



Nationaal Coördinator  
Terrorismebestrijding

## Bekwaam in beveiligingsbewustzijn

*Onderzoek naar de factoren die van belang zijn om personeel op de luchthavens security aware te maken en te houden.*

*Extract van het vertrouwelijke IBB-rapport*

*“Bekwaam in Beveiligingsbewustzijn” uit oktober 2008*

Inspectie Beveiliging Burgerluchtvaart

1e herdruk mei 2009



Nationaal Coördinator  
Terrorismebestrijding

## **Bekwaam in beveiligingsbewustzijn**

Onderzoek naar de factoren die van belang zijn om personeel  
luchthavens security aware te maken en te houden.

Extract van het vertrouwelijke IBB-rapport "Bekwaam in  
Beveiligingsbewustzijn" uit oktober 2008

Datum 1e herdruk mei 2009



## Inhoud

<b>Samenvatting</b>	5
<b>1. Inleiding</b>	8
1.1 Aanleiding	8
1.2 Doel en vraagstelling	8
1.3 Vertrouwelijke versie rapport "Bekwaam in beveiligingsbewustzijn"	9
1.4 Afbakening van het onderzoek	9
1.5 Werkwijze	10
1.6 Leeswijzer	10
<b>2. Security awareness nader bekeken</b>	11
2.1 Wat is security awareness?	11
2.2 Waarom security awareness?	13
2.3 Awareness programma's in de praktijk	14
2.4 Security awareness op luchthavens	15
2.5 Kritische succesfactoren voor security awareness op luchthavens	16
<b>3. Security awareness: wetenschappelijke inzichten</b>	20
3.1 Organisatorisch niveau	20
3.2 Individuele niveau	23
3.3 Een vijfde C : Controle	27
3.4 Conclusie	28
<b>4. Security awareness: de stand van zaken in Nederland</b>	30
4.1 Beleid en wet- en regelgeving over security awareness	30
4.2 Opleiden	30
4.3 Toezicht op de security awareness	30
4.4 Nationaal Trainingsprogramma	31
4.5 Conclusie	31
<b>5. Conclusies</b>	32
<b>Bijlage 1: Overzicht gebruikte bronnen</b>	35
<b>Bijlage 2: Overzicht geïnterviewde organisaties</b>	37
<b>Bijlage 3: Lijst met afkortingen</b>	38



## ***Samenvatting***

Voor u ligt een extract van het vertrouwelijke themarapport "Bekwaam in beveiligingsbewustzijn" zoals dat in oktober 2008 door de Inspectie Beveiliging Burgerluchtvaart (IBB) is uitgebracht. De versie die u nu in handen heeft is ontdaan van alle gegevens die het oorspronkelijke rapport vertrouwelijk maken. Hierdoor is het mogelijk om de bevindingen die de IBB heeft gedaan te delen met andere partijen. Het vertrouwelijke rapport is in oktober 2008 uitgebracht en doorgezonden aan de Directie Beveiliging Burgerluchtvaart (DBB), onderdeel van de Nationaal Coördinator Terrorismedebestrijding (NCTb). Direct belanghebbenden kunnen de vertrouwelijke versie van dit rapport bij de DBB opvragen.

### **Aanleiding en opzet**

Verdachte situaties in de omgeving van luchthavens worden eerder opgemerkt als medewerkers zich bewust zijn van de beveiligingseisen die de werkomgeving stelt. In dat daglicht bezien beschikt een luchthaven als Schiphol over 62.000 'beveiligers'. Een hoge mate van beveiligingsbewustzijn (security awareness) bij de luchthavenmedewerkers is daarom een belangrijk onderdeel van de beveiliging van een luchthaven. In dit onderzoek staat daarom de vraag "Welke factoren zijn van belang voor het effectief op peil brengen en houden van de security awareness van medewerkers?" centraal.

Aan de hand van acht kritische succesfactoren heeft de IBB onderzocht hoe volgens de laatste wetenschappelijke inzichten een effectief security awareness programma kan worden opgesteld. Wetenschappelijke artikelen over ervaringen in de informatie security awareness hebben gediend als basis voor dit onderzoek. Naast het gebruik van wetenschappelijke artikelen, is gesproken met partijen die ervaring hebben met het opstellen en uitvoeren van een security awareness programma. Delen van dit rapport zijn ter verificatie voorgelegd aan de experts van het Nationaal Lucht- en Ruimtevaartlaboratorium.

### **Kritische succesfactoren voor een effectieve security awareness**

Het model gaat uit van een aantal fasen in een continu doorlopend proces. Voordat een security awareness programma wordt ontwikkeld, moet eerst in kaart zijn gebracht aan welke risico's de organisatie wordt blootgesteld. Op basis van deze risico's wordt het gewenste niveau van security awareness vastgesteld. Het gaat hierbij om het gewenste kennisniveau, maar ook om de mate waarin een medewerker handelt naar deze kennis (gedrag). Op basis van het gewenste security awareness niveau kunnen op organisatorisch en individueel niveau maatregelen worden getroffen. Op organisatorisch niveau zijn vier kritische succesfactoren onderscheiden, de 4C's. Op het individueel niveau zijn ook vier kritische succesfactoren onderscheiden, de 4B's. Na toepassing van deze maatregelen wordt het niveau van security

awareness gemeten. Op deze wijze kan worden bepaald of het programma effectief is geweest. Vervolgens wordt opnieuw bezien welke risico's de organisatie bedreigen, welk niveau van security awareness daarbij hoort etc.

De volgende kritische succesfactoren zijn onderscheiden:

1. Commitment: de mate waarin het management continu en structureel achter het belang van security awareness staat en het goede voorbeeld geeft;
2. Cultuur: de mate waarin de werkomgeving geschikt en 'vertrouwd' is voor security awareness;
3. Communicatie: de mate en wijze van communicatie over security awareness;
4. Coöperatie: de mate waarin campagnes en trainingen in samenwerking met andere partijen worden opgezet, afgestemd en uitgevoerd;
5. Bewustzijn: de mate waarin medewerkers bewust zijn van de risico's en bekend zijn met de regels;
6. Betrokkenheid: de mate waarin medewerkers zich betrokken voelen bij de maatregelen en deze accepteren;
7. Belang: de mate waarin medewerkers inzicht hebben in het belang van beveiligingsmaatregelen;
8. Beloning: de mate waarin het belang van een medewerker om het gedrag te veranderen tastbaar wordt gemaakt.

Bovenstaande kritische succesfactoren zijn de knoppen die de luchthavenexploitant in samenwerking met andere betrokken partijen kan gebruiken om het niveau van security awareness te verbeteren. De IBB heeft per succesfactor onderzocht welke middelen ingezet kunnen worden om de security awareness bij medewerkers te verhogen.

### **Middelen voor een effectief security awareness programma**

De wetenschap draagt enkele middelen aan die gebruikt kunnen worden om de acht kritische succesfactoren voor een effectief security awareness programma te beïnvloeden. In dit rapport worden deze middelen per kritische succesfactor besproken. Voor de kritische succesfactor commitment gaat het om het opstellen van een beleidsvisie security awareness, het geven van het goede voorbeeld, het beschikbaar stellen van tijd voor trainingen en het vastleggen van security awareness in de bedrijfsvoering. Bij de kritische succesfactor cultuur gaat het om het stimuleren van security positief gedrag, het grenzen stellen aan ongewenst gedrag en het bespreekbaar maken van security awareness. Voor de factor communicatie geldt dat de boodschap op de doelgroep moet zijn afgestemd. Verder is belangrijk dat meerdere elkaar aanvullende communicatiemiddelen worden gebruikt. Het laatste middel voor de communicatie is de onmiddellijke terugkoppeling van testen, inspecties en audits. Bij de kritische factor coöperatie gaat het erom de betrokken partijen te betrekken bij het opstellen van het programma en het afstemmen van de boodschap op de diverse doelgroepen.

Op het individueel niveau zijn ook vier kritische succesfactoren benoemd. Voor de factor bewustzijn gaat het om heldere en

eenduidige definities in de campagnes en trainingen, ook hier geldt dat een op de doelgroep afgestemde boodschap beter is voor het bewustwordingsproces. Ook het gebruik van recente voorbeelden draagt daar een steentje aan bij. Voor de factor betrokkenheid is het van belang om werknemers een duidelijke rol te geven in het proces, uitleg te geven waarom security awareness zo belangrijk is en de medewerkers te stimuleren en motiveren. Een andere belangrijke factor is het belang. Dit kan worden beïnvloed door belangen te creëren voor medewerkers. Hier kan ook de groepsdynamiek worden gebruikt om dit te bereiken. De laatste factor is de beloning. Het niveau van security awareness is te beïnvloeden door gewenst gedrag te belonen en ongewenst gedrag te straffen.

## **1. Inleiding**

### **1.1 Aanleiding**

Mensen die op een luchthaven werken zijn de 'ogen en oren' van de luchthaven. Verdachte situaties worden eerder opgemerkt als medewerkers zich bewust zijn van de beveiligingseisen die de werkomgeving stelt. Dit maakt dat een luchthaven voor zijn beveiliging niet alleen afhankelijk is van het beveiligingspersoneel, maar ook kan profiteren van iedereen die op en om het luchthaventerrein werkt. In dat daglicht beschikt een luchthaven als Schiphol over circa 62.000 'beveiligers'. Het beveiligingsrisico, dat voortkomt uit het feit dat er duizenden mensen op Schiphol werken, wordt hierdoor omgebogen naar een voordeel voor de beveiliging van de luchthaven. Een hoge mate van beveiligingsbewustzijn (security awareness)<sup>1</sup> bij luchthavenmedewerkers is daarom een belangrijk onderdeel van de beveiliging van een luchthaven.

De security awareness is onder andere te meten door gebruik te maken van mysteryguests. Een mysteryguest begeeft zich fysiek binnen de beveiligde gebieden van de luchthaven zonder (zichtbare) luchthavenpas. De werknemers zijn security aware als de mysteryguest binnen deze gebieden zo spoedig mogelijk wordt aangesproken op zijn aanwezigheid. Over het algemeen blijkt het voor veel medewerkers een grote drempel om onbekenden aan te spreken op hun aanwezigheid, helemaal wanneer deze mensen een uniform of kostuum dragen. Op grote luchthavens als Schiphol speelt dit probleem extra sterk, omdat het nu eenmaal onmogelijk is om iedereen te kennen. Luchthavens staan voor de taak om werknemers security aware te maken en te houden. Dit rapport geeft antwoord hoe dit kan worden bereikt.

### **1.2 Doel en vraagstelling**

Het doel van dit themaonderzoek is te onderzoeken welke factoren van belang zijn om werknemers security aware te maken en te houden. Hiervoor zijn wetenschappelijke inzichten uit de informatie security awareness gebruikt om te bepalen hoe een security awareness programma effectief kan zijn. De resultaten van dit onderzoek kunnen worden gebruikt om te bepalen of de effectiviteit van zo'n programma op een luchthaven voldoende gewaarborgd is. De centrale vraag van het onderzoek luidt als volgt:

“Welke factoren zijn van belang voor het security aware maken en houden van de werknemers op een luchthaven?”

<sup>1</sup> In de wetgeving wordt de term security awareness, beveiligingsbewustzijn en luchtvaartbeveiliging door elkaar heen gebruikt. In dit rapport gebruikt de IBB voornamelijk de term security awareness.

Deze vraag wordt beantwoord aan de hand van de volgende deelvragen:

1. Wat wordt verstaan onder het begrip security awareness en wat zijn volgens wetenschappelijke bronnen effectieve maatregelen en kritische succesfactoren om medewerkers security aware te maken en te houden? (hoofdstuk 2, 3)
2. Wie zijn in Nederland betrokken bij het opstellen van eisen aan security awareness, het security aware maken van de werknemers, het op peil houden van kennis en gedrag en de controle hierop? (hoofdstuk 4)
3. Welke instrumenten kunnen volgens wetenschappelijke bronnen worden ingezet om het niveau van security awareness op peil brengen en houden?

### **1.3 Vertrouwelijke versie "Bekwaam in beveiligingsbewustzijn"**

Dit rapport is een extract van het vertrouwelijke themarapport "Bekwaam in beveiligingsbewustzijn", zoals dat in oktober 2008 door de Inspectie Beveiliging Burgerluchtvaart (IBB) is uitgebracht. Deze versie is ontdaan van alle gegevens die het oorspronkelijke rapport vertrouwelijk maakten en is gemaakt om (delen van) de bevindingen te kunnen delen met partnerorganisaties. Het originele rapport is door de IBB doorgezonden aan de Directie Beveiliging Burgerluchtvaart (DBB), onderdeel van de Nationaal Coördinator Terrorismedebestrijding. Voor direct belanghebbenden is de vertrouwelijke versie van het rapport op te vragen bij de DBB.

### **1.4 Afbakening van het onderzoek**

Het begrip 'security awareness' is een breed begrip. Het is toepasbaar op alle terreinen in de samenleving waar beveiliging een rol speelt. In dit onderzoek wordt uiteraard alleen gekeken naar security awareness op luchthavens. Het onderzoek is verder als volgt afgebakend:

- Het onderzoek is een themaonderzoek. Dit houdt in dat het onderzoek niet kijkt of partijen voldoen aan wet- en regelgeving. Er wordt alleen gekeken naar de kwaliteit van het security awareness programma in relatie tot de nieuwste wetenschappelijke inzichten;
- Het onderzoek richt zich op de luchthaven Schiphol. Door de omvang van de luchthaven zijn op Schiphol veel mensen onbekenden van elkaar. Dit is een complicerende factor ten aanzien van security awareness. Op regionale luchthavens is juist het feit dat mensen elkaar kennen weer een belemmering om elkaar aan te spreken bij het niet zichtbaar dragen van de luchthavenpas. Dit is het onderwerp van een vervolgonderzoek.
- Het onderzoek beperkt zich tot de luchthavenautoriteit die verantwoordelijk is voor de security awareness op de luchthaven en het personeel dat werkt op de luchthaven binnen de beveiligde gebieden. Het werken binnen deze gebieden vraagt om trainingen en een beveiligingsbewust gedrag. Het onderzoek richt zich niet op vliegend personeel.

### **1.5 Werkwijze**

Om dit onderzoek vorm te geven is gesproken met verschillende partijen die een security awareness programma hebben ontwikkeld en uitgevoerd. Er is gebruik gemaakt van wetenschappelijke inzichten in de informatie security awareness, omdat er op het gebied van luchtvaart nog geen security awareness onderzoek is uitgevoerd. Om een goed beeld te krijgen van de praktijk is gesproken met een aantal partijen op Schiphol. Daarbij is ook gebruik gemaakt van toezichtresultaten van de Koninklijke Marechaussee. Er is ook gesproken met onafhankelijke experts op het gebied van safety awareness, om gebruik te maken van deze kennis en inzichten. Het theoretisch kader van dit rapport is ter verificatie voorgelegd aan experts van het Nationaal Lucht- en Ruimtevaartlaboratorium. In bijlage 1 is een overzicht opgenomen van de bronnen die zijn gebruikt. In bijlage 2 is een overzicht opgenomen van de organisaties waarmee gesproken is. Het onderzoek is uitgevoerd conform het ISO9001:2000 gecertificeerde werkproces van de IBB.

### **1.6 Leeswijzer**

Dit rapport bestaat uit een aantal hoofdstukken die naar eigen inzicht afzonderlijk van elkaar te lezen zijn. Hier volgt een toelichting op de hoofdstukken. In hoofdstuk twee beantwoordt de IBB de vraag: "Wat wordt verstaan onder security awareness?" De beantwoording van deze vraag resulteert in een model dat de mate van security awareness verklaart aan de hand van een aantal kritische succesfactoren. In hoofdstuk drie licht de IBB de eerder gedefinieerde succesfactoren toe en werkt deze verder uit. Per succesfactor beschrijft de IBB middelen en instrumenten die volgens de wetenschap een bijdrage kunnen leveren aan een verhoogde mate van security awareness. In dit hoofdstuk is daarmee de vraag beantwoord: "Welke middelen kunnen ingezet worden om de mate van security awareness te verhogen?". In hoofdstuk vier beschrijft de IBB wie verantwoordelijk is voor het op peil brengen en houden van de security awareness op luchthavens in Nederland. De vraag die in hoofdstuk vier centraal staat is: "Wie is verantwoordelijk voor het op peil brengen en houden van de security awareness?". Het rapport eindigt met conclusies en aanbevelingen in hoofdstuk 5.

## **2. Security awareness nader bekeken**

In dit hoofdstuk wordt dieper ingegaan op het begrip 'security awareness'. Er zal een nadere toelichting gegeven worden op de achtergronden van het begrip en uiteraard zal ook een definitie, zoals die in dit onderzoek gehanteerd wordt, niet ontbreken. Na een zoektocht naar beschikbare literatuur over security awareness op luchthavens bleek dat er nog geen onderzoek gedaan is naar het onderwerp in deze context. Tijdens de zoektocht werd de term security awareness vooral in verband gebracht met 'informatie security awareness', waarbij het gaat om de beveiliging van kennis en hardware, zoals computers en informatiedragers. Ook de wereld van de 'informatie security awareness' is pas sinds kort in ontwikkeling: sinds 2002 zijn er meerdere artikelen en boeken over het onderwerp verschenen. Echter security awareness is nog een onontgonnen terrein. Awareness wordt als een belangrijk onderwerp beschouwd, maar staat nog wel in de kinderschoenen. Om meer grip te krijgen op de informatie uit de literatuur heeft de IBB interviews gehouden met personen die zich bezig houden met (informatie) security awareness projecten (zie bijlage 2). Op basis van deze gesprekken en de wetenschappelijke artikelen heeft de IBB een model ontwikkeld voor het maken van een effectief security awareness programma. Dit model is ter verificatie voorgelegd aan het Nationaal Lucht- en Ruimtevaartlaboratorium (NLR). De IBB dankt het NLR voor de geleverde bijdrage aan het verder verfijnen van dit model. Het beveiligen van luchthavens en de kennis over deze getroffen beveiligingsmaatregelen vertoont overeenkomsten met de bescherming van kennis van bedrijven en computergerelateerde zaken. Daarom heeft de IBB ervoor gekozen om de kennis die is opgedaan in de informatie security awareness als inspiratiebron te gebruiken voor dit onderzoek. Voor het beantwoorden van de vragen in dit onderzoek is gekozen voor het Information Security Forum Framework.

### **2.1 Wat is security awareness?**

Iedereen kan dezelfde definitie van security awareness gebruiken: dat wil zeggen het belang van beveiliging onderschrijven. Echter de mate waarin dit bewustzijn aanwezig is en de mate waarin deze kennis ook werkelijk wordt toegepast en de strengheid van de security maatregelen op zich kunnen verschillen per persoon en per bedrijfstak. Zo zal een beveiligiger in een supermarkt andere gedachten hebben bij security awareness dan een beveiligiger van een kerncentrale. Doordat security awareness een relatief nieuw vakgebied is, zijn er verschillen in uitvoering en interpretatiemogelijkheden van wat nou precies een noodzakelijk niveau van security awareness is. Security awareness is onderhevig aan menselijke interpretaties. Beïnvloeding van deze interpretaties is erg moeilijk en vereist een redelijke kennis van de menselijke psyche. Het is moeilijk te bepalen welke factoren een rol spelen bij het security aware maken en houden van mensen. Enige nadere toelichting op het begrip is daarom niet overbodig. In de literatuur wordt security awareness op een eenduidige manier omschreven.

Vrijwel alle studies die voor dit onderzoek gebruikt zijn, gaan uit van de volgende definitie:

Security awareness is de mate waarin elke medewerker op elk niveau in de organisatie:

- het belang van beveiliging begrijpt
- het niveau van beveiliging dat voor de organisatie noodzakelijk is begrijpt
- zijn eigen individuele beveiligingsverantwoordelijkheden begrijpt
- en daar ook naar handelt<sup>2</sup>.

De definitie maakt duidelijk dat security awareness in verschillende soorten organisaties en in allerlei facetten van een organisatie een rol kan spelen. Het laatste deel van de definitie is cruciaal. Mensen dienen actief te handelen naar de beveiligingsrisico's in een organisatie. De vraag is echter hoe een organisatie zijn medewerkers zover kan krijgen.

Om werknemers security aware te maken moeten ze worden getraind. In de literatuur (Hofland, 2005, p. 33) worden twee manieren beschreven: de ad hoc methode en het Information Security Forum Framework (kortweg ISF Framework). De ad hoc methode wordt gekenmerkt door het impulsieve en reactieve karakter: slechts bij een incident wordt actie ondernomen en wordt aan de hand van het incident een verduidelijking gegeven van de do's en don'ts met betrekking tot de beveiliging. Het ISF Framework is een continu proces. Het framework is opgebouwd uit een aantal stappen. Het is een methode waarbij gebruik wordt gemaakt van een terugkerend programma, waarbij security awareness op meerdere manieren wordt herhaald. De kracht van deze methode zit in de herhaling. Het ISF framework is een zogenaamde 'tweede generatiemethodiek', dat in de wetenschap gezien wordt als de methode om een organisatie security aware te maken. In tweede generatie methodieken spelen 'continuïteit' en 'het management' een cruciale rol (Neys, 2003).

Globaal schrijft het IFS framework vier stappen voor om een organisatie security aware te maken. De eerste stap is het bepalen van het doel van het security awareness programma. Vervolgens dient men als tweede stap de scope en het ontwerp van het programma vast te stellen. Ten derde moeten er security awareness campagnes en trainingen ontwikkeld en geïmplementeerd worden. En tot slot dient de effectiviteit van deze maatregelen geëvalueerd te worden. De laatste stap is weer bepalend voor de inhoud van de eerste stap. Het proces is weergegeven in figuur 1.

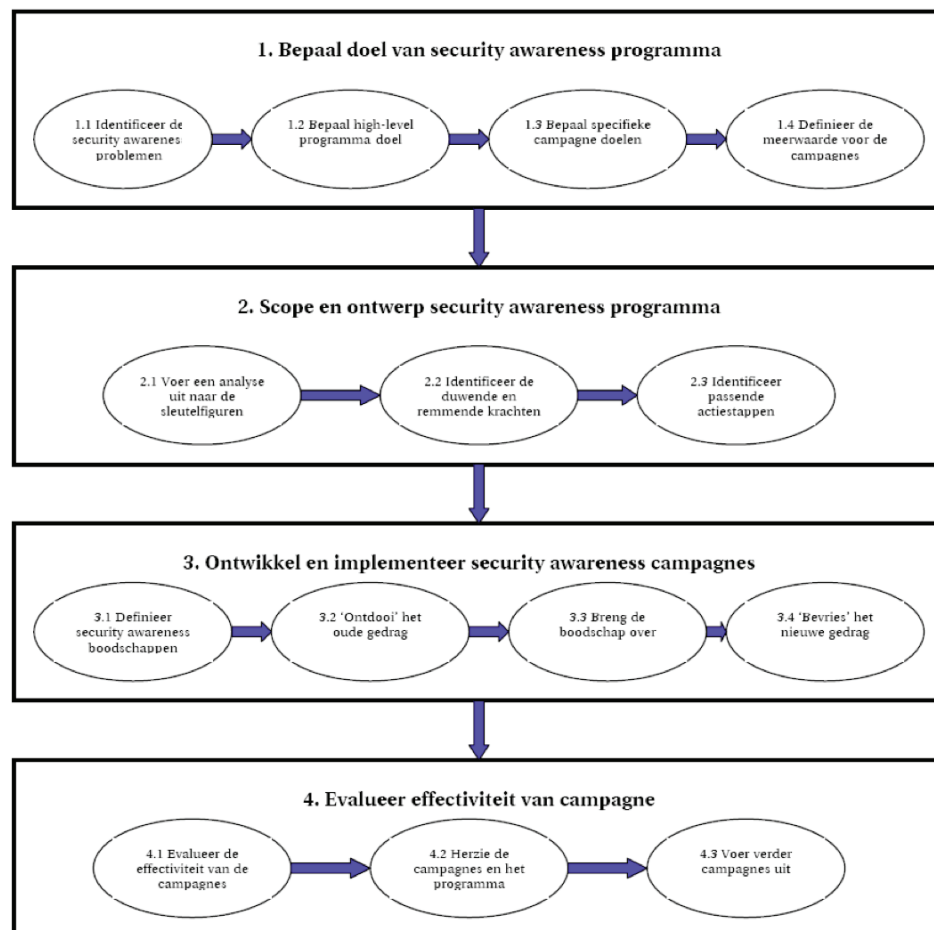
Het Information Security Forum<sup>3</sup> beschrijft een aantal voorwaarden waaraan een effectief security awareness programma moet voldoen.

<sup>2</sup> C. Neys, IT'ers, regels en security awareness, april 2003

V. Hofland, Bewust van informatiebeveiliging, januari 2005

Information Security Forum, Effective security awareness, workshop report, april 2002

Dit programma bestaat idealiter uit verschillende bewustwordingscampagnes die op hun beurt weer bestaan uit activiteiten die gericht zijn op een specifieke doelgroep of securityprobleem. Het programma dient daarbij een doorgaand proces te zijn dat gericht is op het opbouwen van een zogenaamde 'security-positieve' omgeving. In zo'n omgeving zien mensen het nut van beveiliging in en zijn bereid zich daarvoor in te zetten. Twee essentiële zaken vallen op in deze omschrijving van een security awareness programma, te weten: security awareness is een continu proces en security awareness is maatwerk. Zonder deze twee voorwaarden kan een security awareness programma niet effectief zijn.



Figuur 1: ISF Framework (ontleend aan Hofland 2005)

## 2.2 Waarom security awareness?

Een organisatie kan verschillende redenen hebben om met security awareness aan de slag te gaan. Soms wordt een organisatie door externe factoren gedwongen om een security awareness programma te starten. Te denken valt aan wet- en regelgeving. Een organisatie kan echter ook vanuit eigen motivatie security awareness als een speerpunt binnen de organisatie benoemen. Bijvoorbeeld omdat

<sup>3</sup> Information Security Forum, Effective security awareness, workshop report, april 2002

men vaak slachtoffer is geweest van diefstal. De literatuur (NEN 27002/2007) noemt drie hoofdbronnen aan de hand waarvan een organisatie haar beveiligingsbehoefte bepaald:

- 1) De eerste bron komt voort uit de beoordeling van de risico's voor de organisatie. Via risicobeoordeling worden de kwetsbaarheid voor en waarschijnlijkheid van het optreden van bedreigingen beoordeeld en worden de mogelijke effecten ervan ingeschat.
- 2) De tweede bron wordt gevormd door eisen uit wet- en regelgeving en contractuele eisen waaraan de organisatie en dienstverlenende bedrijven moeten voldoen.
- 3) De derde bron wordt gevormd door het eigen stelsel van uitgangspunten, doelstellingen en bedrijfseisen dat een organisatie heeft ontwikkeld ter ondersteuning van haar bedrijfsvoering.

Het 'waarom' voor het invoeren van security awareness programma's door organisaties kan zeer bepalend zijn voor de mate waarin security awareness tussen de oren van werknemers zit. Wanneer een organisatie bijvoorbeeld door externe factoren gedwongen wordt om met security awareness aan de slag te gaan, kan het personeel minder gemotiveerd zijn, dan wanneer men er zelf het nut van in ziet. Binnen de burgerluchtvaart kunnen alle drie genoemde bronnen bepalend zijn voor de beveiligingsbehoefte. Het reputatiemechanisme is erg belangrijk voor luchtvaartorganisaties<sup>4</sup>. Dit zou kunnen betekenen dat Nederlandse luchthavens klanten verliezen als ze niet veilig zijn of zouden lijken. Voor de burgerluchtvaart is een risicoanalyse gemaakt door de Directie Beveiliging Burgerluchtvaart (hierna DBB). Op basis van deze analyse is een aantal beveiligingsmaatregelen getroffen. Het creëren van security awareness hoort daar ook bij. Daarnaast is in wet- en regelgeving opgenomen dat de luchthavenautoriteiten zorg moeten dragen voor voldoende mate van security awareness. Ten slotte hebben luchthavens er in het kader van de bedrijfscontinuïteit belang bij dat hun processen niet verstoord worden door security incidenten.

### **2.3 Awareness programma's in de praktijk**

Zoals eerder opgemerkt zijn awareness programma's niet uniek voor de luchtvaartindustrie. Ook in andere bedrijfstakken speelt 'awareness' een belangrijke rol. Zo is in vele organisaties 'safety awareness' een belangrijk aandachtspunt en is in de IT-wereld de zogenaamde 'informatie security awareness' een hot item. Dergelijke programma's hebben als overeenkomst dat ze medewerkers bewust proberen te maken. Kenmerkend daarbij is dat de meeste awareness programma's medewerkers bewust proberen te maken van iets dat schijnbaar niet op een natuurlijke manier onder hun primaire werkzaamheden valt. Zo hebben safety awareness programma's tot doel om medewerkers bewust te maken van de veiligheidsrisico's die aan hun werk kleven. Informatie security awareness programma's hebben tot doel

<sup>4</sup> Prof dr. F. L. Leeuw (universiteit Maastricht/WODC), *Trends in toezichtland en toezicht op ondernemingen gedragswetenschappelijk beschouwd*, Discussiemiddag Toezicht en compliance, WODC, 26 september 2008

medewerkers bewust te maken van het feit dat men informatie dient te beschermen tegen onbevoegden. Dit heeft echter slechts betrekking op de randvoorwaarden van hun werk.

Het ligt voor de hand om de reeds opgedane ervaringen bij andere awareness programma's te gebruiken voor het inrichten van security awareness programma's op luchthavens en andersom. Dergelijke onderzoeken bieden vele raakvlakken voor onderzoek naar security awareness programma's binnen de beveiliging van de burgerluchtvaart. Echter, er is een belangrijk verschil tussen security awareness op luchthavens en de eerder genoemde safety awareness en informatie security awareness. En dat is het belang dat de werknemers er zelf bij hebben. Een vliegtuigmonteur ondervindt namelijk zelf last van een onveilige omgeving. Ook een accountant heeft er belang bij om back-ups te maken van zijn documenten. Voor een bagageafhandelaar heeft het betreden van de bagageruimte door onbevoegden echter geen gevolgen voor zijn eigen werkzaamheden. Het grote verschil is dat een monteur door jarenlange safety trainingen geleerd heeft wat de gevolgen van onveilig gedrag zijn. Hij ziet hier het belang van in. Bagageafhandelaars hebben nog geen jarenlange security training gehad. Extra punt is dat de frequentie van safety incidenten hoger is dan security incidenten, waardoor de werknemers minder de urgentie van security actie zullen voelen of zien. Hierdoor zijn er minder prikkels om hierop alert te zijn. Dit maakt het extra lastig om mensen te motiveren voldoende aandacht te hebben voor security awareness.

#### **2.4 Security awareness op luchthavens**

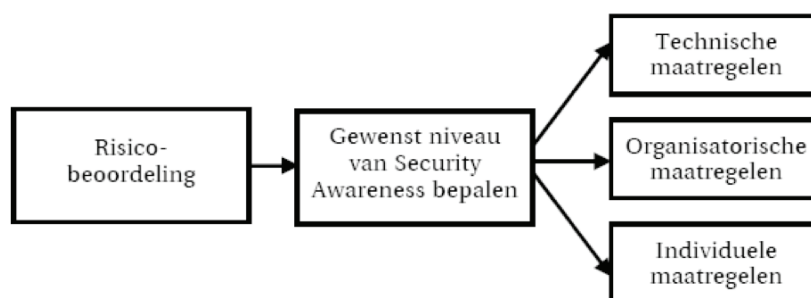
Binnen de beveiliging van de burgerluchtvaart speelt security awareness een belangrijke rol in het beveiligingsconcept dat bestaat uit verschillende beveiligingsringen. Het idee is dat indien kwaadwillenden erin slagen om door de eerste fysieke beveiligingsringen heen te dringen, men alsnog opgemerkt wordt door oplettende luchthavenmedewerkers. Door gebruik te maken van alle aanwezige medewerkers op de luchthaven heeft Schiphol (in theorie) hierdoor de beschikking over circa 62.000 in plaats van 4.000 'beveiligers'. Security awareness is summier opgenomen in wet- en regelgeving, maar niet nader uitgewerkt. Volgens de regelgeving zijn luchthavenautoriteiten, schoonmaakbedrijven, cateraars en luchtvaartmaatschappijen verantwoordelijk voor het 'voldoende security aware houden van de mensen die toegang hebben tot beveiligde gebieden'. Echter, er is geen norm die aangeeft wanneer een medewerker over 'voldoende security awareness' beschikt. Ook zijn er geen randvoorwaarden voor een effectief security awareness programma of aanknopingspunten voor een effectieve security awareness training. Voor luchthavens en andere bedrijven op de luchthaven is het zodoende onduidelijk wanneer luchthavenmedewerkers voldoende security aware zijn en of zij aan de wettelijke eisen voldoen. De luchthaven is verantwoordelijk voor de security awarenesopleidingen van alle medewerkers op het luchthavengebied, ook degene die niet bij de luchthaven zelf in dienst zijn. Daarmee is zij ook indirect verantwoordelijk voor de security awareness programma's van

andere bedrijven op de luchthaven. Dit maakt het extra moeilijk om grip te houden op het niveau van security awareness.

Onder de huidige omstandigheden kunnen luchthavens de security awareness van de medewerkers controleren door achteraf proberen te meten of het niveau orde is. Het niveau is ten eerste af te meten aan de mate waarin onbevoegde medewerkers aangesproken worden op de reden van hun aanwezigheid op een bepaalde plaats. Daarnaast is het succes van security awareness programma's te meten aan het aantal incidenten dat gemeld wordt. Naarmate mensen meer security aware zijn, zal men vaker risicovolle situaties melden, waardoor het aantal geregistreerde incidenten zal stijgen. Als laatste, maar daarom niet minder belangrijk, dient het management de security doelstellingen van het bedrijf volledig te onderschrijven. Dit moet duidelijk zijn in aanwezigheid van procedures, checklists, security management plannen, aanwezigheid van reporting systems, maar dient tevens gesteund te worden door verklaringen van werknemers op de werkvloer die overtuigd moeten zijn van de steun van hun management. Dit zou door geselecteerde interviews en inspecties gecontroleerd kunnen worden.

## 2.5 Kritische succesfactoren voor security awareness op luchthavens

Nu er meer duidelijkheid is over het begrip security awareness is het tijd om nader in te gaan op de vraag hoe een luchthaven ervoor kan zorgen dat de luchthavenmedewerkers security aware worden en blijven. Ofwel: aan welke knoppen kan een luchthaven draaien om ervoor te zorgen dat de medewerkers security aware zijn? Over security awareness zijn verschillende wetenschappelijke stukken verschenen. Deze artikelen zijn door de IBB gebruikt om een model samen te stellen met kritische succesfactoren voor security awareness. Zoals gezegd zijn er veel onderzoeken gedaan, die gericht zijn op informatie security awareness. Een eerste aanknopingspunt voor een model voor het creëren van een effectief security awareness programma is dan ook gevonden binnen de informatietechnologie. Neys<sup>5</sup> heeft een model ontwikkeld waarin zij aangeeft welke stappen een organisatie dient te nemen om tot een effectief security awareness programma te komen. Dit model is gebaseerd op de stappen in het eerder besproken ISF-model en ziet er als volgt uit (gedeeltelijke weergave):



Figuur 2: Totstandkoming security awareness programma (Neys, 2004)

<sup>5</sup> C. Neys & T. van der Schaaf, *Grip op 'de factor mens'*, Informatiebeveiliging, december 2004

Het model laat zien dat een organisatie, voordat een security awareness programma ontwikkeld wordt, in kaart moet brengen aan welke risico's de organisatie bloot is gesteld en welk niveau van security awareness gewenst is. Neys stelt vervolgens maatregelen voor op drie niveaus voor het creëren van security awareness in een organisatie. Ten eerste zijn dat maatregelen op technisch niveau. Deze maatregelen zijn vrij specifiek voor IT-organisaties, zoals het verplicht wijzigen van wachtwoorden en automatisch activeren van screensavers om informatie af te schermen. Op luchthavens spelen technische maatregelen een minder grote rol bij het creëren van security awareness dan bij informatietechnologie. De andere twee niveaus zijn echter wel van belang voor security awareness op luchthavens. Te weten: het organisatieniveau en het individuele niveau. Neys stelt dat enerzijds organisatorische maatregelen genomen moeten worden voor het waarborgen van een effectief niveau van security awareness. Anderzijds moeten maatregelen genomen worden, die de individuen in de organisatie ertoe bewegen om security awareness serieus te nemen.

Het model van Neys gaat helaas niet in op de uitvoering van security awareness maatregelen op de verschillende niveaus. Maar waar het model van Neys ophoudt, zijn aanknopingspunten te vinden in de theorie van Hofland (Hofland 2005). Hofland geeft namelijk aan hoe de organisatorische dimensie en de individuele dimensie te beïnvloeden zijn. De organisatorische dimensie richt zich op maatregelen die zich op het niveau van het management en de organisatiecultuur afspelen. In de literatuur (Hofland, 2005 p. 68) wordt het zogenaamde '4C-model' aangehaald voor het beschrijven van de kritische succesfactoren waarmee organisaties voorwaarden kunnen scheppen voor een effectief security awareness programma. De vier C's staan achtereenvolgens voor:

- **Commitment:** Het management moet continu en structureel achter het belang van security awareness staan en moet het goede voorbeeld geven. Men dient tijd, geld en capaciteit vrij te maken. Het management heeft een sleutelrol en bepaalt de randvoorwaarden van de security awareness.
- **Cultuur:** Medewerkers moeten in vertrouwen verdachte situaties kunnen melden. Een verdachte situatie kan namelijk ook betrekking hebben op een directe collega. Daarnaast moet security awareness en de eventuele meldingen die daaruit voortvloeien serieus genomen worden.
- **Communicatie:** Er moet regelmatig communicatie plaatsvinden over het belang van security awareness om het zodoende tussen de oren van de medewerkers te krijgen en te houden.
- **Coöperatie:** In de Informatie security awareness wordt te vaak gedacht dat het alleen een probleem is van de IT-afdeling, dit is echter niet waar. Managers van verschillende afdelingen en onderliggende instellingen moeten samenwerken en de taken verdelen. Hiervoor is een goede samenwerking en afstemming tussen de verschillende onderdelen nodig.

De vier C's kunnen gezien worden als de kritische succesfactoren voor het slagen van een security awareness programma op organisatieniveau.

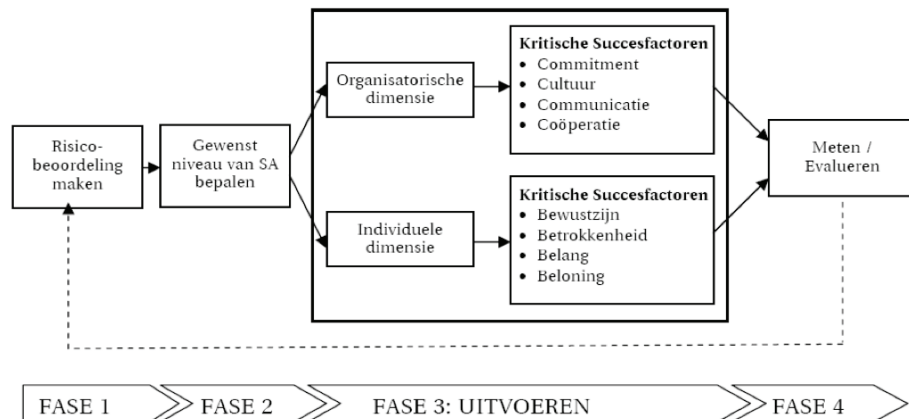
Hofland noemt ook vier factoren die van belang zijn voor de individuele dimensie van security awareness. De individuele dimensie richt zich op de maatregelen die zich op het niveau van het individu in een organisatie afspelen. Vragen als: "waarom besluit een medewerker al dan niet melding te maken van een onveilige situatie?" of "wat motiveert een medewerker om security aware te zijn?" komen hierbij aan de orde. De Tafel van Elf is een aanknopingspunt voor antwoorden op deze vragen over individuen. De Tafel van Elf is een instrument dat is ontwikkeld in samenwerking met het Ministerie van Justitie en dient als hulpmiddel om de naleving van regels door organisaties en individuen vast te stellen, te verklaren en te verbeteren. Deze verklaringen kunnen ook worden toegepast op het naleven van regels die voortvloeien uit security awareness programma's. De elf factoren uit de Tafel van Elf komen overeen met de vier belangrijke aspecten die Hofland (2005, p. 33)<sup>6</sup> beschrijft die bij gedragsbeïnvloeding van personen een rol spelen, de vier B's. Deze vier B's staan voor:

- Bewustzijn: het bewustzijn van personen dat er verschillende risico's zijn. In de Tafel van Elf gaat het om de factor Kennis: de personen moeten ten eerste bekend zijn met de regels en ten tweede moeten de regels duidelijk zijn;
- Betrokkenheid: de mate waarin personen zich betrokken voelen met de maatregelen. In de Tafel van Elf gaat het om de factor Mate van acceptatie, de mate waarin de regels en de uitwerking in beleid door de personen acceptabel worden gevonden. Daarnaast speelt ook de factor Normgetrouwheid een rol. Deze factor wordt gevormd door de eigen normen en waarden en gewoonten. De factor Maatschappelijke controle is hier ook van belang: het gaat om de mate waarin de omgeving gedrag goed- of afkeurt, verantwoordelijkheid neemt en actie onderneemt.
- Belang: personen zijn eerder geneigd hun gedrag aan te passen als het in hun belang is. De Tafel van Elf spreekt over de factor Kosten en baten: het naleven van regels kan worden uitgedrukt in tijd, geld en moeite. Het naleven van regels mag niets kosten, anders passen personen hun gedrag niet aan.
- Beloning: met een beloning of straf wordt het belang van een persoon om het gedrag te veranderen tastbaar gemaakt. De Tafel van Elf beschrijft een aantal factoren dat van belang is voor de straf: de Meldingskans, de Controlekans, de Detectiekans, de Selectiviteit, de Sanctiekans en de Sanctie-ernst. Het gaat daarbij om de (verhoogde gepercipieerde) kans om betrapt te worden bij het niet naleven van de regels en de daarbijbehorende straf.

<sup>6</sup> zie ook A. Koot, J. de Haas, *Organisaties overschatten niveau van awareness*, Informatiebeveiliging, juli 2005, p.30-33

Tot slot geeft Hofland aan dat het meten van de mate van security awareness onmisbaar is voor een effectief programma. Door te meten en te evalueren wordt duidelijk of het niveau van security awareness op peil is. Desgewenst kan het programma aangepast worden. Dit maakt dat het security awareness programma een continu proces is en voortdurend de nodige aandacht krijgt.

De zojuist besproken inzichten over security awareness leveren het volgende model op dat als basis zal dienen voor dit onderzoek:



Figuur 3: Kritische succesfactoren voor security awareness op luchthavens

De stappen in het model komen overeen met de stappen die gezet worden in het eerder gepresenteerde ISF-model. Met dien verstande dat het model is aangevuld met de kritische succesfactoren die van belang zijn voor security awareness op een luchthaven en waar een organisatie op moet letten bij het inrichten van een security awareness programma.

### **3. Security awareness: wetenschappelijke inzichten**

In hoofdstuk twee is een achttal kritische succesfactoren besproken die nodig zijn voor het security aware maken en houden van personeel. De kritische succesfactoren hebben enerzijds betrekking op de organisatie als geheel (4 C's) en anderzijds op de individuen die in organisaties werken (4 B's). In dit hoofdstuk worden de middelen besproken die door de wetenschap worden aangedragen om de acht genoemde succesfactoren te beïnvloeden.

#### **3.1 Organisatorisch niveau**

##### *3.1.1 Kritische succesfactor: Commitment*

Uit onderzoek (ISF 2002) blijkt dat het topmanagement achter het belang van security awareness moet staan. Het topmanagement is de basis voor de noodzakelijke cultuurverandering. Zij moeten het belang van security awareness activiteiten inzien en deze boodschap duidelijk naar het middenmanagement en de werknemers communiceren, zodat de commitment uiteindelijk binnen alle lagen van de organisatie aanwezig is. Het topmanagement kan haar commitment tonen door haar visie ten aanzien van security awareness vast te leggen in het beleid en op te nemen in de bedrijfsvoering. Verder kan het management commitment tonen door geld vrij te maken voor trainingen en tijd vrij te maken voor het personeel om deze training te volgen. Het management vervult een voorbeeldfunctie en moet zelf het goede voorbeeld geven. Zij zijn er voor verantwoordelijk dat alle werknemers zich betrokken voelen bij het probleem van security awareness. Zolang niet iedereen binnen de organisatie doordrongen is van het feit dat security awareness een taak is van iedereen, zal de beveiliging niet gewaarborgd zijn<sup>7</sup>.

Verder blijkt uit onderzoek (ISF 2002) dat security awareness programma's meer succes hebben als er een speciaal team wordt vrijgemaakt om deze programma's in de gehele organisatie in te voeren, regelmatig metingen uit te voeren en het programma aan de hand van de metingen aan te passen. Het is daarbij wel belangrijk dat het team voor dit project eigen doelstellingen opneemt, om te voorkomen dat de betrokkenheid van de teamleden vermindert als andere activiteiten tijdelijk meer aandacht vragen. Ook in de interviews die de IBB gehouden heeft in het kader van dit onderzoek is het belang van management commitment door de respondenten meermaals onderstreept. Eén van de respondenten geeft aan: " Zonder commitment is het trekken aan een dood paard." Kortom: voor het security aware maken en houden van het personeel is het noodzakelijk dat het management het security awareness programma steunt, hiervan het nut inziet en tijd en financiële

<sup>7</sup> S. Hinderink & S. Hendrikx, Informatiebeveiliging en awareness, onlosmakelijk verbonden, Informatiebeveiliging juni 2007  
Information Security Forum, Effective security awareness, workshop report, april 2002

middelen vrijmaakt voor het ontwerpen van dit programma en het laten volgen van dit programma door het personeel.

### *3.1.2 Kritische succesfactor: Cultuur*

De traditionele benadering van het ontwikkelen van bewustzijn is meestal geconcentreerd op het beïnvloeden van de individuele risicobeleving. De aanname daarbij is dat een persoon als hij het risico bij fout gedrag begrijpt zijn gedrag overeenkomstig aan zal passen. Volgens het ISF-model is deze traditionele aanname echter niet juist. (ISF 2002, p. 20). Het ISF-model stelt dat het doel van een security awareness programma een gedragsverandering zou moeten zijn in plaats van kennisoverdracht over security awareness. Het blijkt namelijk dat mensen erg slecht zijn in het inschatten van risico's. Mensen beoordelen risico's meestal op gebeurtenissen uit het verleden.

Ook blijkt uit sociaal-psychologisch onderzoek dat de organisatiecultuur een belangrijke invloed heeft op iemands gedrag. Dit onderzoek toont aan dat mensen zichzelf stelselmatig veel meer macht over een situatie toeschrijven dan ze werkelijk hebben en dat mensen tegelijkertijd onvoldoende erkennen welke invloed de (sociale) omgeving op hen uitoefent. Deze ingebakken inschattingfout maakt het extra moeilijk om inzicht te krijgen in motieven waarom iemand niet volgens de regels<sup>8</sup> handelt.

Volgens het ISF moet een security awareness programma daarom gericht zijn op het maken en behouden van een organisatiecultuur die security positief gedrag stimuleert en ondersteunt (p.21). De collectieve cultuur van een organisatie bestaat uit het totaal van alle gedeelde en algemeen geaccepteerde normen en waarden die het personeel zich door de tijd heen eigen heeft gemaakt. Deze cultuur beïnvloedt het individuele en het groepsgedrag, en kan daarom ook worden gebruikt om het beveiligingsgedrag van het personeel te veranderen en aan scherpen<sup>9</sup>. Goed getrainde en toegewijde werknemers zijn immers de sterkste schakel in de beveiliging van een luchthaven. Daarom is het belangrijk dat beveiligingsbewustzijn een gewoonte wordt in de collectieve cultuur van de organisatie. De vraag is hoe dit wordt bereikt.

Om de cultuur te veranderen moeten de normen, waarden en het gedrag van de werknemers worden veranderd. Uit onderzoek blijkt dat een cultuurverandering kan leiden tot veel onrust en verzet bij de werknemers, omdat mensen nou eenmaal gehecht zijn aan hun oude (slechte) gewoonten. Een cultuurverandering is mogelijk door het volgen van een veranderingsproces, zoals bijvoorbeeld de krachtenveldanalyse van K. Lewin.

Het topmanagement heeft een sleutelrol in het bepalen van de cultuur. Dit geldt ook voor security awareness. Als het management

<sup>8</sup> Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Directie Arbeidszaken Openbare Sector, *Leidraad motieven voor niet-integer handelen. Sociaal-psychologische factoren*, November 2007

<sup>9</sup> K. Thomson, R. von Solms & L. Louw, Centre for Information Security Studies, Nelson Mandela Metropolitan University, South Africa, *Cultivating an organizational information security culture*, Computer Fraud & Security, October 2006.

laat zien dat zij positief gedrag waardeert en beloont, is het personeel sneller geneigd dit gedrag over te nemen. Ook het meer of minder expliciete gedrag van leidinggevendenden is een belangrijke factor in het bepalen van het gedrag van medewerkers (MinBZK, november 2007, p. 12). Het topmanagement heeft tot taak beleid op te stellen en aan te geven welke richting zij uit willen met de beveiliging/security awareness. Een belangrijk onderdeel van dit beleid is het beïnvloeden van het gedrag van de werknemers, door duidelijk aan te geven welk gedrag wel en niet wordt geaccepteerd.<sup>10</sup> Een andere belangrijke voorwaarde is dat de security awareness bespreekbaar wordt gemaakt in een organisatie. Een individu moet zich veilig voelen om een incident te melden, zonder angst voor sancties. Er moet een 'no blame' cultuur ontstaan, waarbij alleen gestraft wordt als opzettelijk handelen leidt tot inbreuken. Het topmanagement moet vervolgens dit beleid steunen en commitment tonen (zie vorige succesfactor). Door dit beleid breed binnen de organisatie uit te dragen, geeft het topmanagement de aanzet om het personeel security aware te maken.

### 3.1.3 Kritische succesfactor: Communicatie

Communicatie wordt ook wel het smeermiddel genoemd tussen de drie andere C's commitment, cultuur en coöperatie. Het zorgt voor de verandering in deze drie succesfactoren. Voor het ontwikkelen van een effectief security awareness programma moet allereerst door het management een helder doel worden gesteld: namelijk het gewenste niveau van security awareness dat de organisatie en de onderliggende instanties moeten behalen. Het gaat hier naast het gewenste kennisniveau om de gewenste gedragsverandering. Het vaststellen van dit niveau is echter niet zo gemakkelijk als niet duidelijk is wat men wil bereiken. Het ISF beschrijft een hulpmiddel: het kijken naar de huidige bekende security awareness problemen. Op basis van deze bekende problemen kan de noodzaak voor het security awareness programma worden bepaald. De specifieke doelen en hoe deze kunnen worden bereikt kunnen dan ook worden bepaald. Het vastleggen van de noodzaak voor het security awareness programma en de specifieke doelen is ook belangrijk omdat aan de hand van een duidelijk gespecificeerd doel kan worden bepaald of het programma succes heeft gehad.

Het security awareness programma dient daarbij te worden aangepast aan de diverse doelgroepen. Het is belangrijk dat de trainingen en campagnes op de doelgroep zijn afgestemd, omdat de cursisten de training anders als irrelevant ervaren. Dit geldt ook wanneer voorbeelden gebruikt worden die niet correct zijn of te oud. Dergelijke voorbeelden zullen de geloofwaardigheid van de training ondermijnen en zorgen er voor dat het personeel afhaakt. Het heeft de voorkeur om voorbeelden te nemen die recent zijn gebeurd. De trainingen moeten in begrijpelijke taal zijn opgesteld. Andere voorwaarden voor het programma zijn: voor wie is de boodschap bedoeld, wat is het probleem, wat zijn de consequenties, wat moet je doen, wie heeft deze (nieuwe) regels opgelegd en waar kan je

<sup>10</sup> M.E. Whitman & H.J. Mattord, Principles of Information Security. Kennesaw State University, 2003.

terecht voor meer informatie (ISF p.48). Het security awareness programma moet naast een training gebruik maken van meerdere communicatiemiddelen, zoals presentaties, workshops, posters, nieuwsbrieven, videofilmjes op plekken waar veel personeel komt (bijvoorbeeld in de kantine), informatie op placemats of keycards. De gekozen communicatiemiddelen moeten elkaar versterken. Een ander belangrijk instrument voor een goede security awareness is het instellen van een incident reporting systeem en een incident respons systeem. Medewerkers kunnen hier verdachte situaties melden, desnoods anoniem. Deze melding moet vervolgens snel worden opgevolgd. Een terugkoppeling naar de melder zorgt er voor dat de melder in de toekomst weer zal melden<sup>11</sup>. Om de werknemers bewust te maken en het gedrag aan te passen zijn training en andere vormen van communicatie noodzakelijk.

#### *3.1.4 Kritische succesfactor: Coöperatie*

Coöperatie is erg belangrijk bij de ontwerpfase van het security awareness programma en bij het bepalen van de doelgroepen. Om zoveel mogelijk steun te krijgen voor het programma en om het effectief te laten zijn, moeten alle belanghebbenden (Hofland (2005) spreekt over sleutelfiguren) worden betrokken in het ontwerpen van het programma. Hierbij gaat het niet alleen om het management, maar juist ook om de mensen die het moeten waarmaken op de werkvloer. Door samen te werken met alle betrokken afdelingen en andere betrokken partijen wordt gezorgd voor betrokkenheid en commitment. In deze fase is het belangrijk om alle betrokken partijen te inventariseren en te kijken naar hun duwende en remmende krachten. Voordat het programma wordt afgebakend moeten de belanghebbenden zijn aangespoord om dit programma te steunen. Voor een goede samenwerking is afstemming tussen de verschillende onderdelen nodig.

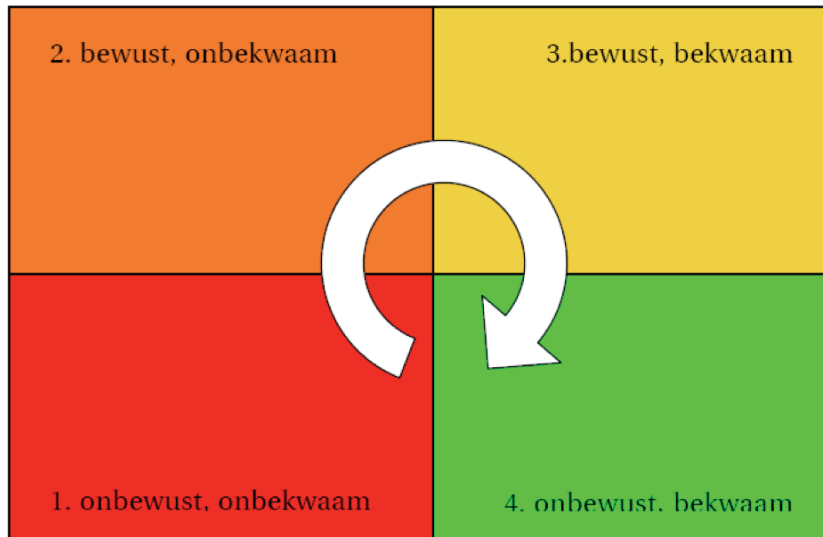
### **3.2 Individuele niveau**

#### *3.2.1 Kritische succesfactor: Bewustzijn*

Het management moet zorgen dat het personeel in staat is om security aware te zijn. Dat wil zeggen dat men het personeel de kennis en de vaardigheden over security awareness het personeel bij moeten brengen. Zo moet het personeel weten wat security awareness is en dat het belangrijk is (bewustwording). Daarnaast moet het personeel weten wat het moet doen als men in een ongewone situatie terecht komt (bekwaamheid). Uit de bekwaamheidsmatrix van Maslow is bekend dat het leren van nieuwe gewoonten in vier stadia gebeurt (Hofland, 2005). De bekwaamheidsmatrix beschrijft dit leerproces, zie figuur 4. De leerstijl van Maslow gaat uit van vier verschillende fasen:

1. onbewust, onbekwaam
2. bewust, onbekwaam
3. bewust, bekwaam
4. onbewust, bekwaam (routine)

<sup>11</sup> J.A. Valentine, *Enhancing the employee security awareness model*, Computer Fraud & Security, june 2006



Figuur 4: Bekwaamheidsmatrix van Maslow

Een voorbeeld zal de verschillende fasen verduidelijken: een persoon die nog nooit geprobeerd heeft om auto te rijden is zich niet bewust van alle te verrichten handelingen en noodzakelijke kennis voor het deelnemen aan het verkeer. Bij de eerste praktijkles zal duidelijk worden dat het autorijden nog niet zo gemakkelijk is. De persoon is zich bewust dat er nog meer praktijklessen nodig zijn. Na een aantal praktijklessen zijn de handelingen wel duidelijk, al moet de persoon nog wel nadenken over deze handelingen. Het is nog geen automatisme geworden. In de laatste fase zijn de handelingen een tweede natuur geworden, de persoon hoeft niet meer na te denken welke handelingen verricht moeten worden. Het is routine geworden.

Het ISF Framework gaat uit van een continu proces, het programma wordt aangepast aan nieuwe omstandigheden, nieuwe technieken en nieuwe procedures. Door deze nieuwe kennis blijft het personeel bewust. Uit de matrix van Maslow blijkt ook dat een individu moet blijven leren om in fase vier te blijven. Een belangrijk instrument om werknemers security aware te maken en te houden, is de resultaten van testen of gemelde incidenten terug te koppelen. Door de terugkoppeling bij een incident krijgt de persoon bevestiging dat hij goed heeft gehandeld. Door de terugkoppeling bij testen krijgt de persoon inzage in zijn eigen security awareness. De terugkoppeling is een belangrijk leermoment voor de werknemers.

De security awareness campagne moet op de doelgroep zijn afgestemd. De medewerkers moeten de beveiligingsmaatregelen begrijpen, zodat ze weten waarom deze zijn toegepast. Begrijpen ze niet waarom een beveiligingsmaatregel is toegepast, dan zijn ze blinde procedurevolgers en daarmee onbewust en onbekwaam (niveau 1)<sup>12</sup>.

<sup>12</sup> <sup>12</sup> L. van de Bosch, A. Hofman & M.C. Hoogenboom, De menselijke benadering van beveiligingsbewustwording, Informatiebeveiliging 7, 2003, p. 14-19

Ook de Tafel van Elf (2006) geeft aan dat onbekendheid met de regels en beleid kan leiden tot (onbewuste) overtreding. Oplossing voor dit probleem is te zorgen dat begrippen helder zijn en niet voor meerdere uitleg vatbaar en te zorgen voor gerichte, op de doelgroep afgestemde training en voorlichting.

### *3.2.2 Kritische succesfactor: Betrokkenheid*

Security awareness is geen primaire taak van de medewerkers en toch wordt van hen verwacht dat ze verdacht gedrag melden. Volgens de Tafel van Elf speelt de mate van acceptatie van beleid een grote rol. De "Leidraad motieven voor niet-integer handelen" (MinBZK, november 2007, p. 10-11) spreekt van de mate waarin regelgeving als relevant en ondersteunend wordt ervaren. Of een werknemer ook daadwerkelijk verdacht gedrag meldt, hangt af of hij dit beleid accepteert en zich erbij betrokken voelt. Meestal hangt de acceptatie af van de mate van redelijkheid van dit voorgestane beleid, en van de mate waarin de werknemers zichzelf verantwoordelijk voelen voor dit beleid.

De Leidraad (MinBZK) beschrijft dat medewerkers eerst in voldoende mate de morele dimensies en aspecten van een situatie moeten herkennen en erkennen voor zij adequaat kunnen handelen. De medewerker moet de situatie vervolgens zijn 'pakkie an' vinden, er verantwoordelijkheid voor nemen en het ook echt doen. Dit is echter niet zo gemakkelijk op een luchthaven, waarbij we met gedeelde verantwoordelijkheden te maken hebben. Hierdoor kan het probleem ontstaan dat veel mensen zich betrokken voelen, maar toch niets doen. Deze situatie kan zich voordoen, omdat medewerkers het niet vinden passen bij hun (specifieke) taak, functie of rol, doordat de verantwoordelijkheid niet (formeel) is belegd of omdat mensen bang zijn te worden bestraft, als ze actie ondernemen (zie ook beloning en cultuur). Culturele achtergrond speelt ook een rol, omdat het aanspreken van meerderen op gedrag in sommige culturen minder normaal is dan in Nederland. Daarnaast gaan sommige culturen 'flexibeler' om met regels dan in Nederland.

Belangrijk is daarom om duidelijk aan te geven wat de rol en verantwoordelijkheid is van de werknemers, geef de werknemers een belangrijke rol in het proces. De Tafel van Elf noemt als verbetermogelijkheid het betrekken van de invloedrijke leden van de groep en belangengroeperingen om gezamenlijk een beleid uit te werken dat voor iedereen werkt en waarbij alle rollen en verwachtingen duidelijk zijn. Uit de interviews die de IBB in het kader van dit onderzoek gehouden heeft, bleek ook dat het erg belangrijk is om werknemers uit te leggen waarom iets moet, naast het stimuleren en motiveren van personeel.

Normgetrouwheid speelt ook een rol bij de betrokkenheid. Het gaat hierbij om de eigen normen en waarden die samenhangen met geloof of gewoonte. Helaas is dit zeer moeilijk te beïnvloeden. Dit neemt de IBB daarom niet mee in haar onderzoek, al onderkennen wij wel dat de verschillende culturele en maatschappelijke achtergronden van het personeel op Schiphol deze factor extra moeilijk maakt.

### *3.2.3. Kritische succesfactor: Belang*

Volgens het ISF geven security awareness programma's vaak een eenzijdige boodschap. De boodschap legt meestal uit dat het

gewenste gedrag goed is voor de organisatie. Deze boodschap heeft echter geen enkel effect op het personeel. Het personeel heeft geen boodschap aan het succes van de organisatie of zij zien het verband tussen het succes van de organisatie en hun eigen succes niet in. In deze gevallen is het effectiever om gebruik te maken van de groepsdruk om het gedrag aan te passen. Onder groepsdruk verstaat de IBB dat een individu dingen doet die hij misschien niet persé wil, maar die hij toch doet omdat hij in een groep zit die deze dingen als normaal of goed beoordeelt. Zimbardo (2007, p.257 e.v.) geeft aan dat individueel gedrag voornamelijk wordt bepaald door de sociale situatie waarin dat gedrag plaatsvindt. De meeste mensen maken daarvoor een inschatting van de situatie. Als niet duidelijk is welk gedrag van ons wordt verwacht, wordt ons gedrag afgeleid uit het gedrag van anderen en overeenkomstig aangepast. Twee factoren zijn daarbij van invloed: de sociale rollen van de betrokkenen en de normen van de groep. Sociale rollen vertellen hoe je je moet gedragen. Elke groep ontwikkelt zijn eigen sociale rollen. Daarnaast ontstaan in elke groep 'ongeschreven regels' over de manier waarop de groepsleden zich moeten gedragen. Dit zijn de sociale normen van de groep. Het ISF Framework beschrijft (p. 47) als mogelijke maatregel het verbinden van individuele bonussen aan het gewenste gedrag van het gehele team of het stimuleren van invloedrijke individuen binnen het team om hun gedrag te verbeteren en een goed voorbeeld te zijn voor de rest van het team.

In hoofdstuk twee was al geconcludeerd dat een medewerker op beveiligd gebied geen belang heeft bij security awareness. Het betreden van de beveiligde gebieden door onbevoegden heeft geen consequenties voor zijn werkzaamheden. Om mensen betrokken te houden dient er zodoende gezocht te worden naar een eigen belang. Een direct eigen belang dat benadrukt kan worden is het feit dat de eigen veiligheid en die van collega's en passagiers in het geding is wanneer iemand in staat is om een explosief tot ontploffing te brengen. Daarnaast kunnen er kunstmatig belangen gecreëerd worden door de organisatie voor het personeel door straffen en beloningen te koppelen aan security awareness. Hierover in de volgende paragraaf meer.

#### *3.2.4. Kritische succesfactor: Beloning*

Een belangrijke manier om gedrag te beïnvloeden is te belonen bij gewenst gedrag of te bestraffen bij ongewenst gedrag. Uit psychologische literatuur (Zimbardo, 2007) over gedragsverandering blijkt dat bestraffen in het algemeen een significante invloed heeft op gedrag. Dit is echter alleen effectief als het tijdsverloop tussen het ongewenste gedrag en de straf zo minimaal mogelijk is. Een andere belangrijke voorwaarde is het consistent straffen. De intensiteit van de straf is een derde belangrijke factor. De invloed op het gedrag van de intensiteit van de straf is echter beperkt, omdat de kans om betrapt te worden zwaarder weegt dan de omvang van de straf<sup>13</sup>. Straffen is zeer geschikt bij het beïnvloeden van slecht gedrag, zoals

<sup>13</sup> J. van der Pligt, W.Koomen en F. van Harreveld, Bestrafen: een overzicht, een mythe en nieuwe varianten, Justitiële verkenningen, 2008-2

misbruik maken van de Schipholpas. Straffen is echter niet geschikt bij het creëren van een security-positieve no blame cultuur. Een medewerker moet zich veilig voelen om incidenten te melden. Om dit gewenste gedrag te beïnvloeden is belonen een belangrijke manier.

Uit interviews blijkt dat beloningen goed werken. Het gaat daarbij niet om financiële beloningen, maar om een mentale beloning in de vorm van waardering als goed werk is geleverd. Financiële beloningen leiden tot scheve ogen in de groep, zorgen binnen korte tijd voor gewenning en leiden af van de hoofdtak (IBB, mei 2008). Een mooi voorbeeld dat tijdens een interview werd genoemd om werknemers te belonen was het hebben van een "gouden boek" op de afdeling. In dit gouden boek staan de werknemers die verdachte situaties hadden gemeld en hoe dit was aangepakt ('lessons learned'). Dit boek was voor iedere werknemer inzichtelijk. De werknemers kunnen leren van de vermelde situaties. De genoemde werknemers worden in het boek genoemd en krijgen op deze manier een 'schouderklopje' van collega's en management. Van der Pligt et al.(2008) beschrijven een variant op deze manier: "naming and faming". In deze variant worden namen van werknemers die erg security aware zijn gepubliceerd in de bedrijfskrant of op een andere manier in het zonnetje gezet. Op dezelfde manier beschrijft Van der Pligt hoe notoire kwaadwillenden via "naming and shaming" aan de schandpaal kunnen worden genageld. Het 'namen and shamen' heeft wel beperkingen: het kan contraproductief werken waardoor werknemers gedemotiveerd raken.

Het ISF model beschrijft drie manieren om het gedrag van individuen aan te passen:

1. positieve benadering door het geven van bonussen en gratificaties, het publiceren van succesverhalen of 'faming' van individuen die het beoogde niveau van security awareness bezitten.
2. negatieve benadering door het 'big brother'-effect, 'naming en shaming' van individuen die zich niet aan de regels houden en het hertrainen van hardnekkige weigeraars.
3. neutrale benadering door beveiligingsvereisten op te nemen in een kwaliteitssysteem en in procedures.

### 3.3 Een vijfde C : Controle

Hofland (2005) geeft aan dat het meten van security awareness onmisbaar is voor een effectief programma. Hij voegt daarbij een vijfde C toe aan het model, de C van Controle. Het meten van security awareness is niet eenvoudig, maar wel erg belangrijk. Hiermee kan namelijk de effectiviteit van het security awareness programma worden gecontroleerd. Een meting kan ten eerste gebruikt worden om bij het management nogmaals commitment voor het programma te krijgen. De meting is ook te gebruiken voor het belonen van medewerkers en afdelingen die zich zeer security aware tonen. De eventuele zwakke schakels die naar voren komen kunnen extra training krijgen of, als het onwillende zwakke schakels zijn, desnoods via corrigerende maatregelen alsnog security aware

worden gemaakt. De volgende aspecten zijn van belang bij het meten:

- In welke fase bevindt men zich?
- Welk niveau van security awareness is voor de persoon, afdeling of organisatie nodig? Dat is namelijk niet voor iedereen gelijk!
- Welke mate van beveiligingsbewustzijn is al bij deze persoon, afdeling of organisatie aanwezig (nulmeting)?

R. de Vries et al. (juni 2007, p. 3) geeft drie beproefde manieren waarop een meting zou kunnen plaatsvinden: (1) fysieke observatie en mysteryguests, (2) face-to-face interviews en (3) vragenlijsten via internet. Een mysteryguest en een face-to-face interview zijn te combineren. Door voorbereide gesprekken te voeren met medewerkers is te achterhalen hoe medewerkers tegen security awareness aankijken, wat ze er onder verstaan hoe ze in bepaalde omstandigheden zouden handelen, en hoe ver hun kennis over de regels reikt. Deze face-to-face interviews zijn zeer geschikt als aanvulling op andere bewustzijnsmetingen, omdat ze erg bewerkelijk zijn en niet geschikt voor een grootschalig onderzoek. Een mysteryguest gaat, bekend met de regels voor het personeel, fysiek locaties betreden en let daarbij op incidenten die duiden op een tekort aan bewustzijn. Hij onderzoekt daarbij ook of hij beveiligde gebieden kan betreden en wordt aangesproken op zijn aanwezigheid. Een actie van een mysteryguest moet wel geëvalueerd worden met het slachtoffer. Tijdens dit face-to-face gesprek zal het "slachtoffer" aangeven hoe hij en de omgeving op deze actie hebben gereageerd. Uit dit gesprek kan in kwalitatieve zin het bewustzijn van het slachtoffer en de omgeving worden gedestilleerd. De vragenlijsten via internet kunnen worden losgelaten op alle medewerkers binnen een organisatie. De steekproef wordt hierdoor wel groter, maar de vragenlijst moet zeer zorgvuldig worden opgesteld en moet een goede balans bevatten tussen kennis, attitude en gedrag. Deze vragenlijsten zijn zeer geschikt om een indicatie te krijgen waar het goed gaat en waar de schoen wringt. Op basis van deze indicatie kan gericht worden gezocht naar achterliggende oorzaken met behulp van interviews en mysteryguests.

Het ISF Model spreekt van een continu proces. Na het meten van het niveau van security awareness wordt opnieuw een risicoanalyse gemaakt. De frequentie van het meten is afhankelijk van het feitelijke en gepercipieerde risico voor de luchthaven. Dit risico moet opnieuw worden geanalyseerd, bijvoorbeeld bij een verhoogde dreiging. Het gewenste niveau van security awareness moet aan de hand van deze nieuwe informatie worden vastgesteld. Dit wordt vervolgens via een aangepast programma, met aandacht voor de kritische succesfactoren, bij de werknemers onder de aandacht gebracht en kan vervolgens weer worden gemeten. Het continu proces is dan weer rond.

### 3.4 Conclusie

Uit het bovenstaande blijkt dat er vier knoppen zijn op het organisatorisch niveau (de 4 C's) en vier op het individueel niveau

(de 4 B's) die gebruikt kunnen worden om security awareness te beïnvloeden. Op het organisatorisch niveau is het belangrijk dat het management laat zien dat men security awareness serieus neemt door het goede voorbeeld te geven, door security awareness op te nemen in de bedrijfsvoering, door tijd en geld vrij te maken voor het ontwikkelen van een training en door tijd en geld vrij te maken voor het personeel om deze training te volgen. Dit valt onder de succesfactor Commitment. Het management speelt bij de tweede succesfactor, Cultuur, ook een grote rol. Zij moet zorgen voor een 'no blame' cultuur, zodat de medewerkers niet bang zijn om incidenten te melden. De Communicatie, de derde succesfactor, schept de criteria voor een effectief security awareness programma: heldere doelen, afgestemd op de doelgroep, duidelijke boodschap en de belangrijkste 'w's (wie, wat, waarom, waar). Verder dient het management te zorgen voor een incident reporting en respons systeem. Bij het opstellen en uitvoeren van het programma is Coöperatie, de vierde succesfactor op organisatorisch niveau, erg belangrijk. De betrokkenen moeten samenwerken om het programma tot een goed einde te brengen.

Op individueel niveau heeft de IBB de vier B's beschreven. Medewerkers moeten bewust worden gemaakt van het waarom van security awareness en moeten weten wat ze moeten doen wanneer ze iets verdachts zien (handelingsperspectief). Deze training moet op de doelgroep zijn afgestemd om resultaat te bereiken. Heldere taal en bekendheid met de regels en het beleid zullen bijdragen aan een beter Bewustzijn. Dit is de eerste individuele succesfactor. Betrokkenheid, de tweede factor, kan worden gestimuleerd door de medewerkers duidelijk te vertellen welke rol en verantwoordelijkheden de diverse partijen, en zij zelf in het bijzonder, hebben. Belangrijk is daarbij om duidelijk aan te geven waarom bepaalde handelingen verplicht zijn. De derde succesfactor, Belang, is erg moeilijk te beïnvloeden, omdat een medewerker niet noodzakelijk direct belang heeft bij security awareness. Hiervoor kunnen kunstmatige belangen worden gemaakt (zoals beloningen) of kan er meer nadruk worden gelegd op de eigen veiligheid en die van collega's en passagiers. De vierde succesfactor, Beloning, kan worden gebruikt om gedrag te beïnvloeden. De IBB heeft een aantal manieren beschreven. Straffen is niet gewenst, omdat men wil voorkomen dat mensen uit angst geen incidenten meer melden. Een extra succesfactor, Controle, is opgenomen, omdat door het meten de effectiviteit van het programma kan worden bepaald. De controle kan aanleiding zijn om het programma, inclusief de risico's te herzien. Een nieuwe risicoanalyse kan leiden tot een aangepast (verhoogd) gewenst niveau van security awareness en een aangepast programma.

## **4. Security awareness: de stand van zaken in Nederland**

In Nederland zijn een aantal organisaties direct, dan wel indirect betrokken bij het security aware maken en houden van de medewerkers op de luchthaven. Deze organisaties worden hieronder kort besproken. Zowel overheden als het bedrijfsleven zijn in verschillende rollen (regelgever, uitvoerder of toezichthouder) betrokken bij het security aware maken en houden van de werknemers. In dit hoofdstuk wordt uitgewerkt wie welke rol vervult voor het op peil brengen en houden van security awareness op luchthavens in Nederland. Daarnaast geven we de minimale kenniseisen voor security awareness op luchthavens aan.

### **4.1 Beleid en wet- en regelgeving over security awareness**

De DBB is in Nederland als 'appropriate authority' verantwoordelijk voor het vaststellen van beleid en wet- en regelgeving. Ook voor het vaststellen van het gewenste niveau van security awareness. Daarnaast is de DBB belast met het doorvertalen van Europese wet- en regelgeving naar de Nederlandse situatie en het vaststellen van beleid. Zij stelt ook het Nationaal Trainingsprogramma op, waar de minimale eisen voor de security awareness training in zijn opgenomen.

### **4.2 Opleiden**

Het opleiden van personeel is een verantwoordelijkheid van meerdere partijen. Beveiligingsbedrijven leiden hun eigen personeel op voor het onderwerp security awareness. De luchthavenexploitant, Amsterdam Airport Schiphol (AAS), is verantwoordelijk voor het opleiden van al het personeel dat toegang moet krijgen tot de beveiligde gebieden. De luchthavenexploitant, luchtvaartmaatschappijen, geregistreerde bekende leveranciers, geregistreerde luchtvrachtagenten en schoonmaak- en cateringbedrijven zijn verantwoordelijk voor de inzet van adequaat opgeleid personeel en het verzorgen van de opfriscursussen. De KMar toetst de initiële opleidingen op het gebied van security awareness en keurt de opleidingsorganisaties goed. Het Bureau Handhaving en Toezicht van de KMar (District Schiphol) toetst of de opleidingen voldoen aan de eindtermen die zijn opgenomen in het Nationaal Trainingsprogramma. Vervolgens worden de opleidingen ter goedkeuring aan de DBB voorgelegd, zodat geborgd is dat de initiële opleidingen van voldoende kwaliteit zijn. De opfriscursussen worden noch getoetst noch goedgekeurd.

### **4.3 Toezicht op de security awareness**

Het dagelijks toezicht op de beveiliging, met inbegrip van de security awareness, vindt plaats door de KMar. Het Bureau Handhaving en Toezicht van de KMar (District Schiphol) houdt door middel van testen, inspecties en audits toezicht op de uitvoering van de beveiliging. Hierbij kijkt men naar de security awareness van personeel (wordt de auditor aangesproken op zijn aanwezigheid). De KMar bespreekt de misstanden met de security manager van de geteste organisatie.

De luchthavenexploitant voert testen en audits uit op de security awareness van beveiligingsbedrijven, niet van het overige personeel op de luchthaven. Daarnaast wordt toezicht gehouden door nationale (IBB) en internationale inspecterende instanties (EC, ECAC, ICAO en FAA).

#### **4.4 Nationaal Trainingsprogramma**

De DBB stelt, namens de Minister van Justitie, het Nationaal Trainingsprogramma op. In dit trainingsprogramma staan de "eisen waaraan beveiligingspersoneel, en ander personeel dat betrokken is bij de beveiliging van de burgerluchtvaart, moet voldoen". De minimale eisen die gesteld worden aan de kennis en vaardigheden van personeel dat werkzaam is op de beveiligde gebieden en beveiligingspersoneel zijn vastgelegd in zogenaamde eindtermen. Initiële opleidingen<sup>14</sup> mogen alleen worden gegeven door opleidingsorganisaties dan wel individuele opleiders die door de Minister van Justitie zijn goedgekeurd. Een opleidingsorganisatie, dan wel een individuele opleider, dient haar opleidingsprogramma ter beoordeling aan te bieden aan de KMar en verder te voldoen aan een aantal voorwaarden. De opfriscursussen worden georganiseerd door de voor de security awareness verantwoordelijke organisaties. Deze organisaties moeten vastleggen op welke wijze zij zorgdragen voor adequate opfriscursussen.

Samengevat wordt van een medewerker met toegang tot beveiligde gebieden van een luchthaven verwacht dat hij:

- het onderscheid kent tussen verdachte, gevaarlijke en levensbedreigende situaties;
- weet hoe hij in deze situaties moet handelen;
- weet welke beveiligingsmaatregelen zijn getroffen;
- begrijpt waarom deze beveiligingsmaatregelen zijn getroffen.

#### **4.5 Conclusie**

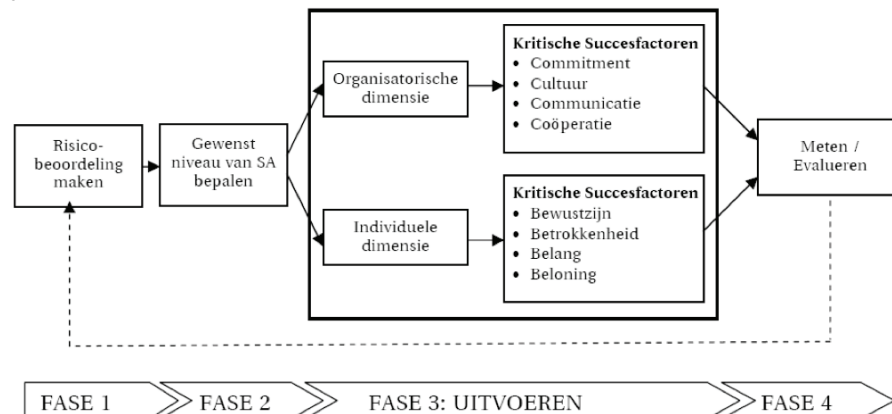
Hierboven hebben we gelezen dat de luchthavenexploitant verantwoordelijk is voor het opleiden van personeel dat toegang heeft tot de beveiligde gebieden. In dit onderzoek is daarom gekeken naar de middelen die de luchthavenexploitant kan inzetten om werknemers security aware te maken en te houden. De luchthavenexploitant kan de security awareness aanpakken door te sturen op de in hoofdstuk twee genoemde kritische succesfactoren. Indien daar aanleiding voor is, is ook de rol van andere partijen (DBB, KMar en anderen) belicht.

<sup>14</sup> Nationaal Trainingsprogramma, december 2007: Met uitzondering van de opleiding voor personeel van de luchtvaartmaatschappij dat belast is met de beveiliging van vliegtuigen en het toezicht op gecontroleerde ruimbagage en voor managers

## 5. Conclusies

De vraag die in dit rapport centraal staat, te weten “Welke factoren zijn van belang voor het security aware maken en houden van de werknemers op een luchthaven?” is beantwoord in hoofdstuk twee. Aan de hand van het model van Neys, Hofland en het Information Security Framework zijn acht kritische succesfactoren gedefinieerd die van belang zijn voor het maken en uitvoeren van een effectief security awareness programma. Het gaat om de 4C’s, Commitment, Cultuur, Communicatie en Coöperatie, en de 4B’s, Bewustzijn, Belang, Betrokkenheid en Beloning. Deze acht kritische succesfactoren zijn in hoofdstuk drie nader toegelicht. Dit hoofdstuk beschrijft ook hoe de succesfactoren beïnvloed kunnen worden. In hoofdstuk vier is beschreven welke organisaties een rol spelen bij het security aware maken en houden van de werknemers en welke eisen minimaal gesteld worden aan de security awareness van de werknemers.

Het in hoofdstuk 2 beschreven model wordt gebruikt om de balans op te maken.



Figuur 5: Kritische succesfactoren voor security awareness op luchthavens

Het is allereerst van belang om een risicoanalyse voor de luchthaven te maken. Uit deze analyse volgt het gewenste niveau van security awareness bij de medewerkers. Het gaat hierbij niet alleen om de kennisoverdracht en vaardigheden, maar ook om het gewenste gedrag. Zodra het gewenste niveau van security awareness is bepaald kan een security awareness programma worden opgesteld met diverse op de doelgroep afgestemde trainingen en bewustwordingscampagnes. Het is belangrijk dat deze trainingen en campagnes onderdeel uitmaken van het integrale samenhangende security awareness programma.

Bij het opstellen van een integraal security awareness programma zijn de acht kritische succesfactoren van belang. Ze worden hieronder genoemd, voorzien van middelen die ingezet kunnen worden door de partijen.

Kritische succesfactor	Middelen
Commitment	<ul style="list-style-type: none"> <li>▪ Stel een beleidsvisie security awareness op;</li> <li>▪ Geef het goede voorbeeld (draag pas zichtbaar, spreek mensen aan);</li> <li>▪ Stel tijd beschikbaar om trainingen te volgen;</li> <li>▪ Leg security awareness vast in de bedrijfsvoering.</li> </ul>
Cultuur	<ul style="list-style-type: none"> <li>▪ Stimuleer security positief gedrag;</li> <li>▪ Stel grenzen aan ongewenst gedrag;</li> <li>▪ Maak security awareness bespreekbaar.</li> </ul>
Communicatie	<ul style="list-style-type: none"> <li>▪ Stem de boodschap af op de doelgroep;</li> <li>▪ Maak gebruik van meerdere, elkaar aanvullende communicatiemiddelen;</li> <li>▪ Geef onmiddellijk terugkoppeling na testen, inspecties en audits.</li> </ul>
Coöperatie	<ul style="list-style-type: none"> <li>▪ Stel het security awareness programma met betrokken partijen op;</li> <li>▪ Stem de doelgroepgerichte campagnes en trainingen op elkaar af.</li> </ul>
Bewustzijn	<ul style="list-style-type: none"> <li>▪ Zorg voor heldere en eenduidige definities in de diverse campagnes en trainingen;</li> <li>▪ Stem de doelgroepgerichte campagnes en trainingen op elkaar af;</li> <li>▪ Zorg voor recente voorbeelden in de trainingen en campagnes;</li> <li>▪ Geef onmiddellijke terugkoppeling na testen, inspecties en audits, zodat de persoon kan leren van zijn gedrag.</li> </ul>
Betrokkenheid	<ul style="list-style-type: none"> <li>▪ Stel het programma met betrokken partijen en werknemers op;</li> <li>▪ Geef de werknemers een duidelijke rol en verantwoordelijkheid in het proces;</li> <li>▪ Leg duidelijk uit <i>waarom</i> security awareness zo belangrijk is;</li> <li>▪ Stimuleer en motiveer de medewerkers.</li> </ul>
Belang	<ul style="list-style-type: none"> <li>▪ Creëer belangen voor de medewerkers om security aware te zijn (bijv. eigen veiligheid, straf bij misbruik van luchthavenpas);</li> <li>▪ Maak gebruik van de groepsprocessen om het gedrag te veranderen.</li> </ul>
Beloning	<ul style="list-style-type: none"> <li>▪ Beloon gewenst gedrag en bestraf ongewenst gedrag (naming en faming vs. naming en shaming);</li> <li>▪ Deel opgedane kennis via 'lessons learned'.</li> </ul>

Als het security awareness programma is opgesteld en uitgevoerd volgt een belangrijke stap: het controleren en meten van het niveau van security awareness. Met de controle wordt bepaald of het gewenste niveau van security awareness is behaald. Daarnaast is deze informatie input voor een nieuwe risicoanalyse. Het nieuwe gewenste niveau van security awareness kan worden bepaald, waarna het integrale programma overeenkomstig kan worden aangepast en uitgevoerd. Op deze wijze wordt security awareness een continu en effectief proces.

In de vertrouwelijke versie is de praktijk op Schiphol getoetst aan de acht kritische succesfactoren. Hiervoor zijn gesprekken gevoerd met partijen die werkzaam zijn op de luchthaven en met de luchthavenexploitant zelf. Deze informatie is vertrouwelijk, maar is voor direct belanghebbende partijen op te vragen bij de Directie Beveiliging Burgerluchtvaart van de Nationaal Coördinator Terrorismebestrijding (NCTb).

Meer informatie over dit rapport is te verkrijgen bij:

Nationaal Coördinator Terrorismebestrijding  
Inspectie Beveiliging Burgerluchtvaart  
Postbus 16950  
2500 BZ Den Haag  
Telefoon: 070-315 0 451

## ***Bijlage 1: Overzicht gebruikte bronnen***

Amsterdam Airport Schiphol, Beveiligingsplan, september 2007.

Bosch, van de, L., Hofman, A. & Hoogenboom, M.C. De menselijke benadering van beveiligingsbewustwording, Informatiebeveiliging 7, 2003

Directie Beveiliging Burgerluchtvaart, Nationaal Trainingsprogramma, december 2007

European Union, Attachment to technical annex to Inspection Report 05/07/AMS/NL/AP

European Union, Attachment to technical annex to Inspection Report 05/07/AMS/NL/FU

Hinderink, S. en Hendriks, S., Informatiebeveiliging en awareness, onlosmakelijk verbonden, Informatiebeveiliging juni 2007

Hoffmann BV: [www.hoffmannbv.nl](http://www.hoffmannbv.nl) Is de mens de zwakste schakel?, 2008

Hofland, V. Bewust van informatiebeveiliging, januari 2005

Inspectie Beveiliging Burgerluchtvaart, X-ray screeners doorgelicht, mei 2008

Information Security Forum, Effective security awareness, workshop report, april 2002

Kanters, F.M., Beveiligingsbewustzijn als missie, IT Beheer 8, november 2006

Koot, A. en Haas, de J., Organisaties overschatten niveau van awareness, Informatiebeveiliging juli 2005

Prof. Dr. F.L. Leeuw, Trends in toezichtsland en toezicht op ondernemingen gedragswetenschappelijk beschouwd, Discussiemiddag Toezicht en compliance, 26 september 2008-10-09

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Leidraad motieven voor niet-integer handelen. Sociaal-psychologische factoren. November 2007

Nederlands Normeninstituut, NEN-ISO/IEC 27002, Informatietechnologie-Beveiligingstechnieken-Code voor informatiebeveiliging (ISO/IEC 27002:2005, IDT), november 2007

Neys, C., IT'ers, regels en security awareness, april 2003

Neys, C. & Van der Schaaf, T., Grip op 'de factor mens', Informatiebeveiliging, december 2004

Pligt, van der J., Koomen, W. & Harreveld, van F., Bestrafen: een overzicht, een mythe en nieuwe varianten, Justitiële verkenningen, 2008-2

Thomson, K. Von Solms, R. & Louw, L., Cultivating an organizational information security culture, Computer Fraud & Security, oktober 2006

Valentine, J.A., Enhancing the employee security awareness model, Computer Fraud & Security june 2006

De Vries, dr. ir. R. en Dolfsma, R. CISSP, Het meten van informatiebeveiligingsbewustzijn, Informatiebeveiliging juni 2007

Whitman, M.E. & Mattord, H.J., Principles of information security, Kennesaw State University, 2003

Zimbardo, P.G., Weber, A.L., Johnson, R.L., Psychologie: de essentie, Pearson Education 2007

## ***Bijlage 2: Overzicht geïnterviewde organisaties***

De IBB heeft gesproken met de volgende organisaties voor achtergrond informatie over security awareness projecten:

- TU Delft, Security manager ICT
- Nationaal Lucht- en Ruimtevaartlaboratorium, Senior Project engineer
- Nationaal Lucht- en Ruimtevaartlaboratorium, R&D engineer
- Ministerie van Defensie, Beveiligingsautoriteit
- Grimbergen SICT, security awareness opleider

De IBB heeft met de volgende organisaties gesproken over de praktijksituatie op Schiphol:

- Amsterdam Airport Schiphol, Manager Badge Center
- Amsterdam Airport Schiphol, Senior Policy Manager
- Amsterdam Airport Schiphol, Communicatiemedewerker
- Amsterdam Airport Schiphol, Auditor security and safety
- Amsterdam Airport Schiphol, Security Advisor
- Menzies, Manager Security Netherlands
- Menzies, Security awareness docent
- Gate Gourmet BV, Manager P&O (telefonisch)
- Alpha Flight Services BV, Outbound Logistics Manager
- KLM, Senior Vice-President Security
- Servisair, Manager Quality Control
- CSU Airport Services, District Manager Schiphol
- KMar, Bureau Handhaving & Toezicht

### ***Bijlage 3: Lijst met afkortingen***

AAS	Amsterdam Airport Schiphol
DBB	Directie Beveiliging Burgerluchtvaart
EC	Europese Commissie
IBB	Inspectie Beveiliging Burgerluchtvaart
ISF	Information Security Framework
KMar	Koninklijke Marechaussee
LVW	Lucht Vaart Wet
MinBZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
NLR	Nationaal Lucht- en Ruimtevaartlaboratorium
WODC	Wetenschappelijk Onderzoek en Documentatie Centrum

## De NCTb werkt aan een veiliger samenleving

De Nationaal Coördinator Terrorisbestrijding heeft als taak het risico van en de vrees voor terroristische aanslagen in Nederland zoveel mogelijk te verkleinen, alsmede het op voorhand beperken van schade als gevolg van een mogelijke aanslag. De NCTb heeft de centrale regie rond terrorisbestrijding en zorgt dat de samenwerking tussen alle betrokken partijen op een structureel hoog niveau komt en blijft.