerde wijzigingen is.	-2 tot en met +2	ongewenst/ gewenst | negatief

Subjective norm

Injunctive norm

Bedrijfsgegevens	SND-IN1 - 1	De meeste mensen die belangrijk voor mij zijn vinden dat ik … … mijn bedrijfsgegevens moet beschermen tegen onbevoegde kennisname.	1 tot en met 5	altijd/nooit | positief
Bedrijfsgegevens	SND-IN1 - 2	De meeste mensen die belangrijk voor mij zijn vinden dat ik … … mijn bedrijfsgegevens moet beschermen tegen ongecontroleerde wijzigingen.	1 tot en met 5	altijd/nooit | positief
Bedrijfsgegevens Back-up	SND-IN1 - 3	De meeste mensen die belangrijk voor mij zijn vinden dat ik … … mijn bedrijfsgegevens moet zekerstellen.	1 tot en met 5	altijd/nooit | positief
Back-up	SND-IN1 - 4	De meeste mensen die belangrijk voor mij zijn vinden dat ik … … back-ups moet maken van mijn bedrijfsgegevens.	1 tot en met 5	altijd/nooit | positief
Wachtwoordgebruik	SND-IN1 - 5	De meeste mensen die belangrijk voor mij zijn vinden dat ik … … een complex wachtwoord moet verzinnen.	1 tot en met 5	altijd/nooit | positief
Wachtwoordgebruik	SND-IN1 - 6	De meeste mensen die belangrijk voor mij zijn vinden dat ik … … periodiek mijn wachtwoord moet wijzigen.	1 tot en met 5	altijd/nooit | positief

Wachtwoordgebruik	SND-IN1 - 7	De meeste mensen die belangrijk voor mij zijn vinden dat ik … … mijn wachtwoord geheim moet houden.	1 tot en met 5	altijd/nooit | positief
Wachtwoordgebruik	SND-IN1 - 8	De meeste mensen die belangrijk voor mij zijn vinden dat ik … … mijn wachtwoord moet onthouden.	1 tot en met 5	altijd/nooit | positief
Bedrijfsgegevens	SND-IN2 - 1	Er wordt van mij verwacht dat ik mijn bedrijfsgegevens bescherm tegen onbevoegde kennisname.	1 tot en met 5	oneens/eens | positief
Bedrijfsgegevens	SND-IN2 - 2	Er wordt van mij verwacht dat ik mijn bedrijfsgegevens bescherm tegen ongecontroleerde wijzigingen.	1 tot en met 5	oneens/eens | positief
Bedrijfsgegevens Back-up	SND-IN2 - 3	Er wordt van mij verwacht dat ik mijn bedrijfsgegevens zekerstel.	1 tot en met 5	oneens/eens | positief
Back-up	SND-IN2 - 4	Er wordt van mij verwacht dat ik back-ups maak van mijn bedrijfsgegevens.	1 tot en met 5	oneens/eens | positief
Wachtwoordgebruik	SND-IN2 - 5	Er wordt van mij verwacht dat ik een complex wachtwoord verzin.	1 tot en met 5	oneens/eens | positief
Wachtwoordgebruik	SND-IN2 - 6	Er wordt van mij verwacht dat ik periodiek mijn wachtwoord wijzig.	1 tot en met 5	oneens/eens | positief
Wachtwoordgebruik	SND-IN2 - 7	Er wordt van mij verwacht dat ik mijn wachtwoord geheimhoud.	1 tot en met 5	oneens/eens | positief
Wachtwoordgebruik	SND-IN2 - 8	Er wordt van mij verwacht dat ik mijn wachtwoord onthoud.	1 tot en met 5	oneens/eens | positief

Descriptive norm

Bedrijfsgegevens	SND-DN - 1	De meeste mensen die belangrijk voor mij zijn beschermen hun bedrijfsgegevens tegen onbevoegde kennisname.	1 tot en met 5	oneens/eens | positief
Bedrijfsgegevens	SND-DN - 2	De meeste mensen die belangrijk voor mij zijn beschermen hun bedrijfsgegevens tegen ongecontroleerde wijzigingen.	1 tot en met 5	oneens/eens | positief
Bedrijfsgegevens Back-up	SND-DN - 3	De meeste mensen die belangrijk voor mij zijn stellen hun bedrijfsgegevens zeker.	1 tot en met 5	oneens/eens | positief
Back-up	SND-DN - 4	De meeste mensen die belangrijk voor mij zijn maken back-ups van hun bedrijfsgegevens.	1 tot en met 5	oneens/eens | positief
Wachtwoordgebruik	SND-DN - 5	De meeste mensen die belangrijk voor mij zijn verzinnen een complex wachtwoord.	1 tot en met 5	oneens/eens | positief

Wachtwoordgebruik	SND-DN - 6	De meeste mensen die belangrijk voor mij zijn wijzigen periodiek hun wachtwoord.	1 tot en met 5	oneens/eens | positief
Wachtwoordgebruik	SND-DN - 7	De meeste mensen die belangrijk voor mij zijn houden hun wachtwoord geheim.	1 tot en met 5	oneens/eens | positief
Wachtwoordgebruik	SND-DN - 8	De meeste mensen die belangrijk voor mij zijn onthouden hun wachtwoord.	1 tot en met 5	oneens/eens | positief

Normative beliefs

Injunctive norm

Organisatie	SNINB-IN1 - 1	De organisatie vindt dat ik … … veilig om moet gaan met mijn bedrijfsgegevens.	-2 tot en met +2	nooit/altijd | negatief
Bedrijfsgegevens	SNINB-IN1 - 2	Mijn direct leidinggevende vindt dat ik … … mijn bedrijfsgegevens moet beschermen tegen onbevoegde kennisname.	-2 tot en met +2	nooit/altijd | negatief
Bedrijfsgegevens	SNINB-IN1 - 3	Mijn direct leidinggevende vindt dat ik … … mijn bedrijfsgegevens moet beschermen tegen ongecontroleerde wijzigingen.	-2 tot en met +2	nooit/altijd | negatief
Bedrijfsgegevens Back-up	SNINB-IN1 - 4	Mijn direct leidinggevende vindt dat ik … … mijn bedrijfsgegevens moet zekerstellen.	-2 tot en met +2	nooit/altijd | negatief
Back-up	SNINB-IN1 - 5	Mijn direct leidinggevende vindt dat ik … … back-ups moet maken van mijn bedrijfsgegevens.	-2 tot en met +2	nooit/altijd | negatief
Wachtwoordgebruik	SNINB-IN1 - 6	Mijn direct leidinggevende vindt dat ik … … een complex wachtwoord moet verzinnen.	-2 tot en met +2	nooit/altijd | negatief
Wachtwoordgebruik	SNINB-IN1 - 7	Mijn direct leidinggevende vindt dat ik … … periodiek mijn wachtwoord moet wijzigen.	-2 tot en met +2	nooit/altijd | negatief
Wachtwoordgebruik	SNINB-IN1 - 8	Mijn direct leidinggevende vindt dat ik … … mijn wachtwoord geheim moet houden.	-2 tot en met +2	nooit/altijd | negatief
Wachtwoordgebruik	SNINB-IN1 - 9	Mijn direct leidinggevende vindt dat ik … … mijn wachtwoord moet onthouden.	-2 tot en met +2	nooit/altijd | negatief

Bedrijfsgegevens	SNINB-IN2 - 1	Naaste collega's, die belangrijk voor mij zijn, vinden dat ik … mijn bedrijfsgegevens moet beschermen tegen onbevoegde kennisname.	…	-2 tot en met +2	nooit/altijd | negatief
Bedrijfsgegevens	SNINB-IN2 - 2	Naaste collega's, die belangrijk voor mij zijn, vinden dat ik … mijn bedrijfsgegevens moet beschermen tegen ongecontroleerde wijzigingen.	…	-2 tot en met +2	nooit/altijd | negatief
Bedrijfsgegevens Back-up	SNINB-IN2 - 3	Naaste collega's, die belangrijk voor mij zijn, vinden dat ik … mijn bedrijfsgegevens moet zekerstellen.	…	-2 tot en met +2	nooit/altijd | negatief
Back-up	SNINB-IN2 - 4	Naaste collega's, die belangrijk voor mij zijn, vinden dat ik … back-ups moet maken van mijn bedrijfsgegevens.	…	-2 tot en met +2	nooit/altijd | negatief
Wachtwoordgebruik	SNINB-IN2 - 5	Naaste collega's, die belangrijk voor mij zijn, vinden dat ik … een complex wachtwoord moet verzinnen.	…	-2 tot en met +2	nooit/altijd | negatief
Wachtwoordgebruik	SNINB-IN2 - 6	Naaste collega's, die belangrijk voor mij zijn, vinden dat ik … periodiek mijn wachtwoord moet wijzigen.	…	-2 tot en met +2	nooit/altijd | negatief
Wachtwoordgebruik	SNINB-IN2 - 7	Naaste collega's, die belangrijk voor mij zijn, vinden dat ik … mijn wachtwoord geheim moet houden.	…	-2 tot en met +2	nooit/altijd | negatief
Wachtwoordgebruik	SNINB-IN2 - 8	Naaste collega's, die belangrijk voor mij zijn, vinden dat ik … mijn wachtwoord moet onthouden.	…	-2 tot en met +2	nooit/altijd | negatief

Descriptive norm

Organisatie	SNINB-DN1 - 1	De organisatie heeft … … voorschriften opgesteld om veilig om te gaan met de informatievoorziening.		-2 tot en met +2	heel weinig/heel veel | negatief
Bedrijfsgegevens	SNINB-DN2 - 1	Naaste collega's, die belangrijk voor mij zijn, zorgen er … … voor dat hun bedrijfsgegevens beschermd zijn tegen onbevoegde kennisname.		-2 tot en met +2	nooit/altijd | negatief
Bedrijfsgegevens	SNINB-DN2 - 2	Naaste collega's, die belangrijk voor mij zijn, zorgen er … … voor dat hun bedrijfsgegevens beschermd zijn tegen ongecontroleerde wijzigingen.		-2 tot en met +2	nooit/altijd | negatief
Bedrijfsgegevens Back-up	SNINB-DN2 - 3	Naaste collega's, die belangrijk voor mij zijn, zorgen er … … voor dat hun bedrijfsgegevens zeker zijn gesteld.		-2 tot en met +2	nooit/altijd | negatief
Back-up	SNINB-DN2 - 4	Naaste collega's, die belangrijk voor mij zijn, maken … … back-ups van hun bedrijfsgegevens.		-2 tot en met +2	nooit/altijd | negatief

Wachtwoordgebruik	SNINB-DN2 - 5	Naaste collega's, die belangrijk voor mij zijn, verzinnen … … een complex wachtwoord.	-2 tot en met +2	nooit/altijd | negatief
Wachtwoordgebruik	SNINB-DN2 - 6	Naaste collega's, die belangrijk voor mij zijn, wijzigen … … periodiek hun wachtwoord.	-2 tot en met +2	nooit/altijd | negatief
Wachtwoordgebruik	SNINB-DN2 - 7	Naaste collega's, die belangrijk voor mij zijn, houden … … hun wachtwoord geheim.	-2 tot en met +2	nooit/altijd | negatief
Wachtwoordgebruik	SNINB-DN2 - 8	Naaste collega's, die belangrijk voor mij zijn, onthouden … … hun wachtwoord.	-2 tot en met +2	nooit/altijd | negatief
Motivation to comply				
Injunctive norm	SNIMC-IDN - 1	Wat de organisatie vindt dat ik moet doen is voor mij belangrijk.	1 tot en met 5	oneens/eens | positief
Injunctive norm	SNIMC-IDN - 2	Wat naaste collega's vinden dat ik moet doen is voor mij belangrijk.	1 tot en met 5	oneens/eens | positief
Injunctive norm	SNIMC-IDN - 3	Wat mijn direct leidinggevende vindt dat ik moet doen is voor mij belangrijk.	1 tot en met 5	oneens/eens | positief
Descriptive norm	SNIMC-IDN - 4	Handelen volgens de voorschriften van de organisatie is voor mij belangrijk.	1 tot en met 5	oneens/eens | positief
Descriptive norm	SNIMC-IDN - 5	Doen wat naaste collega's doen is voor mij belangrijk.	1 tot en met 5	oneens/eens | positief
Perceived behavioral control				
Self-efficacy				
Wachtwoordgebruik	PBCD-SE1 - 1	Voor mij is handelen volgens het wachtwoordbeleid.	1 tot en met 5	gemakkelijk/moeilijk | positief
Back-up	PBCD-SE1 - 2	Voor mij is handelen volgens het back-up beleid.	1 tot en met 5	gemakkelijk/moeilijk | positief

Bedrijfsgegevens	PBCD-SE1 - 3	Voor mij is het beschermen van mijn bedrijfsgegevens tegen onbevoegde kennisname.	1 tot en met 5	gemakkelijk/moeilijk | positief
Bedrijfsgegevens	PBCD-SE1 - 4	Voor mij is het beschermen van mijn bedrijfsgegevens tegen ongecontroleerde wijzigingen.	1 tot en met 5	gemakkelijk/moeilijk | positief
Bedrijfsgegevens Back-up	PBCD-SE1 - 5	Voor mij is het zekerstellen van mijn bedrijfsgegevens.	1 tot en met 5	gemakkelijk/moeilijk | positief
Back-up	PBCD-SE1 - 6	Voor mij is het maken van back-ups van mijn bedrijfsgegevens.	1 tot en met 5	gemakkelijk/moeilijk | positief
Wachtwoordgebruik	PBCD-SE1 - 7	Voor mij is het verzinnen van een complex wachtwoord.	1 tot en met 5	gemakkelijk/moeilijk | positief
Wachtwoordgebruik	PBCD-SE1 - 8	Voor mij is het periodiek wijzigen van mijn wachtwoord.	1 tot en met 5	gemakkelijk/moeilijk | positief
Wachtwoordgebruik	PBCD-SE1 - 9	Voor mij is het geheimhouden van mijn wachtwoord.	1 tot en met 5	gemakkelijk/moeilijk | positief
Wachtwoordgebruik	PBCD-SE1 - 10	Voor mij is het onthouden van mijn wachtwoord.	1 tot en met 5	gemakkelijk/moeilijk | positief
Wachtwoordgebruik	PBCD-SE2 - 1	Ik ben ervan overtuigd dat ik volgens het wachtwoordbeleid kan handelen.	1 tot en met 5	oneens/eens | positief
Back-up	PBCD-SE2 - 2	Ik ben ervan overtuigd dat ik volgens het back-up beleid kan handelen.	1 tot en met 5	oneens/eens | positief
Bedrijfsgegevens	PBCD-SE2 - 3	Ik ben ervan overtuigd dat ik mijn bedrijfsgegevens kan beschermen tegen onbevoegde kennisname.	1 tot en met 5	oneens/eens | positief
Bedrijfsgegevens	PBCD-SE2 - 4	Ik ben ervan overtuigd dat ik mijn bedrijfsgegevens kan beschermen tegen ongecontroleerde wijzigingen.	1 tot en met 5	oneens/eens | positief
Bedrijfsgegevens Back-up	PBCD-SE2 - 5	Ik ben ervan overtuigd dat ik mijn bedrijfsgegevens zeker kan stellen.	1 tot en met 5	oneens/eens | positief
Back-up	PBCD-SE2 - 6	Ik ben ervan overtuigd dat ik back-ups kan maken van mijn bedrijfsgegevens.	1 tot en met 5	oneens/eens | positief
Wachtwoordgebruik	PBCD-SE2 - 7	Ik ben ervan overtuigd dat ik een complex wachtwoord kan verzinnen.	1 tot en met 5	oneens/eens | positief
Wachtwoordgebruik	PBCD-SE2 - 8	Ik ben ervan overtuigd dat ik periodiek mijn wachtwoord kan wijzigen.	1 tot en met 5	oneens/eens | positief
Wachtwoordgebruik	PBCD-SE2 - 9	Ik ben ervan overtuigd dat ik mijn wachtwoord geheim kan houden.	1 tot en met 5	oneens/eens | positief

Wachtwoordgebruik	PBCD-SE2 - 10	Ik ben ervan overtuigd dat ik mijn wachtwoord kan onthouden.	1 tot en met 5	oneens/eens | positief

---

Controllability

Wachtwoordgebruik	PBCD-C1 - 1	Ik heb het handelen volgens het wachtwoordbeleid volledig onder controle.	1 tot en met 5	oneens/eens | positief
Back-up	PBCD-C1 - 2	Ik heb het handelen volgens het back-up beleid volledig onder controle.	1 tot en met 5	oneens/eens | positief
Bedrijfsgegevens	PBCD-C1 - 3	Ik heb het beschermen van mijn bedrijfsgegevens tegen onbevoegde kennisname volledig onder controle.	1 tot en met 5	oneens/eens | positief
Bedrijfsgegevens	PBCD-C1 - 4	Ik heb het beschermen van mijn bedrijfsgegevens tegen ongecontroleerde wijzigingen volledig onder controle.	1 tot en met 5	oneens/eens | positief
Bedrijfsgegevens Back-up	PBCD-C1 - 5	Ik heb het zekerstellen van mijn bedrijfsgegevens volledig onder controle.	1 tot en met 5	oneens/eens | positief
Back-up	PBCD-C1 - 6	Ik heb het maken van back-ups van mijn bedrijfsgegevens volledig onder controle.	1 tot en met 5	oneens/eens | positief
Wachtwoordgebruik	PBCD-C1 - 7	Ik heb het verzinnen van een complex wachtwoord volledig onder controle.	1 tot en met 5	oneens/eens | positief
Wachtwoordgebruik	PBCD-C1 - 8	Ik heb het periodiek wijzigen van mijn wachtwoord volledig onder controle.	1 tot en met 5	oneens/eens | positief
Wachtwoordgebruik	PBCD-C1 - 9	Ik heb het geheimhouden van mijn wachtwoord volledig onder controle.	1 tot en met 5	oneens/eens | positief
Wachtwoordgebruik	PBCD-C1 - 10	Ik heb het onthouden van mijn wachtwoord volledig onder controle.	1 tot en met 5	oneens/eens | positief
Wachtwoordgebruik	PBCD-C2 - 1	Of ik handel volgens het wachtwoordbeleid is volledig aan mij.	1 tot en met 5	oneens/eens | positief
Back-up	PBCD-C2 - 2	Of ik handel volgens het back-up beleid is volledig aan mij.	1 tot en met 5	oneens/eens | positief

Bedrijfsgegevens	PBCD-C2 - 3	Of ik mijn bedrijfsgegevens bescherm tegen onbevoegde kennisname is volledig aan mij.	1 tot en met 5	oneens/eens | positief
Bedrijfsgegevens	PBCD-C2 - 4	Of ik mijn bedrijfsgegevens bescherm tegen ongecontroleerde wijzigingen is volledig aan mij.	1 tot en met 5	oneens/eens | positief
Bedrijfsgegevens Back-up	PBCD-C2 - 5	Of ik mijn bedrijfsgegevens zekerstel is volledig aan mij.	1 tot en met 5	oneens/eens | positief
Back-up	PBCD-C2 - 6	Of ik back-ups van mijn bedrijfsgegevens maak is volledig aan mij.	1 tot en met 5	oneens/eens | positief
Wachtwoordgebruik	PBCD-C2 - 7	Of ik een complex wachtwoord verzin is volledig aan mij.	1 tot en met 5	oneens/eens | positief
Wachtwoordgebruik	PBCD-C2 - 8	Of ik periodiek mijn wachtwoord wijzig is volledig aan mij.	1 tot en met 5	oneens/eens | positief
Wachtwoordgebruik	PBCD-C2 - 9	Of ik mijn wachtwoord geheimhoud is volledig aan mij.	1 tot en met 5	oneens/eens | positief
Wachtwoordgebruik	PBCD-C2 - 10	Of ik mijn wachtwoord onthoud is volledig aan mij.	1 tot en met 5	oneens/eens | positief

Control beliefs

Wachtwoordgebruik	PBCI-CB1 - 1	Ik denk dat ik door het wachtwoordbeleid veiliger om kan gaan met mijn wachtwoord.	1 tot en met 5	onwaarschijnlijk/ waarschijnlijk | positief
Back-up	PBCI-CB1 - 2	Ik denk dat ik door het back-up beleid beter back-ups van mijn bedrijfsgegevens kan maken.	1 tot en met 5	onwaarschijnlijk/ waarschijnlijk | positief
Bedrijfsgegevens	PBCI-CB1 - 3	Ik denk dat ik mijn bedrijfsgegevens kan beschermen tegen onbevoegde kennisname.	1 tot en met 5	onwaarschijnlijk/ waarschijnlijk | positief
Bedrijfsgegevens	PBCI-CB1 - 4	Ik denk dat ik mijn bedrijfsgegevens kan beschermen tegen ongecontroleerde wijzigingen.	1 tot en met 5	onwaarschijnlijk/ waarschijnlijk | positief

Bedrijfsgegevens Back-up	PBCI-CB1 - 5	Ik denk dat ik mijn bedrijfsgegevens zeker kan stellen.	1 tot en met 5	onwaarschijnlijk/ waarschijnlijk | positief
Back-up	PBCI-CB1 - 6	Ik denk dat ik back-ups van mijn bedrijfsgegevens kan maken.	1 tot en met 5	onwaarschijnlijk/ waarschijnlijk | positief
Wachtwoordgebruik	PBCI-CB1 - 7	Ik denk dat ik een complex wachtwoord kan verzinnen.	1 tot en met 5	onwaarschijnlijk/ waarschijnlijk | positief
Wachtwoordgebruik	PBCI-CB1 - 8	Ik denk dat ik mijn wachtwoord periodiek kan wijzigen.	1 tot en met 5	onwaarschijnlijk/ waarschijnlijk | positief
Wachtwoordgebruik	PBCI-CB1 - 9	Ik denk dat ik mijn wachtwoord geheim kan houden.	1 tot en met 5	onwaarschijnlijk/ waarschijnlijk | positief
Wachtwoordgebruik	PBCI-CB1 - 10	Ik denk dat ik mijn wachtwoord kan onthouden.	1 tot en met 5	onwaarschijnlijk/ waarschijnlijk | positief
Trainings- en bewustwordingscampagnes	PBCI-CB1 - 11	Ik denk dat ik door bewustwordingscampagnes veiliger om kan gaan met mijn bedrijfsgegevens.	1 tot en met 5	onwaarschijnlijk/ waarschijnlijk | positief
Trainings- en bewustwordingscampagnes	PBCI-CB1 - 12	Ik denk dat ik door training veiliger om kan gaan met mijn bedrijfsgegevens.	1 tot en met 5	onwaarschijnlijk/ waarschijnlijk | positief

Power to influence

Trainings- en bewustwordingscampagnes	PBCI-PI1 - 1	Door bewustwordingscampagnes denk ik dat het … … is om veiliger met mijn bedrijfsgegevens om te gaan.	-2 tot en met +2	moeilijk/gemakkelijk | negatief
Trainings- en bewustwordingscampagnes	PBCI-PI1 - 2	Door informatiebeveiligingstraining denk ik dat het … … is om veiliger met mijn bedrijfsgegevens om te gaan.	-2 tot en met +2	moeilijk/gemakkelijk | negatief

Bedrijfsgegevens	PBCI-PI1 - 3	Ik vind het … … om mijn bedrijfsgegevens te beschermen tegen onbevoegde kennisname.	-2 tot en met +2	moeilijk/gemakkelijk | negatief
Bedrijfsgegevens	PBCI-PI1 - 4	Ik vind het … … om mijn bedrijfsgegevens te beschermen tegen ongecontroleerde wijzigingen.	-2 tot en met +2	moeilijk/gemakkelijk | negatief
Bedrijfsgegevens Back-up	PBCI-PI1 - 5	Ik vind het … … om mijn bedrijfsgegevens zeker te stellen.	-2 tot en met +2	moeilijk/gemakkelijk | negatief
Back-up	PBCI-PI1 - 6	Ik vind het … … om back-ups van mijn bedrijfsgegevens te maken.	-2 tot en met +2	moeilijk/gemakkelijk | negatief
Wachtwoordgebruik	PBCI-PI1 - 7	Ik vind het … … is om een complex wachtwoord te verzinnen.	-2 tot en met +2	moeilijk/gemakkelijk | negatief
Wachtwoordgebruik	PBCI-PI1 - 8	Ik vind het … … is om periodiek mijn wachtwoord te wijzigen.	-2 tot en met +2	moeilijk/gemakkelijk | negatief
Wachtwoordgebruik	PBCI-PI1 - 9	Ik vind het … … is om mijn wachtwoord geheim te houden.	-2 tot en met +2	moeilijk/gemakkelijk | negatief
Wachtwoordgebruik	PBCI-PI1 - 10	Ik vind het … … om mijn wachtwoord te onthouden.	-2 tot en met +2	moeilijk/gemakkelijk | negatief
Wachtwoordgebruik	PBCI-PI1 - 11	Ik vind het … … om volgens het wachtwoordbeleid veilig om te gaan met mijn wachtwoord.	-2 tot en met +2	moeilijk/gemakkelijk | negatief
Back-up	PBCI-PI1 - 12	Ik vind het … … om volgens het back-up beleid mijn bedrijfsgegevens te beschermen.	-2 tot en met +2	moeilijk/gemakkelijk | negatief

8.9 Bijlage Cronbach's alpha hoofdonderzoek

Tabel 60

Beschrijvende statistieken schaalgegevens van het hoofdonderzoek (n = 224): aantal items, gemiddelde schaal frequentie, standaarddeviatie van schaalscores en de Cronbach's α

Construct	Aantal items	Gemiddelde schaal frequentie	Standaarddeviatie schaalscores	Cronbach's α
Gedragsintentie				
Bedrijfsgegevens	3	2,143	1,464	,688
Back-up	3	5,336	2,310	,813
Wachtwoordgebruik	3	1,783	1,335	,624
Attitude toward the behavior				
Bedrijfsgegevens	15	36,291	6,024	,819
Back-up	10	20,196	4,494	,756
Wachtwoordgebruik	20	103,890	10,193	,874
Subjective norm				
Injunctive norm				
Bedrijfsgegevens	6	22,120	4,703	,850
Back-up	4	10,787	3,284	,747
Wachtwoordgebruik	8	37,331	6,110	,829
Descriptive norm				
Bedrijfsgegevens	3	6,162	2,482	,919
Back-up	2	3,181	1,784	,855
Wachtwoordgebruik	4	7,828	2,798	,772
Perceived behavioral control				
Self-efficacy				
Bedrijfsgegevens	6	16,134	4,017	,854
Back-up	6	17,486	4,182	,826
Wachtwoordgebruik	10	37,050	6,087	,853
Controllability				
Bedrijfsgegevens	6	19,245	4,387	,760
Back-up	6	18,651	4,319	,704
Wachtwoordgebruik	10	41,471	6,440	,761

8.10 Bijlage Scoring key

Tabel 61
Scoring key

Vraagcode	**Antwoordformaat**	**Cronbach's alpha**	**Spiegelen**	**Vraag formule**	**TpB construct onderdeel**
AI1 - 1 tot en met 3 AI2 - 1 tot en met 3 AI3 - 1 tot en met 3	1 tot en met 5	(AI11 + AI21 + AI31) (AI12 + AI22 + AI32) (AI13 + AI23 + AI33)	AI2		Generalised intention
AD1 - 1 tot en met 8 AD2 - 1 tot en met 8 AD3 - 1 tot en met 8 AD4 - 1 tot en met 8 AD5 - 1 tot en met 8	1 tot en met 5	(AD1, AD2, AD3, AD4 en AD5 - 1 tot en met 3) (AD1, AD2, AD3, AD4 en AD5 - 3 tot en met 4) (AD1, AD2, AD3, AD4 en AD5 - 5 tot en met 8)	AD2 en AD4		Direct measurement of attitude
					Indirect measurement of attitude: measuring behavioral beliefs and outcome evaluations
AIBB - 1 tot en met 5	1 tot en met 5			AIBB - 1 x AIOE - 1 AIBB - 2 x AIOE - 2 AIBB - 3 x AIOE - 2 AIBB - 4 x AIOE - 2 AIBB - 5 x AIOE - 2	Behavioral beliefs
AIOE - 1 en 2	-2 tot en met +2				Outcome evaluations

					Direct measurement of subjective norm
SND-IN1 - 1 tot en met 8 SND-IN2 - 1 tot en met 8	1 tot en met 5	((SND-IN1 - 1 tot en met 3) + (SND-IN2 - 1 tot en met 3)) ((SND-IN1 - 3 en 4) + (SND-IN2 - 3 en 4)) ((SND-IN1 - 5 tot en met 8) + (SND IN2 - 5 tot en met 8))	SND-IN1		Injunctive norm
SND-DN - 1 tot en met 8	1 tot en met 5	(SND-DN - 1 tot en met 3) (SND-DN - 3 en 4) (SND-DN - 5 tot en met 8)			Descriptive norm
					Indirect measurement of subjective norm: measuring normative beliefs and motivation to comply
SNINB-IN1 - 1 tot en met 8	-2 tot en met +2			(SNINB-IN1 - 1 x SNIMC-IDN - 1) (SNINB-IN2 - 1 tot en met 8 x SNIMC-IDN - 2) (SNINB-IN1 - 2 tot en met 8 x SNIMC-IDN - 3)	Normative beliefs (Injunctive norm)
SNINB-DN1 - 1	-2 tot en met +2				Normative beliefs (Descriptive norm)
SNIMC-IDN - 1 tot en met 3	1 tot en met 5				Motivation to comply
SNINB-IN2 - 1 tot en met 8	-2 tot en met +2				Normative beliefs (Injunctive norm)
SNINB-DN2 - 1 tot en met 8	-2 tot en met +2				Normative beliefs (Descriptive norm)

SNIMC-IDN - 4 tot en met 5	1 tot en met 5			(SNINB-DN1 - 1 x SNIMC-IDN - 4) (SNINB-DN2 - 1 tot en met 8 x SNIMC-IDN - 5)	Motivation to comply
					Direct measurement of perceived behavioral control (PBC)
PBCD-SE1 - 1 tot en met 10 PBCD-SE2 - 1 tot en met 10	1 tot en met 5	((PBCD-SE1 - 1 + 7 tot en met 10) + (PBCD-SE2 - 1 + 7 tot en met 10)) ((PBCD-SE1 - 2 + 5 en 6) + (PBCD-SE2 - 2 + 5 en 6)) ((PBCD-SE1 - 3 tot en met 5) + (PBCD-SE2 - 3 tot en met 5))	PBCD-SE1		Self-efficacy
PBCD-C1 - 1 tot en met 10 PBCD-C2 - 1 tot en met 10	1 tot en met 5	((PBCD-C1 - 1 + 7 tot en met 10) + (PBCD-C2 - 1 + 7 tot en met 10)) ((PBCD-C1 - 2 + 5 en 6) + (PBCD-C2 - 2 + 5 en 6))			Controllability

		((PBCD-C1 - 3 tot en met 5) + PBCD-C2 - 3 tot en met 5))			
					Indirect measures of PBC: Measuring control beliefs and their perceived power to influence behavior
PBCI-CB1 - 1 tot en met 10	1 tot en met 5			(PBCI-CB1 - 11 en 12 x BCI-PI1 - 1 en 2) (PBCI-CB1 - 1 en 2 x BCI-PI1 - 11 en 12) (PBCI-CB1 - 3 tot en met 10 x BCI-PI1 - 3 tot en met 10)	Control beliefs
PBCI-PI1 - 1 tot en met 10	-2 tot en met +2				Power to influence

8.11 Bijlage Bivariate correlaties

Tabel 62

Bivariate correlaties voor bedrijfsgegevens tussen de onafhankelijk directe en indirecte variabelen (n = 216)

		AD_1	SND_IN_1	SND_DN_1	PBCD_SE_1	PBCD_C_1
AI_1	Pearson Correlation	,484(**)	-	-	-	-
	Sig. (2-tailed)	,000	-	-	-	-
SNI_IN_NC_1	Pearson Correlation	-	,540(**)	-	-	-
	Sig. (2-tailed)	-	,000	-	-	-
SNI_DN_1	Pearson Correlation	-	-	,413(**)	-	-
	Sig. (2-tailed)	-	-	,000	-	-
PBCI_1	Pearson Correlation	-	-	-	,584(**)	,362(**)
	Sig. (2-tailed)	-	-	-	,000	,000

(** p < .01)

Tabel 63

Bivariate correlaties voor back-up tussen de onafhankelijk directe en indirecte variabelen (n = 216)

		AD_2	SND_IN_2	SND_DN_2	PBCD_SE_2	PBCD_C_2
AI_2	Pearson Correlation	,422(**)	-	-	-	-
	Sig. (2-tailed)	,000	-	-	-	-
SNI_IN_NC_2	Pearson Correlation	-	,567(**)	-	-	-
	Sig. (2-tailed)	-	,000	-	-	-
SNI_DN_2	Pearson Correlation	-	-	,414(**)	-	-
	Sig. (2-tailed)	-	-	,000	-	-
PBCI_2	Pearson Correlation	-	-	-	,651(**)	,474(**)
	Sig. (2-tailed)	-	-	-	,000	,000

(** p < .01)

Tabel 64

Bivariate correlaties voor wachtwoordgebruik tussen de onafhankelijk directe en indirecte variabelen (n = 216)

		AD_3	SND_IN_3	SND_DN_3	PBCD_SE_3	PBCD_C_3
AI_3	Pearson Correlation	,394(**)	-	-	-	-
	Sig. (2-tailed)	,000	-	-	-	-
SNI_IN_NC_3	Pearson Correlation	-	,595(**)	-	-	-
	Sig. (2-tailed)	-	,000	-	-	-
SNI_DN_3	Pearson Correlation	-	-	,403(**)	-	-
	Sig. (2-tailed)	-	-	,000	-	-
PBCI_3	Pearson Correlation	-	-	-	,648(**)	,357(**)
	Sig. (2-tailed)	-	-	-	,000	,000

(** p < .01)

9. GLOSSERY

Actual behavioral control: is de mate waarin een individu de vaardigheden, kennis, eigen middelen en andere eerste vereisten heeft om bepaald gedrag uit te voeren of te kunnen vertonen.

Attitude: is een relatief stabiele houding tegenover een concreet object zoals een voorwerp, individu, groep, organisatie, idee, bepaalde gebeurtenis of het eigen werk en de werksituatie.

Bedreiging(en): is een proces of een gebeurtenis die in potentie een verstorende invloed heeft op de betrouwbaarheid van objecten in de informatievoorziening.

Bedrijfsrol(len): zijn de verschillende rollen die medewerkers binnen de organisaties kunnen vervullen, te weten: managers, IT- specialisten en overige medewerkers.

Bedrijfstak: Hightech industrie, overige industrie, kennisintensieve dienstverlening, overige dienstverlening.

Behavioral beliefs: zijn de waargenomen gevolgen van een handeling die bestaat uit een combinatie van behavioral belief strength en outcome evaluation.

Behavioral information security: is het gedrag dat medewerkers in organisaties (kunnen) vertonen ten aanzien van informatiebeveiliging.

Belangrijke mensen: dit zijn referentiepersonen uit de omgeving van de medewerker, die voor hem of haar belangrijk zijn.

Beschikbaarheid: is het beschermen van gegevens tegen onbevoegde kennisname.

Betrouwbaarheid (betrouwbaar): is een verzamelnaam voor de aspecten beschikbaarheid, integriteit en vertrouwelijkheid waarmee bedreigingen worden onderverdeeld.

Bewustzijn: is het momentane besef van externe of interne stimuli, wat voorwerpen in de omgeving kunnen zijn (externe stimuli) en lichaamsgewaarwordingen, herinneringen, gevoelens of gedachten (interne stimuli).

Control beliefs: deze gaan in op de aanwezigheid van factoren die het gedrag kunnen vergemakkelijken of juist kunnen belemmeren.

Daadwerkelijk gedrag: is het feitelijk gedrag dat de manifestatie is van de waarneembare reactie bij een individu in een bepaalde situatie met betrekking tot een bepaald doel.

Emotie: is een intens gevoel voor iets of iemand.

Gedragsintentie: geeft aan hoe en hoever een individu bereid is om een bepaalde hoeveelheid inspanning te leveren om een bepaald gedrag te vertonen.

Hightech industrie: zijn onder andere chemische industrie, vervaardiging van machines, elektrische en optische apparaten, transportmiddelen.

Informatiebeveiliging: is een samenhangend geheel van technische en sociale benaderingen die er voor zorgen dat de informatievoorziening beschikbaar, integer en vertrouwelijk blijft.

Informatiebeveiligingsbewustzijn: is de mate waarin elke medewerker de volgende punten begrijpt: het belang van informatiebeveiliging, het niveau van informatiebeveiliging dat voor de organisatie noodzakelijk is en er ook naar handelt.

Informatievoorziening: is het geheel van IT-infrastructuur, gegevensinfrastructuur, applicaties en organisatie, dat tot doel heeft om te voorzien in de informatiebehoefte van de processen van een organisatie.

Insider threat: is een insider die regels bewust of onbewust overtreedt en daarmee de organisatie met of zonder opzet schaadt.

Integriteit: is het waarborgen dat gegevens niet ongecontroleerd worden gewijzigd of verloren gaan.

ISF: Information Security Forum.

Kennisintensieve dienstverlening: zijn onder andere telecommunicatie, informatietechnologie, onderzoeksbureaus, rechtskundige dienstverlening, accountants, architecten, ingenieurs, technische adviesbureaus en reclamebureaus.

Kwetsbaarheid: is de mate waarin de informatievoorziening gevoelig is voor bedreigingen.

Medewerkers: zijn zij die tot de groep eindgebruikers behoren binnen een organisatie.

Meta-analyse: is een onderzoek waarbij de gegevens ontleend worden aan de literatuur.

Modal salient beliefs: beliefs waarbij het gaat om zaken die bij een groep of populatie als gemeenschappelijke gedachten gelden.

Motivatie: is de bereidheid om iets te doen, afhankelijk van de mate waarin het mogelijk is om een behoefte van het individu te bevredigen.

N of n: is het aantal respondenten in dit onderzoek.

NIST: National Institute of Standards and Technology.

Non-response: de uitvallers bij een onderzoek. Het kan gaan om de respondenten die benaderd zijn, maar niet deelnemen aan een onderzoek.

Normative beliefs: zijn de normatieve verwachtingen of sociale druk (strength of normative beliefs) van andere mensen en motivaties (motivation to comply) om deze verwachtingen na te leven.

Organisatie: is een doelrealiserend samenwerkingsverband.

Overige dienstverlening: zijn onder andere (semi-)overheidsinstanties, productie en distributie van elektriciteit, aardgas en water, bouwnijverheid, handel en reparatie, horeca, vervoer, opslag en communicatie, verhuur van en handel in roerende en onroerende goederen, uitzendbureaus, beveiliging, reiniging en fotografie.

Overige industrie: zijn onder andere voedings- en genotmiddelen, textiel, houtindustrie, papierindustrie, vervaardiging van rubber, kunststof, glas, aardewerk, metaalproducten en meubels, scheepsbouw en –reparatie.

Perceived behavioral control: is de perceptie van een individu ten aanzien van zijn capaciteit en controle om bepaald gedrag uit te voeren.

Perceived ease of use: is de mate waarin een individu verwacht dat het gebruiken van de informatietechnologie gemakkelijk of moeilijk zal zijn.

Perceived usefulness: is de mate waarin de informatietechnologie als beter wordt gezien.

Perceptie: is het proces waarin individuen hun zintuiglijke indrukken ordenen en interpreteren om zin te geven aan hun omgeving.

Personal salient beliefs: gaan in op zaken die bij een individuele respondent uniek in zijn gedachten opkomen.

Persoonlijkheid: is de samenstelling van psychologische trekken die men gebruikt om individuen te classificeren.

Risico: is de gemiddelde schade over een gegeven tijdsperiode, die verwacht wordt doordat één of meer bedreigingen leiden tot een mogelijke (ver)storing van één of meer objecten van de informatievoorziening en wel zodanig dat dit leidt tot (ver)storing in de beschikbaarheid, integriteit en/of vertrouwelijkheid van de gegevensverwerking en informatievoorziening.

Salient beliefs: zijn de eerste zaken die bij een respondent in zijn gedachten opkomen.

Self-efficacy: zie **Perceived behavioral control**.

Subjective norm: is de norm die vanuit de sociale omgeving druk uitoefent op een individu om bepaald gedrag wel of niet te vertonen.

Thuisgebruiker: is een eindgebruiker die in de privésfeer arbeidsgedrag verricht voor de organisatie.

TpB: theorie van gepland gedrag.

Verstorende variabelen: zijn variabelen die verantwoordelijk zijn voor een vertekende weergave van de relatie tussen de primaire bestudeerde determinanten en de uitkomsten.

Vertrouwelijkheid: is het zekerstellen dat gegevens en informatiediensten op de gewenste momenten beschikbaar zijn voor gebruikers.

Werkextrinsieke motieven: zijn bijvoorbeeld veiligheid, promotie, salaris, status en werkomstandigheden wat extrinsiek aan het werk is.

Werkintrinsieke motieven: hebben te maken met de uitdaging die van het werk zelf uitgaat, zoals bijvoorbeeld erkenning, plezier in het werk en verantwoordelijkheid wat intrinsiek aan het werk is.

10. REGISTER

11. CONTACTGEGEVENS

Onderwerp: The human firewall of behavioral information security
Studierichting: Informatiekunde
Universiteit: Radboud Universiteit Nijmegen
Faculteit: Faculteit der Natuurwetenschap, Wiskunde & Informatica (FNWI)
Instituut: Nijmeegs Instituut voor Informatica en Informatiekunde (NIII)

Auteur: Michiel Dam
Afstudeernummer: 83 IK
Studentnummer: s0503304
E-mail adres: M.Dam@student.ru.nl

Auteur: Kevin Wessels
Afstudeernummer: 84 IK
Studentnummer: s0624454
E-mail adres: KJGWessels@student.ru.nl

Eerste begeleider: Prof. dr. B.P.F. Jacobs
Faculteit: Faculteit der Natuurwetenschap, Wiskunde & Informatica
E-mail adres: bart@cs.ru.nl

Tweede begeleider: Drs. G.P.A. Bergers
Faculteit: Faculteit der Sociale Wetenschappen
E-mail adres: G.Bergers@psych.ru.nl

Eerste referent: Dr. P.J. van Rossum
Faculteit: Faculteit der Natuurwetenschap, Wiskunde & Informatica
E-mail adres: petervr@cs.ru.nl

Tweede referent: Prof. dr. E. Barendsen
Faculteit: Faculteit der Natuurwetenschap, Wiskunde & Informatica
E-mail adres: E.Barendsen@cs.ru.nl