# Informatiebeveiliging- een gedragsbenadering



# Informatiebeveiliging – een gedragsbenadering

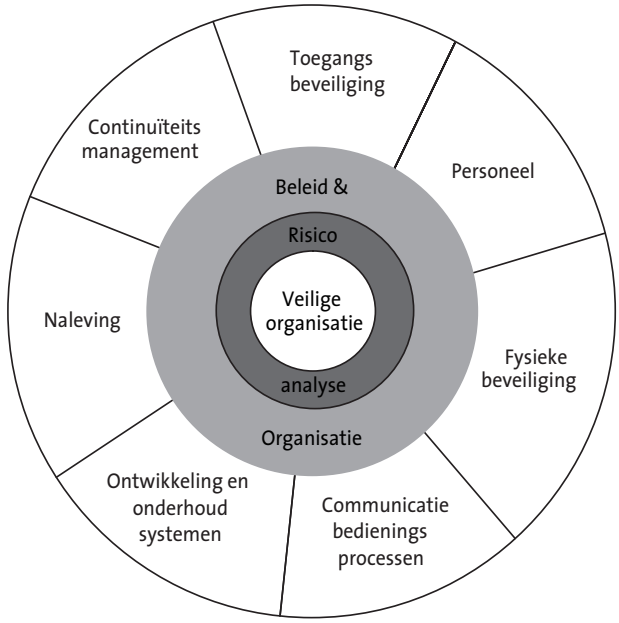
Marcel Koers en Arno Nuijten

Organisaties worden geconfronteerd met de problematiek rond informatiebeveiliging. Managers en security officers zijn verantwoordelijk voor het structureren en implementeren van beveiligingsmaatregelen en moeten in toenemende mate daarover verantwoording afleggen aan belanghebbende partijen en toezichthouders. IT-auditors spelen een belangrijke rol in het beoordelen van de mate waarin de organisatie haar beveiligingsrisico's beheerst.

**Drs A.L.P. Nuijten RE** werkt als zelfstandig IT-auditor en adviseur. Hij is docent en onderzoeker bij de Erasmus Universiteit. Daarbij richt hij zich vooral op de vraag hoe informatie over IT-risico's de besluitvorming beïnvloedt.

**Dhr. A.F. Koers** werkt als management consultant en IT-auditor bij Ordina Security & Risk Management.

Om op een gestructureerde en marktconforme wijze de beveiligingsmaatregelen in te richten en te beoordelen wordt vaak de Code van Informatiebeveiliging (ofwel ISO17799:2005) gehanteerd. Zoals figuur 1 weergeeft, bakent de Code domeinen af en beschrijft het een groot aantal te treffen beheersmaatregelen ('controls'). Aan de basis van het treffen van maatregelen staat een analyse van beveiligingsrisico's.




Figuur 1. Positionering Code van Informatiebeveiliging

Voor ieder domein van de Code van Informatiebeveiliging neemt de organisatie een aantal technische, procedurele en organisatorische maatregelen zodat een 'veilige organisatie' wordt bewerkstelligd. De IT-auditor beoordeelt per domein van de Code of de maatregelen daadwerkelijk getroffen zijn. Hierin zit de veronderstelling dat het geheel aan getroffen maatregelen conform de Code een effectieve bijdrage levert aan een 'veilige' organisatie.

Wij vragen ons echter af of een organisatie die de Code toepast daarmee automatisch de beveiligingsrisico's met betrekking tot het personeel effectief beheerst. Onder 'beheersen' verstaan wij dat doelstellingen worden bepaald, maatregelen worden getroffen, effecten worden gemeten en dat wordt bijgestuurd, in dit geval op (on)veilig gedrag van medewerkers.

In de Code wordt personeel namelijk als een verbijzonderd domein benaderd. Maatregelen binnen dit domein vinden we in de praktijk terug als bewustwordingscampagnes, flyers, e-learning modules en het communiceren van beveiligingsincidenten (hopelijk bij concurrenten). Deze maatregelen maken de mensen in de organisatie bewust van het belang van een adequate informatiebeveiliging.
In de praktijk zien wij ook dat maatregelen gericht op het beveiligingsbewustzijn van personeel als een separaat traject worden ingericht. Ook de IT-auditor die de informatiebeveiliging toetst aan de Code zal voor maatregelen gericht op beveiligingsrisico's van het personeel veelal op zoek gaan naar de security-awareness programma's en vaststellen dat er een clean desk policy en een gedragscode is opgesteld en gecommuniceerd. Daarmee worden mogelijk de voorgeschreven maatregelen en aandachtspunten van het domein 'personeel' geadresseerd en bij een formele toetsing door de IT-Auditor zelfs goedgekeurd. De kern van de problematiek wordt echter daarmee mogelijk onvoldoende geraakt, namelijk of het gewenste "veilig gedrag" wordt bereikt en beheerst. Dit is een onbevredigende constatering als je in ogenschouw neemt dat:

- Daarmee de doelmatige inzet van budgetten op het gebied van informatiebeveiliging onvoldoende wordt zeker gesteld;
- Veel van de beveiligingsincidenten die de laatste jaren in de publiciteit zijn gekomen, juist werden veroorzaakt door menselijke fouten of onachtzaamheid (onveilig gedrag);
- De effectiviteit van technische en procedurele beveiligingsmaatregelen veelal onderhevig is aan (on)veilig gedrag van de medewerkers, met als voorbeelden het onzorgvuldig omspringen met Pincode, toegangspas, e-mail, USB-sticks en notebooks.

Daarom vinden wij het van belang om in dit artikel 'informatiebeveiliging' te beschouwen vanuit het perspectief 'veilig gedrag' van medewerkers binnen een organisatie. Dit is dus een ruimere scope dan alleen het domein 'personeel' binnen de Code. Omdat medewerkers 'actoren' zijn binnen de vele processen en beheersmaatregelen uit de overige domeinen (bijvoorbeeld wijzigingsbeheer, toegangsbeveiliging en beschikbaarheidsbeheer) strekt de problematiek van onveilig gedrag zich ook uit over die domeinen.
De centrale vraag voor dit artikel is daarom of er vanuit een gedragsinvalshoek een model kan worden uitgewerkt dat bijdraagt aan een betere beheersing van (informatie)risico's door onveilig gedrag van het personeel.

Voor de beantwoording van deze vraag worden in dit artikel de volgende deelvragen onderzocht:

a) Is volgens de literatuur gedrag van mensen in organisaties te beïnvloeden en door middel van welke variabelen/factoren is dit gedrag te beïnvloeden?
b) Is op basis hiervan een model uit te werken gericht op de beheersing van risico's door 'onveilig gedrag' van de medewerkers.

De indeling van dit artikel volgt deze vraagstelling. Paragraaf 2 beantwoordt de vraag of veilig gedrag van medewerkers te beïnvloeden is en via welke variabelen. In paragraaf 3 wordt dit uitgewerkt tot een beheersingsmodel gericht op 'veilig gedrag' van medewerkers. Om het model operationeel te maken wordt in paragraaf 4 een voorbeeld uitgewerkt waarin wordt ingegaan op doelstellingen, maatregelen, meting en bijsturing van risico's van onveilig gedrag.

In paragraaf 5 sluiten wij dit artikel af met conclusies ten aanzien van de vraagstelling van dit artikel. Daarbij beschrijven wij in welke zin het uitgewerkte model voor security officers en IT-auditors een aanvulling zou kunnen vormen op de Code van Informatiebeveiliging. Daarbij worden tevens kanttekeningen geplaatst bij het beschreven model.

## Beïnvloedingsfactoren van (on)veilig gedrag

In deze paragraaf staat de vraag centraal of veilig gedrag van medewerkers te beïnvloeden is en welke factoren/variabelen daarbij een rol zouden kunnen spelen.

Voor de beantwoording van deze vraag hebben wij literatuur onderzocht op het gebied van organisatiecultuur, omdat collectief gedrag in organisaties daarmee wordt geassocieerd. Daarnaast is onderzocht of literatuur uit het vakgebied 'behavioral control' inzicht verschaft in eventuele factoren die (on)veilig gedrag binnen organisaties zouden kunnen verklaren en wellicht beïnvloedbaar maakt.

### Cultuur

Allereerst gaan wij na of literatuur over organisatiecultuur duidelijke aanknopingspunten geeft voor het verklaren en beïnvloeden van (on)veilig gedrag binnen organisaties. Daarbij dient natuurlijk eerst vastgesteld te worden wat onder 'cultuur' wordt verstaan en in hoeverre de gedragscomponent daarin wordt belicht.

Hofstede (Hofstede,1980) definieert cultuur als de collectieve programmering van de geest die de ene groep mensen van een andere onderscheidt. Simons (Simons,1992)
geeft een soortgelijke definitie, namelijk het systeem van door leden gedeelde zingeving, waardoor de ene organisatie zich van de ander onderscheidt. Beide definities zien cultuur niet als gedrag, maar als gedeelde normen en waarden onder mensen en hoe die zich manifesteren (onder andere in gedrag). Het tweede element uit de definitie betreft dat juist cultuur groepen mensen van elkaar onderscheidt.

Schein (Schein, 1992) komt met de volgende definitie van cultuur: 'a pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way you perceive, think, and feel in relation to those problems.'

Geen enkele van bovenstaande definities stelt specifiek gedrag van de medewerker of groepen medewerkers centraal. Cultuur wordt gezien als collectieve normering over dat wat gangbaar is in een organisatie, of juist niet. Een normering ook die volgens Schein aan verandering onderhevig is en kan worden aangeleerd (door nieuwe medewerkers).

Ons literatuuronderzoek leert dat organisatiecultuur zeker van invloed is op het gedrag (en dus wellicht ook veilig/onveilig gedrag) van medewerkers. Het verband tussen cultuur en gedrag resulteert echter niet in de beïnvloedingsfactoren voor gedrag waarnaar wij op zoek zijn. Omdat in de literatuur (Morgan, 1997) ook naar voren komt dat beïnvloeding van de organisatiecultuur complex is, lijkt het niet voor de hand liggend dat beïnvloeding van gedrag van medewerkers het meest direct en meetbaar te realiseren is via een cultuurverandering. Cultuur biedt daarom onvoldoende aanknopingspunten voor een uit te werken beheersingsmodel.

**Gedrag**

Studie van gedragsliteratuur levert op dat 'motivatie' een belangrijke factor is die het gedrag van mensen bepaalt en die te beïnvloeden is.

*Motivatie* wordt door Thierry (Thierry, 1989) omschreven als het proces dat zowel datgene betreft waarop een mens zich oriënteert als het specifieke handelen (gedrag) om dat doel te bereiken. In de motivatietheorieën zijn 2 stromingen te onderkennen: de zogenoemde 'need' theorieën en 'goal' theorieën (Vroom, 1964). De 'need' theorieën nemen als uitgangspunt dat als op een bepaald gebied of in een bepaalde behoefte bij de medewerker een tekort ontstaat, deze persoon gemotiveerd raakt om die behoefte te bevredigen. De 'goal' theorieën redeneren vanuit het feit dat een medewerker bepaalde doelen of opbrengsten aantrekkelijk vindt, waardoor hij zich inzet om deze te bereiken.

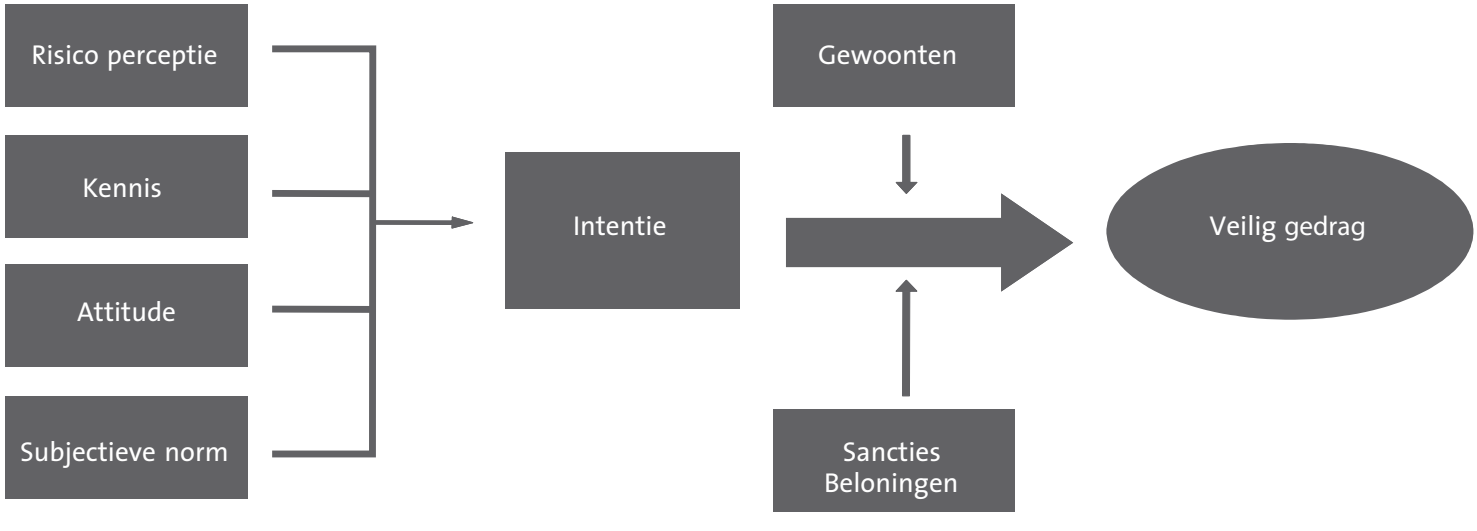
*Motivatie* zou een beïnvloedbare factor kunnen zijn gericht op het bewerkstelligen van veilig gedrag bij medewerkers. Dit veronderstelt echter dat medewerkers een intrinsieke behoefte hebben aan informatiebeveiliging, zodat deze behoefte of een tekort aan informatiebeveiliging hen motiveert tot veilig gedrag. Deze veronderstelling wordt in de praktijk niet bevestigd. Informatiebeveiliging wordt eerder als lastig dan als aantrekkelijk ervaren. Anders was er geen probleem geweest. Motivatietheorie lijkt derhalve onvoldoende aanknopingspunten te geven voor het beïnvloeden van veilig gedrag van medewerkers.

De (negatieve) attitude die velen hebben ten opzichte van informatiebeveiliging zal onderdeel moeten uitmaken van het gedragsmodel.

Een in de jaren '70 en '80 ontwikkeld model van Fishbein en Ajzen (Fishbein, 1975) beschouwt *attitude* als één van de factoren die van invloed kan zijn op het gedrag van mensen. Hun model staat bekend onder de naam Theory of Reasoned Action (TRA) en heeft zich geëvolueerd tot de Theory of Planned Behavior (TPB). Zij voegen een schakel toe tussen attitude en gedrag. Leidt een veranderende attitude niet direct tot ander gedrag, dan zeker wel tot een andere *intentie* bij de persoon dat gedrag te willen vertonen.

*Attitude* omschrijven zij als het gevoel van iemand, negatief of positief, bij het verrichten van een bepaald gedrag (Fishbein, 1975). Plausibel is, dat iemand die een negatieve attitude ten opzichte van beveiliging erop nahoudt, zeker niet bereid is een inspanning te leveren voor veilig gedrag. Plausibel is ook, dat als iemand eerder last ondervindt van bepaalde veiligheidsmaatregelen, hij of zij een negatieve attitude vormt.

*Intenties* vormen in het model van Fishbein en Ajzen de belangrijkste determinant voor gedrag, daarmee de gedachte




Figuur 2. Gedragsmodel voor informatiebeveiliging

vormgevend dat de mens bewust bepaald gedrag vertoont. Intenties van mensen zijn volgens Fishbein en Ajzen wel degelijk te beïnvloeden. Intentie wordt volgens hen niet alleen gevormd door de attitude, maar tevens door *subjectieve groepsnorm*[1], en de behoefte van een individu zich hieraan te conformeren.

In een later stadium is door Ajzen nog 'perceived behavior control' of 'self efficacy' toegevoegd. Het denkbeeld bij het individu over hoe moeilijk het is bepaald gedrag succesvol te vertonen, beïnvloedt ook zijn of haar gedrag.

#### Gedragsmodel voor informatiebeveiliging

Het model van Fishbein & Ajzen is toepasbaar voor informatiebeveiliging. De gedachte dat intenties van medewerkers, en daarmee gedrag, te beïnvloeden is, biedt goede aanknopingspunten voor het uit te werken "beïnvloedings"-model. In het toepasbaar krijgen van het model zijn die factoren van belang waarop invloed kan worden uitgeoefend, en die meetbaar zijn. *Attituden* en *subjectieve normen* zijn aan verandering onderhevig en te meten, bijvoorbeeld door de toepassing van de Likert-schaal.
Vanuit het vakgebied informatiebeveiliging spelen nog enkele specifieke zaken die intenties bij medewerkers beïnvloeden. Bewustwording is bijvoorbeeld een belangrijk thema, gezien de dominante betekenis die aan awarenesscampagnes wordt toegekend. Als algemeen onderkende problemen worden een gebrek aan kennis over informatiebeveiliging onder medewerkers of een verkeerde risicoperceptie over de eventuele gevolgen van bepaald gedrag bij medewerkers genoemd (Wouters, 2002).

Het model Fishbein en Ajzen gekoppeld aan de specifieke aandachtspunten voor bewustwording over informatiebeveiliging levert een model op voor gedragsbeïnvloeding, zoals weergegeven in figuur 2.
In dit model zijn de mogelijkheden voor het beïnvloeden van de intentie van een individu of groepen individuen:

- de kennis van een individu op het gebied van informatiebeveiliging; wat zijn kenmerkende bedrijfsrisico's, hoe is de classificatie van de informatie waarmee men werkt, wat is het huidige beleid, welke maatregelen zijn van kracht; kennis is toetsbaar en bijvoorbeeld te beïnvloeden door middel van trainingen en bij het aannemen van personeel;
- de risicoperceptie die een individu ervaart ten aanzien van informatieverlies of -schade; risicoperceptie is te meten en is bijvoorbeeld te beïnvloeden door middel het verschaffen van risico-informatie;
- de attitude van een individu waarmee hij of zij beveiligingszaken waardeert of niet waardeert; attitude is te meten en bijvoorbeeld te beïnvloeden door positieve ervaringen met beveiliging;
- de subjectieve norm van een individu die ontstaat door hoe hij of zij denkt dat de directe omgeving bepaald gedrag waardeert of niet waardeert; deze subjectieve norm is te meten en bijvoorbeeld te beïnvloeden door duidelijkheid te creëren over wat wel en niet toelaatbaar wordt geacht.

Of de medewerker het gedrag ook daadwerkelijk vertoont, of intenties worden omgezet naar gedrag, kan afhangen van andere stimuli, vooral door sancties en beloningen.

Verder worden 'gewoonten' of 'habits' genoemd als een belangrijke determinant voor het feitelijke gedrag. Gewoonten zijn vormen van gedrag die onbewust plaatsvinden en waarbij de medewerker geen verdere afweging maakt over waarom hij of zij dit doet. De deur op slot draaien thuis, belangrijke papieren direct opbergen, zijn vormen van gewoonten. Het beïnvloeden van gewoontes volgens Maslow (Maslow, 1954) kan plaatsvinden door mensen eerst bewust te maken van onveilig gewoontegedrag, hen er vervolgens toe aan te zetten dat zij bewust veilig gedrag gaan vertonen, die vervolgens onderdeel gaat uitmaken van hun (onbewust) veilig gewoontegedrag.

In deze paragraaf hebben wij aan de literatuurstudie over gedrag een model ontleend dat bruikbaar wordt geacht voor het beïnvloeden van (on)veilig gedrag in organisaties.

### Besturingsmodel voor veilig gedrag

Nu we enig inzicht hebben verkregen in de beïnvloedbaarheid van veilig gedrag binnen een organisatie, is nu de vraag of een structurele en doelgerichte beïnvloeding van veilig gedrag mogelijk is. Daarbij hebben wij niet de illusie dat alle veilig gedrag 'maakbaar' is, maar een zekere mate van management-control over de risico's door onveilig gedrag binnen de organisatie is wenselijk en interessant genoeg om uit te werken. Daartoe doen wij in deze paragraaf een aanzet, op basis van de eerder uitgewerkte beïnvloedingsfactoren.

Management control vereist dat sprake is van een continu cyclisch proces van doelen bepalen, maatregelen implementeren, effecten meten en het bijstellen van doelen en maatregelen. Een eenmalige of periodieke losstaande awareness campagne of andersoortige "gedragsinterventie" leidt daarom niet tot management control.

Onderstaand werken wij ons model uit, waarin de onderwerpen doelbepaling, implementatie, meting en bijsturing aan de orde komen.

#### Doelbepaling

Doelbepaling is noodzakelijk om budgetten en instrumenten ter beïnvloeding van veilig gedrag effectief en efficiënt in te zetten. Daarom dienen we te bepalen welk veilig gedrag van medewerkers we nastreven (of onveilig gedrag we willen voorkomen). Aan welke vormen van (on)veilig gedrag we in een organisatie prioriteit wensen te geven kan niet worden los gezien van de karakteristieken van de organisatie en het

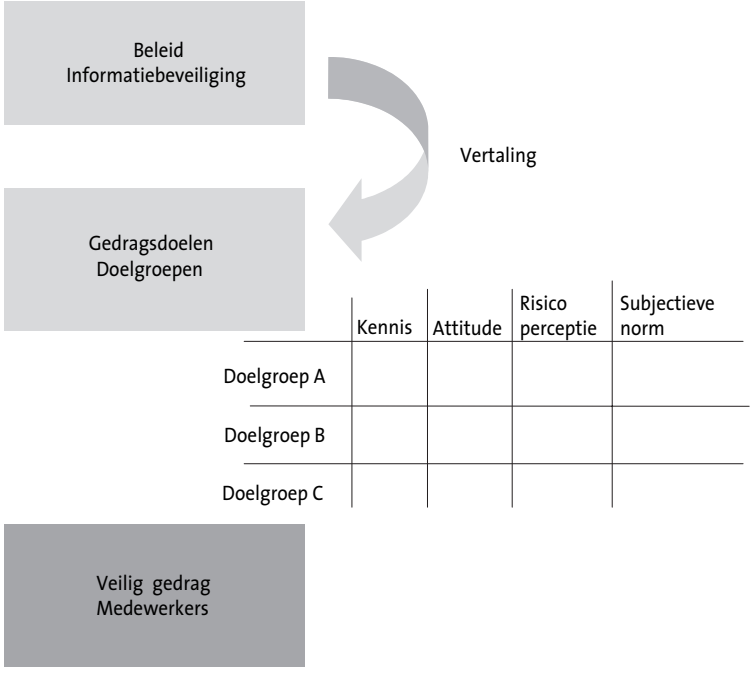
beleid voor informatiebeveiliging ('wat vinden we belangrijk').

De Code geeft vele handreikingen over wat onder veilig gedrag kan worden verstaan, zoals 'clear desk', het classificeren van informatie, het veiligstellen van informatiemiddelen, het gebruik van screensavers, bewustzijn over wat waar tegen wie wordt gezegd, tijdig je gegevens veiligstellen door backups et cetera. Deze zijn echter veeleer gekoppeld aan maatregelen dan aan gedragsdoelen.

Vanuit het beleid van informatiebeveiliging en analyse van beveiligingsrisico's bepalen wij gedragsdoelen: welk veilig gedrag willen we realiseren en welk onveilig gedrag willen we voorkomen.

Niet van alle individuen in de organisatie wordt hetzelfde gedrag verwacht. Leidinggevenden hebben bijvoorbeeld een voorbeeldfunctie en een aansturende rol. Zij sanctioneren en belonen bepaald gedrag.
Een buitendienstmedewerker werkt met andere informatie en gebruikt andere middelen dan de persoon op de crediteurenadministratie. De IT-ontwikkelaars binnen het bedrijf dienen 'veilige' programma's en web-sites te bouwen. Wat de organisatie van verschillende medewerkers verwacht in termen van veilig gedrag, is verschillend.

Door doelgroepen te onderscheiden in het stellen van gedragsdoelen kan veilig gedrag expliciet gemaakt worden. Op deze manier worden de doelen gerelateerd aan de werkbeleving van specifieke groepen medewerkers en hun specifieke gebruik van informatie of informatiemiddel. Gedragsdoelen dienen zo gekozen te worden, dat het past binnen de mogelijkheden van de medewerker zich er aan te kunnen houden, hetgeen Fishbein en Ajzen aanduiden als Perceived Behavioral Control.




Figuur 3. Van Beleid naar veilig gedrag

Los van het bovenstaande blijft overeind dat bepaalde vormen van veilig gedrag organisatiebreed gelden (denk bijvoorbeeld aan de toegangsregeling tot panden, het gebruik van USB-geheugen, e-mail et cetera).

In figuur 3 vindt u een schematische weergave van het bepalen van gedragsdoelen voor veilig gedrag. Daarbij worden deze gedragsdoelen tevens gekoppeld aan de eerder beschreven beïnvloedingsfactoren. Hierdoor kan worden nagegaan of verbeteringsimpulsen op kennis, attitude et cetera een zinvolle bijdrage leveren aan het gewenste veilig gedrag.

**Meting en bijsturing**
Meten vormt een logisch beginpunt voor het treffen van maatregelen. Het is zinvol om na het formuleren van een gedragsdoel eerst de huidige situatie vast te stellen. Het meetinstrumentarium richt zich op de intentievariabelen onder de medewerkers of groepen medewerkers. Enquêtes of ander vormen van metingen maken duidelijk waaraan het schort. Het geeft aan wat het probleem is door vast te stellen of het onkunde is, gebrek aan kennis, een attitude probleem of het ontbreken van een groepsnorm? Een combinatie van bovenstaande intentievariabelen is ook mogelijk.

De diagnose leidt tot een probleemdefinitie als startpunt voor een interventieprogramma (Gerichhauzen, 1994). Hetzelfde meetinstrumentarium wordt na het uitvoeren van het pakket van interventies ingezet om de verandering te meten. Het meet de effecten van de ondernomen acties. Op basis van dit vervolgonderzoek wordt de probleemstelling bijgesteld en dit vormt het startpunt van een nieuw pakket aan interventies met de leerpunten van en de aanpassingen op de eerste cyclus.

**Implementatie van maatregelen**
Implementatie van maatregelen gericht op gedragsverandering vindt plaats in de vorm van interventieprogramma's (Gerichhauzen, 1994), zijnde een pakket van maatregelen die in samenhang bijdragen tot de beoogde gedragsverandering.

Om de maatregelen binnen een interventie-programma in samenhang te brengen (zodat ze elkaar over en weer versterken) gebruiken wij het 7S-en model van McKinsey (Peters, 1982), voor deze specifieke toepassing enigszins aangepast, zoals weergegeven in figuur 4. Centraal in dit zogenoemde 'bollen'-model staat het gewenste gedragsdoel, het doel van gestructureerd interveniëren.

Het model plaatst de genoemde maatregelen of best practices uit de Code in een ander daglicht. De maatregelen uit de Code kunnen worden opgevat als interventies. Door deze te relateren aan gedragsdoelen, ontstaat op de eerste plaats een

goede afweging of de manier van interveniëren wel past binnen de diagnose en opgestelde probleemdefinitie, en of de maatregelen leiden tot het gewenste effect.

Vanuit de vijf bollen zijn allerlei vormen van interventies op te starten. Een aantal trefwoorden voor het doen van interventies worden genoemd in de kaders van het 'bollen'-model.

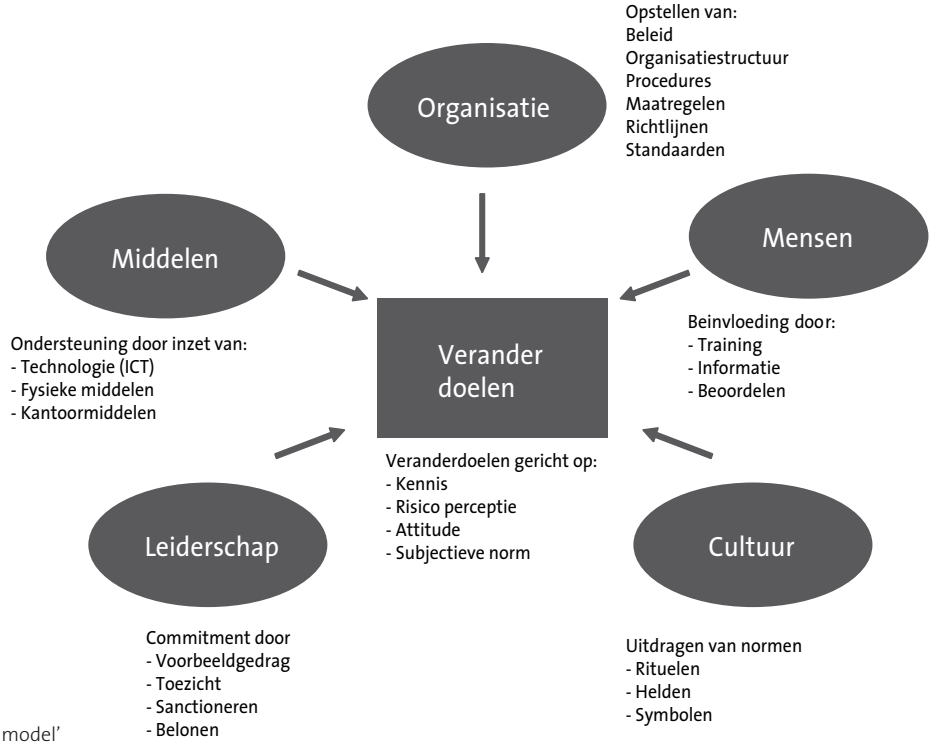
De eerste bol is 'Structuur'. Deze bol definieert alle elementen van de formele organisatie. Voorbeelden van interventies voor informatiebeveiliging op dit gebied betreffen een gedragscode, functiescheiding, beleid, standaarden, instructies et cetera. Succesvolle interventies op dit gebied zijn vooral van invloed op de intentievariabelen kennis en subjectieve norm. Instructies en standaarden zijn vormen van kennis waarlangs (informatie)processen plaatsvinden. Ook wordt daarmee door de organisatie aan de medewerker een norm opgelegd: zo moet het.

'Leiderschap' in het bollenmodel richt zich op de formele leiding van de organisatie, of het management. Vooral direct leidinggevenden zullen commitment ten opzichte van het veranderdoel moeten tonen, door bijvoorbeeld voorbeeldgedrag, overdragen van kennis, belonen, sanctioneren en toezicht. Dergelijke handelingen worden in het model opgevat als interventies. Coaching en ondersteuning door de Security Officer is daarbij van belang. Hier geldt dat succesvolle interventies op dit gebied vooral van invloed zijn op de intentievariabele subjectieve norm.

De derde bol is 'Cultuur'. Na de eerdere verhandeling over cultuur is het een terechte vraag hoe dit begrip als een middel terugkomt. De bol 'Cultuur' geldt hier echter als een containerbegrip aan interventies met vooral een visuele uitwerking. Soeters in (Gerrichhauzen, 1994) kent cultuur een aantal dimensies toe, waaronder 'vorm'. Bij de verdere invulling van deze dimensies sluit hij aan bij de indeling van Hofstede in symbolen, helden, rituelen en waarden. Waarden zijn niet als beïnvloedingsinstrument in te zetten, maar visualisatie in de vorm van symbolen, helden en rituelen wel. Zo kunnen posters, kubussen of andere speeltjes met boodschappen op het gebied van informatiebeveiliging, worden opgevat als symbolen, het benoemen van ambassadeurs onder medewerkers als helden en een maandelijkse terugkerende stiptheidsactie voor 'clear desk' als een ritueel.

Door te werken met symbolen, helden en rituelen als denkkader kan met de nodige creativiteit interventies worden verzonnen die inzetbaar zijn als onderdeel van een veranderingstraject. De intentievariabelen die hiermee worden beïnvloed, betreffen vooral de subjectieve norm in de organisatie en de attitude van de medewerker.

De vierde bol is de bol 'Mensen'. Het zijn de medewerkers die uiteindelijk invulling geven aan het gedragsdoel. Denkend in de intentievariabelen betreffen het hier vooral interventies op het gebied van kennis en risico perceptie. Deze bol is bedoeld de medewerkers een meer diepgaand begrip over de noodzaak van het gestelde gedragsdoel te geven, eventueel uitgebreid met verdergaande instructies. Trainingen in de vorm van bijvoorbeeld workshops zijn vooral bedoeld samen met de medewerker een goed beeld van de risico's te creëren. Afhankelijk van het te stellen gedragsdoel zijn interventies meer of minder intensief.




Figuur 4: 'bollenmodel'

De laatste bol is de bol 'Middelen'. De bol neemt een bijzondere plaats in. Onder deze bol worden alle technologische of andere middelen bedoeld, die ingezet worden om een bepaald gedragsdoel te bereiken. De bol is bijzonder, omdat door goed gekozen interventies gedrag direct afgedwongen wordt. Een 'smartcard' voor het inloggen op het netwerk betekent dat naast het wachtwoord ook een toegangskaart nodig is. Daarmee is verondersteld dat een hoger niveau van veiligheid wordt bereikt doordat het delen van elkaars wachtwoord aan banden wordt gelegd. Omdat natuurlijk altijd nog de toegangskaart met elkaar gedeeld kan worden, is het van belang om deze beveiligingsmaatregelen te blijven relateren aan (onveilig) gedrag.

**Verzekeringsbedrijf**

Het beschreven model wordt als voorbeeld uitgewerkt voor een verzekeringsmaatschappij. Er worden hoge eisen gesteld aan de interne bedrijfsvoering van verzekeringsbedrijven. Regelgeving is aan ingrijpende veranderingen onderhevig met belangrijke gevolgen voor de interne administratie van de verschillende verzekeringsvormen, zoals medische zorg, pensioen en arbeidsongeschiktheid. Tegelijkertijd stappen klanten makkelijker over naar de concurrent en is er sprake van reorganisaties en fusies.

Een significant deel van de activiteiten van een verzekeringsmaatschappij is 'mensenwerk' (bijvoorbeeld het te woord staan van klanten, beoordelen van dossiers) waarbij gebruik gemaakt wordt van gevoelige informatie. Het mag duidelijk zijn dat het zorgvuldig en veilig omgaan met klantgegevens cruciaal is voor een verzekeringsmaatschappij.
Vandaar dat in deze branche intensief gewerkt wordt aan informatiebeveiliging, vaak conform de Code voor Informatiebeveiliging. De vraag is of middelen daarmee effectief en doelmatig worden ingezet. Dragen de ingerichte maatregelen daadwerkelijk ertoe bij dat 'veiliger' wordt gewerkt? Wordt het gedrag van medewerkers echt beïnvloed? Kortom, zijn interventies effectief?

Binnen het verzekeringsbedrijf onderkennen we de volgende doelgroepen:
- Het management
- De verzekeringsmedewerkers
- De IT-medewerkers

Op basis van de risicoanalyse conform de Code voor Informatiebeveiliging kwam naar voren dat een tweetal beveiligingsrisico's prominent aanwezig zijn:
- het gebruik van e-mail voor het versturen van vertrouwelijke informatie;
- het gebruik van mobiele gegevensdragers, in het bijzonder USB-sticks.

**Het versturen van e-mail**

De zorg over het gebruik van e-mail richt zich op de doelgroepen: het management (informatie over de bedrijfsresultaten), de verzekeringsmedewerkers (informatie over klanten en schades) en de IT-medewerkers (informatie-uitwisseling met IT-leveranciers over projecten en systemen).
Analyse van het e-mail verkeer heeft geleerd dat medewerkers niet altijd gebruik maken van de procedure om vertrouwelijke informatie voldoende beveiligd te versturen. Het gedrag staat in contrast met het gestelde beleid. Op basis hiervan wordt het volgende gedragsdoel vastgesteld:

Management, verzekeringsmedewerkers en IT-medewerkers versturen geen vertrouwelijke informatie per e-mail naar derden zonder de inzet van aanvullende beveiligingsmaatregelen.

Nader onderzoek is nodig voor het opzetten en inrichten van een interventieprogramma dat deze situatie bewerkstelligt. Met een enquête wordt het volgende over de intentievariabelen vastgesteld:

| Intentie-variabele | Bevinding |
|---|---|
| Kennis | Doelgroepen hebben onvoldoende kennis over de spelregels in het gebruik van e-mail. Dit komt omdat de regels onvoldoende zijn uitgewerkt en niet gecommuniceerd. Ook is het voor betrokkenen niet duidelijk wanneer informatie vertrouwelijk is. |
| Risico perceptie | Doelgroepen ervaren e-mail niet als onveilig. Het feit dat berichten onderschept kunnen worden of niet juist bezorgd, zien zij als een gering gevaar dat sporadisch optreedt. |
| Attitude | Doelgroepen staan niet negatief tegenover nader te stellen regels over het gebruik van e-mail verkeer. Zij zien wel de risico's als mailverkeer in de verkeerde handen komt. Zij hebben nooit stilgestaan bij het gebruiken van e-mail en over wat wel kan of niet kan. |
| Subjectieve norm | Doelgroepen geven aan elkaars gedrag nooit ter discussie te stellen, nooit elkaar hierop aan te spreken. Er is geen sprake van een groepsnorm op het gebied van e-mail verkeer. |

Uit onderzoek naar het gebruik van e-mail in termen van de intentievariabelen blijkt dat het probleem zich vooral manifesteert door een gebrek aan kennis, een onjuist risico perceptie en de subjectieve norm. Een op te stellen interventieaanpak richt zich op deze elementen.

De interventieaanpak is een sociotechnisch verandertraject met het zwaartepunt van interventies in de bollen 'Leiderschap', 'Mensen' en 'Cultuur'. De volgende interventies worden verricht:

| Bol | Interventies |
|---|---|
| Structuur | • Classificatiemodel dat aangeeft welke informatie vertrouwelijk is.<br>• E-mail verkeer opnemen in de gedragscode, met daarin de sancties bij foutief gebruik. |
| Leiderschap | • Actief uitdragen van de norm door de directie van de onderneming door communicatie hierover en voorbeeldgedrag.<br>• Periodieke terugkoppeling aan directie over stand van zaken en vastgestelde overtredingen (incidenten). |
| Mensen | • Brochure met uitleg over hoe e-mail binnen de organisatie wordt gebruikt, de risico's van verkeerd gebruik, de gedragscode en verdere uitleg van het e-mailproduct. |
| Cultuur | • Screensavers met een compacte boodschap over hoe e-mail te gebruiken.<br>• Terugkerende boodschap aan doelgroepen in het personeelsblad.<br>• Melding in de headers van e-mails of elektronische communicatie indien het vertrouwelijke informatie betreft en niet naar buiten mag. |
| Techniek | • E-mail wordt altijd voorzien van classificatie voordat het kan worden verstuurd. Techniek voorkomt dat vertrouwelijke informatie naar buiten gaat.<br>• Monitoring van mailverkeer op juiste toepassing van het classificatiemodel door gebruikers (door scan op steekwoorden). |

De techniek is hier niet leidend, maar eerder ter ondersteuning. Het doel is vooral een subjectieve norm te ontwikkelen onder gebruikers, zodat in het gebruik van e-mail rekening wordt gehouden met de vertrouwelijkheid van het verstuurde. De techniek voorkomt dat toch vertrouwelijke informatie via e-mail naar buiten gaat en helpt in het verzamelen van informatie hierover.
Na een jaar vindt toetsing plaats van de interventieaanpak door de enquête te herhalen, worden de resultaten beoordeeld, en wordt besloten over een vervolg.

**Het gebruik van USB-sticks**

De zorg over het gebruik van USB-sticks richt zich op medewerkers die de USB-stick mee naar huis nemen om daar aan documenten te werken. Dit komt voor bij het management (concept documenten over de interne organisatie en bedrijfsresultaten), de verzekeringsmedewerkers (bijvoorbeeld het verslag van een schadeopname) en IT-medewerkers (systeembeschrijvingen, testresultaten, projectverslagen etc).

Het beveiligingsbeleid geeft in algemene termen richtlijnen over het gebruik van mobiele gegevensdragers. Dit is vertaald in het voorschrift dat USB-sticks niet toegestaan zijn voor zakelijk gebruik.
Onderzoek stelt vast dat het gebruik van USB-sticks veelvuldig voorkomt, in de vorm van privé aangeschafte USB-memorysticks of in de vorm van mp3-spelers of iPods. De USB-stick is zelfs opgenomen in de interne productencatalogus. Kenmerkend is dat deze USB-sticks niet beveiligd zijn met encryptie of biometrie. De USB-poorten op de werkplekken zijn niet afgeschermd voor het gebruik van extern geheugen op de USB-sticks. Op basis hiervan wordt het volgende gedragsdoel vastgesteld:

*Management, Verzekeringsmedewerkers en IT-medewerkers gebruiken geen USB-sticks voor zakelijke doeleinden.*

Met een enquête wordt het volgende over de intentievariabelen vastgesteld:

| Intentie variabele | Bevinding |
|---|---|
| Kennis | Doelgroepen weten dat USB-sticks die ze gebruiken onveilig zijn in geval van verlies of diefstal. Het is voor betrokkenen niet duidelijk wanneer informatie vertrouwelijk is. |
| Risico perceptie | Doelgroepen weten uit de krant dat het verlies van een USB-stick negatieve publiciteit heeft. Dit beïnvloedt hun gedrag voor enkele dagen, echter ze vervallen daarna weer terug naar het oude gedrag. Zij achten de kans dat zij zélf een USB-stick verliezen lager in dan de kans dat een collega deze verliest. |
| Attitude | Doelgroepen vinden dat beveiliging nodig maar hinderlijk is. Het verbieden van USB-sticks en controle op het gebruik ervan wordt als betuttelend ervaren. |
| Subjectieve norm | Doelgroepen spreken elkaar niet aan op het gebruik van onveilige USB-sticks, ook omdat het management gebruik maakt van de USB-sticks en ze in de inkoopcatalogus zijn opgenomen. De norm 'USB-sticks mogen niet' is niet zo zwart-wit. |

Geconstateerd mag worden dat USB-sticks niet zijn weg te denken in een innovatieve organisatie maar dat het gebruik ervan niet onder controle is. Verbieden past niet bij de cultuur en wordt teniet gedaan als blijkt dat ook leidinggevenden (en zelfs beveiligingsfunctionarissen) de USB-sticks gebruiken.

Zowel de attitude onder medewerkers als de subjectieve norm is anders dan het beleid en het gedragsdoel voorschrijft. Uit de analyse komt een ander beeld dan het geval in het gebruik van e-mail. Daar betrof het probleem vooral een gebrek aan voorlichting. In het geval van USB-sticks is sprake van een andere opvatting over veiligheid.

De interventieaanpak is daarom anders. De kern van de aanpak richt zich niet op de opvattingen onder het personeel, maar op het voorkomen dat medewerkers gebruik maken van onbeveiligde USB-sticks. Het wordt als zinloos ervaren het gebruik volledig te verbieden en af te schermen. Het initiële gedragsdoel wordt bijgesteld:

*Management, Verzekeringsmedewerkers en IT-medewerkers gebruiken alleen met biometrie beveiligde USB-sticks.*

Door de inzet van middelen kan toch een veilige situatie worden gecreëerd, met het gebruik van de volgende interventies:

| Bol | Interventies |
|---|---|
| Structuur | • Classificatiemodel dat aangeeft welke informatie vertrouwelijk is.<br>- Gebruik van mobiele gegevensdragers wordt opgenomen in de gedragscode, met daarin de sancties bij foutief gebruik. |
| Leiderschap | • USB-sticks worden uitgedeeld door senior medewerkers op de afdelingen. |
| Mensen | • Medewerkers worden getraind in het classificatiemodel. |
| Cultuur | • Elke medewerker krijgt een nieuwe beveiligde USB-sticks. De USB-stick wordt daarmee ook als een symbool van beveiliging ingezet, dat beveiliging leuk en innovatief kan zijn. |
| Techniek | • Gekozen wordt voor een met biometrie uitgeruste USB-stick. Er komt slechts één type in omloop. Deze wordt opgenomen in de productencatalogus.<br>• Werkplekken worden uitgerust met een security patch dat alleen dit type USB-sticks toestaat. |

Na een periode van een jaar wordt opnieuw het gedragsdoel gemeten en eventueel het interventieprogramma op de uitkomsten van deze meting aangepast.

**Conclusies**

In dit artikel is op basis van literatuuronderzoek vastgesteld via welke factoren (on)veilig gedrag van medewerkers binnen een organisatie te beïnvloeden is. Dit beïnvloedingsmodel is vervolgens uitgewerkt tot een model waarin op een doelgerichte, planmatige en gestructureerde wijze interventieprogramma's worden uitgevoerd gericht op vastgestelde gedragsdoelen, gevolgd door meting van resultaten en bijsturingacties. Daarmee wordt invulling gegeven aan een zekere mate van management control op risico's van (on)veilig gedrag in organisaties, zonder de illusie te willen wekken dat hiermee het risico van onveilig gedrag wordt gemitigeerd.

Het beschreven model wordt een zinvolle aanvulling geacht op de Code van Informatiebeveiliging, doordat de beheersingsmaatregelen ('controls') uit het domein 'Personeel' maar ook uit andere domeinen van de Code worden geplaatst tegen het licht van gedragsdoelstellingen en risico's. Daarnaast worden maatregelen uit de Code ondergebracht in een pakket van maatregelen die elkaar wederzijds versterken en daarmee aan effectiviteit winnen. In tegenstelling tot de Code strekt het analyseren en sturen van 'veilig gedrag' zich in dit model dus uit tot alle domeinen van de Code, dus ook de gedragscomponent binnen bijvoorbeeld wijzigingsbeheer, toegangsbeveiliging of beschikbaarheidbeheer. Daarmee wordt veilig gedrag van personeel minder een losstaand subsysteem (domein) maar meer een aspect van informatiebeveiliging dat in alle domeinen van belang is.

Voor de security officer is het model bruikbaar om beperkte financiële middelen effectief en efficiënt te benutten. Voor de IT-auditor is het model een zinvolle aanvulling op de Code voor Informatiebeveiliging, omdat niet de aanwezigheid van 'controls' maar de 'management control' van gedragsrisico's en de effectiviteit van maatregelen centraal kan worden gesteld in de beoordeling.

Naast deze voordelen zijn er echter ook kanttekeningen te plaatsen bij het beschreven model:

- het model is conceptueel afgeleid uit literatuuronderzoek en is nog slechts in beperkt toegepast in de praktijk. Het is daarom niet bedoeld als 'recept' voor veilig gedrag, maar wel als denk- en toetsingsmodel om de juiste vragen te stellen en de juiste acties te treffen;
- Gedragsveranderingen zijn niet te realiseren met enkelvoudige en eenmalige interventies: de kracht zit in de herhaling. Daar waar traditionele beveiligingsprogramma's afgerond worden als beveiligingsmaatregelen zijn ingericht, richt dit model zich op een het inrichten van een jaarlijkse cyclus van meten, plannen, handelen, bijstellen en weer meten. In perceptie kan dit leiden tot langer durende programma's. ■

**Literatuurlijst**

(Fishbein,1975) M. Fishbein & I. Aizen - Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research, Addison-Wesley, 1975
(Gerrichhauzen,1994) J. Gerrichhauzen, A. Kamperman en F. Kluytmans - Interventies bij Organisatieverandering, 1994

(Hofstede,1980) G. Hofstede - Culture's consequences, International differences in work-related values, 1980
(Maslow,1954) A.H. Maslow – Motivation and Personality, 1954
(Morgan,1997) G. Morgan - Images of Organisation, Sage, 1986/1997
(Peters,1982) Peters and Waterman - In search for excellence, 1982
(Schein,1992) E.H. Schein – Organizational Culture & Leadership, Jossey-Bass, 1992
(Simons,1992) S. Simons, Gedrag in organisaties, Prentice Hall, 1992
(Thierry, 1989) H. Thierry en A. Koopman-Iwema, Motivatie en satisfactie uit het handboek arbeids- en organisatie-psychologie, redactie P. Drenth, H. Thierry, P. Willems, Ch. De Wolff, 1989
(Vroom,1964) H. Vroom, Work and Motivation, Wiley, 1964
(Wouters,2002) E. Wouters - Alle zegen komt van boven, in Jaarboek Informatiebeveiliging 2001/2002;

**Eindnoot**

Dit artikel is gebaseerd op het afstudeer referaat van de heer Koers aan de EDP Audit opleiding van de Erasmus Universiteit te Rotterdam.
Aan de thematiek en oplossingsrichting is mee-ontwikkeld vanuit het adviesbureau Xion Consulting bv te Amstelveen, waar hij gedurende het schrijven van zijn referaat werkzaam was.

**Noot**

1 Het begrip en de meetbaarheid van een subjectieve groepsnorm is uit te leggen aan de hand van hoe onze maatschappij omgaat met roken. Vroeger was roken op de werkplek heel normaal, keek hier niemand van op. Tegenwoordig is de subjectieve groepsnorm dat dit niet kan, roken op de werkplek. Het gebeurt ook niet meer. De overheid is o.a. door wetgeving zeer actief geweest in het veranderen van deze norm, met succes.