Integratie van informatiebeveiliging

Noodzakelijk voor effectieve bedrijfsvoering

Organisaties verwerken steeds meer en steeds sneller informatie, en wisselen steeds meer informatie uit. Het al dan niet beschikken over de juiste informatie en ervoor zorgen dat die informatie niet in verkeerde handen valt, kan het verschil zijn tussen een bloeiende onderneming en faillissement. Informatiebeveiliging is dan ook onontbeerlijk. Maar informatiebeveiliging wordt nog te vaak als een opzichzelfstaand fenomeen gezien en aangepakt. Dit komt de effectiviteit en de efficiëntie ervan niet ten goede. Integratie van informatiebeveiliging en de overige bedrijfsprocessen is noodzakelijk. Maar in welke mate is integratie nodig?

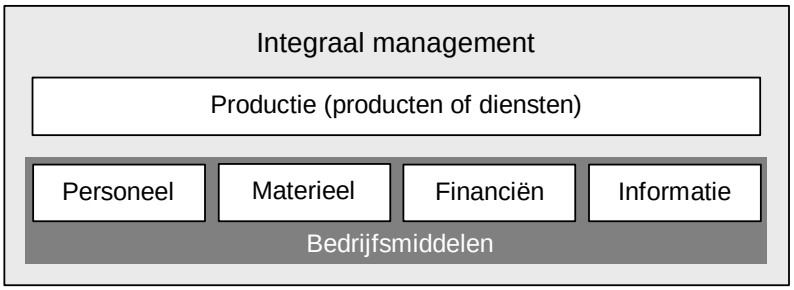
Auteur: **Dr. Marcel Spruit** is lector Informatiebeveiliging aan de Haagse Hogeschool en TH Rijswijk, en tevens als adviseur verbonden aan Het Expertise Centrum.

Iedere organisatie functioneert in een context. Hieruit ontstaan enerzijds nieuwe kansen voor de organisatie, maar anderzijds ook risico's. Organisaties zijn immers vatbaar voor allerlei verschillende bedreigingen, zoals koersschommelingen, arbeidsonrust, criminaliteit en computervirussen. Risico's kunnen betrekking hebben op verschillende aspecten van de bedrijfsvoering: personeel, materieel, financiën, maar ook de informatievoorziening. Risico's zijn nooit helemaal te voorkomen, ze horen nu eenmaal onlosmakelijk bij ondernemen. Wel zullen verantwoordelijke managers ernaar streven om de risico's te beperken, om maatregelen te treffen tegen alle bedreigingen die tot onacceptabele risico's leiden. Het effectief managen van risico's vereist dat managers oog hebben voor de relevante bedreigingen en de daaruit voortvloeiende risico's. Bovendien dienen managers de risico's met betrekking tot verschillende bedrijfsaspecten in onderlinge samenhang te beschouwen en op basis daarvan prioriteiten te stellen. Het aanpakken van risico's met betrekking tot de informatievoorziening is dan geïntegreerd met het aanpakken van andere risico's voor de bedrijfsvoering [SpGr, 2004].

Integraal management en informatiebeveiliging

Het integraal managen van risico's door het management van een organisatie is noodzakelijk voor een effectieve bedrijfsvoering. Het management gedraagt zich dan zoals een goede huisvader zijn huishouden bestiert. Dit wordt ook wel aangeduid als corporate governance. Corporate governance gaat impliciet uit van integraal management [BuJa, 1999]. Hierbij is het topmanagement van een organisatie volledig verantwoordelijk voor de gehele bedrijfsvoering, inclusief alle daarvoor benodigde processen en middelen (zie figuur 1). Bij toenemende omvang en complexiteit van een organisatie is het topmanagement echter niet meer in staat alles direct aan te sturen. Delegeren is dan nodig. Ook als het topmanagement bepaalde verantwoordelijkheden aan lijn-, proces- of projectmanagers delegeert, blijft de eindverantwoordelijkheid hiervoor toch bij het topmanagement liggen. De managers waaraan de betreffende verantwoordelijkheden gedelegeerd zijn, zijn dan vanuit het topmanagement ge-

zien weliswaar verantwoordelijk geworden, maar van buiten de organisatie gezien is het topmanagement nog steeds volledig verantwoordelijk.



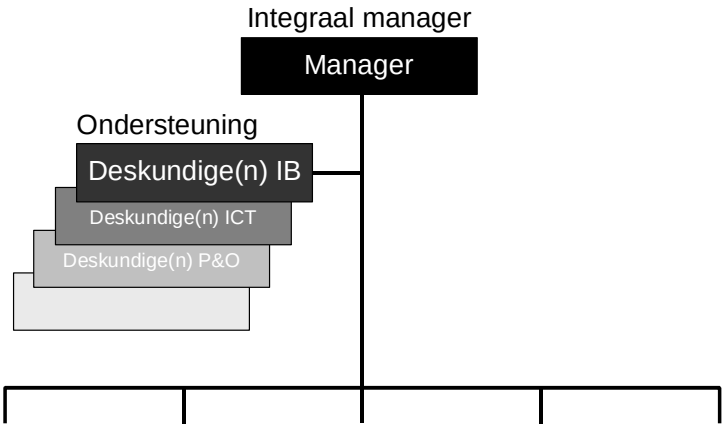
Figuur 1: Integraal management [1]

Zoals het topmanagement bepaalde verantwoordelijkheden aan het onderliggende management kan delegeren (eventueel met uitsluiting van bepaalde bedrijfsmiddelen, of onder beperkende randvoorwaarden), zo kan dit management zelf weer verantwoordelijkheden verder de organisatie in delegeren. Ook hierbij geldt dat de verantwoordelijkheid de daarvoor benodigde processen en middelen omvat, zonder dat de eindverantwoordelijkheid meeschuift. Daarmee valt het managen van het bedrijfsmiddel informatie, en ook het beveiligen ervan, onder de reguliere verantwoordelijkheid van lijn-, proces- en projectmanagers.
Echter, een integraal manager zal veelal niet genoeg tijd en aandacht voor informatiebeveiliging kunnen en willen opbrengen [Spruit, 2004]. Dit wordt ten eerste veroorzaakt doordat de meeste managers geen achtergrond op het gebied van informatiebeveiliging hebben, en daardoor onvoldoende kennis en ervaring op dit terrein bezitten. Ten tweede moet elke manager zijn tijd en aandacht over allerlei verschillende aandachtspunten verdelen, van personeel tot informatie, en van productie tot beveiliging. Ten derde constateren veel managers (onterecht, maar wel verklaarbaar) dat er binnen de eigen organisatie zelden incidenten met betrekking tot de informatievoorziening optreden. In dit krachtenveld ligt het voor de hand dat een manager in het algemeen weinig aandacht heeft voor informatiebeveiliging.
Toch staat of valt informatiebeveiliging bij de aandacht vanuit het management, hoe gering ook. Informatiebeveiliging heeft namelijk top-down sturing nodig om effectief en efficiënt te zijn. Dit betekent dat elke manager die vanuit zijn integrale managementverantwoordelijkheid ook verantwoordelijk is voor informatiebeveiliging een minimale interesse voor informatiebeveiliging moet hebben. Vanuit die interesse kan de manager tot de conclusie komen dat het onderwerp voldoende relevant is om daar zelf tijd aan te besteden, of dit anders bij een of meer deskundigen te beleggen. Deze deskundige(n) kan (kunnen) de manager adviseren over de informatiebeveiligingsvraagstukken en bovendien een belangrijke rol vervullen in het coördineren en ondersteunen van beveiligingsactiviteiten [Goor, 2002; OvRo, 2002]. Hierbij valt onder meer te denken aan het uitvoeren van risicoanalyses, het installeren en onderhouden van beveiligingsapparatuur, het registreren van beveiligingsincidenten, het afstemmen met specialistische organisatie-eenheden zoals de automatiseringsafdeling, en het overleggen met externe beveiligingspartijen. De manager heeft dan zelf alle tijd om zich met

[1] Andere indelingen van bedrijfsmiddelen komen ook voor, zoals binnen de overheid PIOFAH (personeel, informatie, organisatie, financiën, administratie, huisvesting).

andere zaken bezig te houden. Wel blijft de manager eindverantwoordelijk. Dit betekent dat alle beslissingen met betrekking tot informatiebeveiliging in principe door de manager genomen worden (eventueel pro forma), terwijl al het voorbereidende werk door de deskundige(n) kan worden gedaan.
Een informatiebeveiligingsdeskundige die een manager ondersteunt, kan een staffunctionaris binnen de organisatie(-eenheid) van de manager zijn (zie figuur 2), maar dat is niet perse nodig. Het is heel goed mogelijk dat de deskundige elders binnen de organisatie gepositioneerd is en functioneel aangestuurd wordt door de manager. Het is zelfs mogelijk dat de deskundige een externe is die hiervoor tijdelijk is aangetrokken. Waar de deskundige ook vandaan komt en hoe hij ook gepositioneerd is, er worden hoge eisen aan gesteld: ruime bedrijfskundige kennis en inzicht, uitgebreide ICT-kennis en goede communicatieve vaardigheden.

Een manager die verantwoordelijk is voor informatiebeveiliging, hoeft daar dus maar weinig tijd aan te besteden. Desalniettemin moet de manager tenminste één of meer deskundigen, of een stuurgroep, op het gebied van informatiebeveiliging aanwijzen. Bovendien moet de manager zijn medewerkers motiveren om informatiebeveiliging serieus te nemen, onder meer door zelf het goede voorbeeld te geven. Als deze weinige inspanning te veel gevraagd is, moet vanuit het hogere management worden aangestuurd op een serieuzere aanpak van informatiebeveiliging. Als echter het hoogste management van de organisatie informatiebeveiliging niet serieus neemt, dan komt informatiebeveiliging in de betreffende organisatie niet goed van de grond. Slechts de wetgever en de markt kunnen dan bijsturen, maar dat zal veelal slechts gebeuren als het de spuigaten uitloopt.



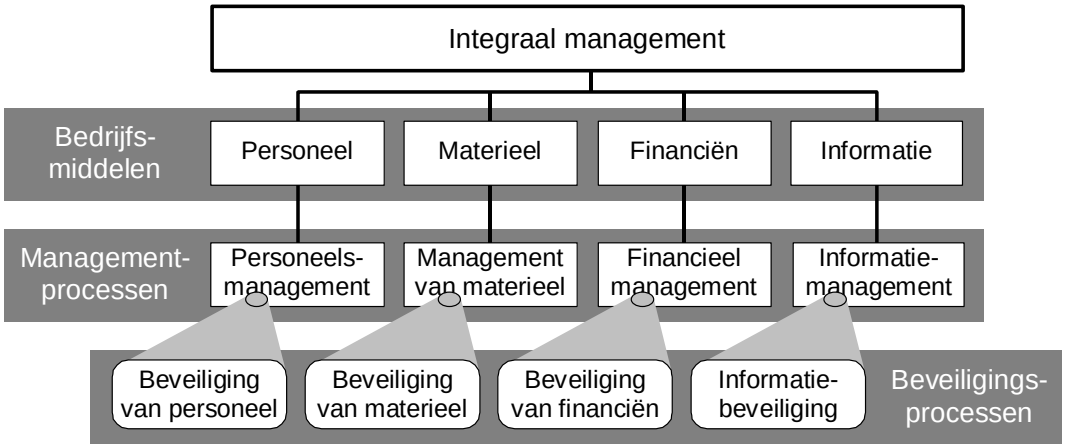
Figuur 2: De (integraal) manager en zijn deskundigen

Een manager die informatiebeveiliging heel serieus neemt, komt overigens voor een lastig dilemma te staan: alle bedrijfsmiddelen die je voor informatiebeveiliging inzet, kunnen niet voor andere zaken ingezet worden. Door ad hoc getroffen maatregelen binnen een doorsnee organisatie treden echter zelden tot nooit ernstige informatiebeveiligingsincidenten op. Hoe rechtvaardig je in dat geval de inzet van middelen voor informatiebeveiliging? Zijn die middelen geen pure verspilling? Deze vragen zijn door veel managers niet zonder meer te beantwoorden en dat kan een negatief effect hebben op de motivatie voor informatiebeveiliging.

De oplossing voor dit dilemma van de manager ligt in de aangewezen informatiebeveiligingsdeskundigen. Deze deskundigen dienen zich niet alleen bezig te houden met informatiebeveiligingsvraagstukken die op het bordje van de integraal manager liggen, maar ze dienen bovendien uit eigen beweging te werken aan het verbeteren van de risicoperceptie van de manager. Hiervoor verzamelen ze gegevens over opgetreden bedreigingen, (bijna-)incidenten en reeds getroffen maatregelen. In het algemeen blijkt dan dat zich regelmatig bedreigingen manifesteren, maar dat ze veelal door de (weliswaar ad-hoc)maatregelen worden opgevangen. Het ad-hockarakter van de getroffen maatregelen is echter inefficiënt en laat bovendien onacceptabele gaten vallen. De informatiebeveiligingsdeskundigen kunnen de managers op dit gebied gevraagd en ongevraagd voorlichten. Met name het ongevraagd voorlichten schiet er in de praktijk nogal eens bij in, maar toch is juist dat zeer belangrijk voor het verbeteren van de motivatie voor informatiebeveiliging bij de managers.

Integratie van informatiefuncties versus beveiligingsfuncties

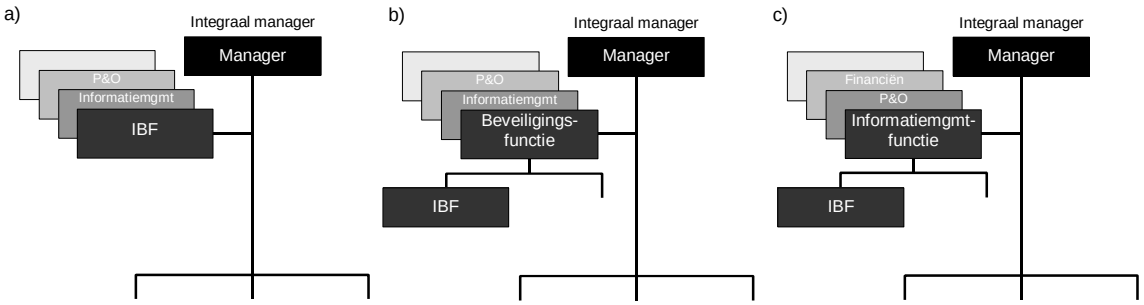
In het kader van integraal management is elke manager verantwoordelijk voor het managen van de risico's die betrekking hebben op de middelen die 'zijn' organisatie(-eenheid) nodig heeft. Ten aanzien van al deze middelen zal de betreffende manager maatregelen moeten treffen tegen de bedreigingen die tot onacceptabele risico's leiden. Het inrichten en onderhouden van deze maatregelen is onderdeel van de beveiligingsprocessen van de betreffende organisatie(-eenheid).
In eerste instantie ligt het voor de hand om de beveiligingsprocessen te relateren aan de verschillende bedrijfsmiddelen (zie figuur 3). Zo omvat informatiebeveiliging het beveiligen van de geautomatiseerde en niet-geautomatiseerde informatievoorziening. De beveiliging van materieel omvat de beveiliging van het bedrijfspand, de ruimten in het pand, het meubilair en de apparatuur, enzovoort. De grens tussen de beveiliging van informatie en de beveiliging van de andere bedrijfsmiddelen is echter niet altijd even duidelijk. Zo valt bijvoorbeeld de beveiliging van kasten en apparatuur onder de beveiliging van materieel, maar de beveiliging van personeelsdossierkasten en ICT-apparatuur valt (ook) onder informatiebeveiliging. Daarnaast wordt voor de beveiliging van personeel, materieel en financiën steeds vaker ICT ingezet, waarvan de beveiliging op het bordje van de informatiebeveiliging ligt. In feite gaan de beveiligingsprocessen van de verschillende bedrijfsmiddelen in elkaar over. Er is dan ook sprake van een geïntegreerde verzameling beveiligingsprocessen. De integratie van de beveiligingsprocessen gaat hand in hand met de integratie van de managementprocessen van de bedrijfsmiddelen, en past dus goed in het concept van integraal management.



Figuur 3: De integratie van informatiebeveiliging

Als desondanks de informatiebeveiligingsprocessen in de organisatie los van de andere beveiligingsprocessen ingericht zijn, is het resultaat daarvan dat de informatiebeveiligers en de andere beveiligers langs elkaar heen werken. Hierdoor ontstaan inefficiënties en problemen in de organisatie, bijvoorbeeld het dubbel beveiligen van bepaalde objecten, het herhalen van analyses door de verschillende beveiligingsdisciplines en het kiezen van onderling incompatibele methoden en technieken. Ook kunnen er gaten in de beveiliging vallen doordat verschillende beveiligingsdisciplines elkaar verantwoordelijk houden voor bepaalde beveiligingsmaatregelen.
Dit betekent overigens niet dat informatiebeveiliging, of onderdelen daarvan, geen aparte aandacht zouden kunnen krijgen. Integendeel, het is bijvoorbeeld heel goed mogelijk om een verbeterproject te starten voor de beveiliging van gevoelige bedrijfsdocumenten. Ook kan het nodig zijn om een specialistisch onderwerp binnen de informatiebeveiliging apart te beschouwen omdat daarvoor specifieke expertise nodig is die speciaal daarop toegespitst is [ORS, 2005]. Het apart aandacht geven aan onderdelen van (informatie)beveiliging kan geen kwaad en is in bepaalde gevallen zelfs gewenst, als men maar niet vergeet dat men met een onderdeel van de beveiliging als geheel bezig is en daarbij bedacht is op mogelijke relaties tussen informatiebeveiliging en andere beveiligingsaspecten.

In het kader van integraal management is een manager verantwoordelijk voor de informatiebeveiliging binnen zijn organisatie(-eenheid). Om zich te laten ondersteunen kan hij in zijn organisatie(-eenheid) één of meer staffunctionarissen aanwijzen die deskundig zijn op dit gebied (zie figuur 4a). Echter, informatiebeveiliging is een integraal onderdeel van (bedrijfs)beveiliging en kan dus gezien worden als een specialisatie binnen (bedrijfs)beveiliging. Het is daarom ook mogelijk informatiebeveiligingsdeskundigen in de organisatie onder te brengen bij een beveiligingsfunctionaris of -groep (zie figuur 4b). Aan de andere kant is informatiebeveiliging ook een onderdeel van informatiemanagement, wat ervoor pleit om informatiebeveiligingsdeskundigen in de organisatie juist onder te brengen bij een informatiemanagementfunctionaris of -groep (zie figuur4c).



Figuur 4: De positionering van de informatiebeveiligingsfunctie (IBF)

Ieder van deze positioneringen heeft voordelen. Zo heeft de positionering zoals in figuur 4a het voordeel dat informatiebeveiliging apart aandacht krijgt en niet gauw een 'ondergeschoven kindje' zal worden. De positionering onder een beveiligingsfunctie, zoals in figuur 4b, leidt daarentegen tot een relatief goede afstemming tussen beveiligingsfunctionarissen over beveiligingsvraagstukken, wat de integratie tussen de verschillende beveiligingsdisciplines ten goede komt. Aan de andere kant leidt een positionering onder een informatiemanagementfunctie, zoals in figuur 4c, juist tot een relatief goede afstemming over de verschillende aspecten van de al dan niet geautomatiseerde informatievoorziening.
De keuze tussen deze alternatieven lijkt een beetje lood om oud ijzer, maar toch zijn er wel richtlijnen te geven:

- Als er voorschrijvende regels zijn waarin de keuze al vastgelegd is, is er feitelijk geen keuze. Dit geldt bijvoorbeeld voor organisaties van de Rijksdienst die de verschillende beveiligingsdisciplines bij een beveiligingsambtenaar (BVA) moeten onderbrengen [PSV, 2005].
- Als de integraal manager een voorkeur voor een bepaalde positionering heeft, is die positionering te prefereren. Uiteindelijk is het doel van de ondersteunende deskundigen om de manager te ondersteunen, dus als de manager een voorkeur heeft die goed aansluit bij zijn belevingswereld, dan geeft dat de doorslag.
- Als er geen voorschrijvende regels gelden en de manager bovendien geen voorkeur heeft, heeft een positionering van de informatiebeveiligingsfunctie losstaand (figuur 4a) of onder de informatiemanagementfunctie (figuur 4c) de voorkeur. De keuze voor een losstaande positionering heeft met name de voorkeur als informatiebeveiliging een hoge urgentie heeft binnen de organisatie(-eenheid) van de manager. Dit kan bijvoorbeeld het geval zijn als informatiebeveiliging een belangrijk aspect van het primaire proces is, zoals een opsporingsdienst, of als informatiebeveiliging het primaire proces of product is, zoals een organisatie die beveiligingsdiensten levert. In de meeste andere gevallen heeft een positionering onder de informatiemanagementfunctie de voorkeur.

Integratie van informatiebeveiliging op de werkvloer

In het kader van integraal management zijn de verantwoordelijkheid voor informatiebeveiliging, alsmede de sturing ervan, geïntegreerd met andere aspecten van de bedrijfsvoering. De operationele invulling van informatiebeveiliging is daarmee echter nog onvoldoende geregeld. Deze invulling speelt zich af bij de grootste groep mensen in de organisatie, de medewerkers. Hun betrokkenheid is tweeledig: enerzijds veroorzaken zij door bewuste en onbewuste fouten (meestal te goeder trouw) een groot deel van de incidenten; anderzijds zijn zij degenen die het merendeel van de beveiligingsmaatregelen uitvoeren. Het is dus van groot belang om de medewerkers voldoende te motiveren voor informatiebeveiliging. Ook hierbij speelt integratie van informatiebeveiliging een rol.
De initiële motivatie van medewerkers voor informatiebeveiliging is in het algemeen in orde, maar kan makkelijk negatief beïnvloed worden. Om de motivatie op peil te houden is het nodig dat de medewerkers de maatregelen voor informatiebeveiliging zinnig vinden, en dat ze bovendien de implementatie van de maatregelen redelijk vinden.
De medewerkers vinden de maatregelen voor informatiebeveiliging pas zinnig als aan een aantal randvoorwaarden voldaan is, te weten [Noord, 2001; Spruit, 2004]:

1. De bedrijfsprocessen en procedures, alsmede de bijbehorende taken, verantwoordelijkheden en bevoegdheden, zijn goed ingevuld. Dit leidt ertoe dat de medewerkers voldoende vertrouwen hebben in de aanpak van het management.
2. De medewerkers zijn ervan overtuigd dat de door het management en de specialisten opgelegde beveiligingsmaatregelen redelijk zijn, oftewel proportioneel, eerlijk en effectief.
3. De medewerkers zijn zelf, of via vertegenwoordigers, betrokken (geweest) bij het selecteren en implementeren van de beveiligingsmaatregelen.

Als deze randvoorwaarden gerealiseerd zijn, zijn de maatregelen weliswaar acceptabel voor de medewerkers, maar dan is het bovendien nog nodig dat ook de implementatie van de maatregelen acceptabel is. Daarvoor moeten naast de bovengenoemde randvoorwaarden tevens de onderstaande randvoorwaarden gerealiseerd zijn:

4. De medewerkers ervaren dat de maatregelen de onvoorwaardelijke steun van het management hebben, onder meer doordat het management zelf het goede voorbeeld geeft.
5. Het vanuit beveiligingsoptiek gewenste gedrag wordt beloond, en ongewenst gedrag wordt niet beloond. Dus geen pluim voor medewerkers die wel veel ‘productie draaien’, maar zich niet aan de beveiligingsmaatregelen houden.
6. De voor beveiligingsmaatregelen benodigde handelingen passen in de cultuur en de gewoonten van de organisatie. De beveiligingsmaatregelen moeten daarvoor zodanig ingericht zijn dat de medewerkers zich in het kader van informatiebeveiliging niet heel anders hoeven te gedragen dan ze voor de andere processen gewend zijn.
7. De voor beveiligingsmaatregelen benodigde handelingen zijn zo veel mogelijk geïntegreerd in de rest van het werk. Zo kunnen bijvoorbeeld toegangsbeperkende maatregelen gecombineerd worden met overwerkregistratie en declaratie.

8. De beveiligingsmaatregelen vereisen geen handelingen die al eerder uitgevoerd zijn voor andere doeleinden. Dus niet voor de zoveelste keer de bedrijfsprocessen in kaart brengen omdat het deze keer nodig is voor de risicoanalyse ten behoeve van informatiebeveiliging.

De genoemde randvoorwaarden hebben enerzijds betrekking op de invulling van integraal management en top-down sturing van informatiebeveiliging (nr. 1-5), en anderzijds op de integratie van informatiebeveiliging op operationeel niveau (nr. 6-8). Zolang de medewerkers door het realiseren van de randvoorwaarden de maatregelen voor informatiebeveiliging zinnig vinden, en bovendien de implementatie ervan redelijk vinden, blijft de motivatie van de medewerkers voor informatiebeveiliging in het algemeen op peil. Als echter aan één van de bovenstaande randvoorwaarden niet (meer) voldaan wordt, zal de motivatie voor informatiebeveiliging bij veel medewerkers al sterk afnemen. Als aan meerdere voorwaarden niet voldaan wordt, blijft er van de motivatie weinig over. Integratie, ook op operationeel niveau, is dus cruciaal voor de motivatie van de medewerkers voor informatiebeveiliging, en daarmee voor het welslagen van informatiebeveiliging in de organisatie.

Wanneer de integratie van informatiebeveiliging in de organisatie goed doorgevoerd is, is de omgeving dat veelal (nog) niet. Dit uit zich in allerlei verschillende verzoeken voor informatie in het kader van inspectie, controle of audit. Veelal gaat het om vergelijkbare of zelfs dezelfde informatie. Als deze externe invloeden eerst in kaart gebracht en vervolgens zo veel mogelijk geharmoniseerd worden, hoeven de medewerkers niet steeds opnieuw dezelfde informatie op te zoeken en soortgelijke interviews af te geven. Hierdoor worden medewerkers ontlast en hebben ze het idee dat de overblijvende informatieverzoeken redelijk zijn.

Ten slotte

Het topmanagement en de andere managers van een organisatie zijn verantwoordelijk voor het beheersen van de bedrijfsrisico's. Het gaat hierbij zowel om de risico's met betrekking tot de informatievoorziening als om de risico's met betrekking tot andere aspecten van de bedrijfsvoering. Het beheersen van al deze risico's is gebaat bij een geïntegreerde aanpak. Temeer omdat het dan mogelijk is risico's met betrekking tot verschillende bedrijfsaspecten in onderlinge samenhang te beschouwen en op basis daarvan prioriteiten te stellen. Onder de vlag van integraal management is een dergelijke geïntegreerde aanpak ook volstrekt normaal.
Veel managers realiseren zich onvoldoende wat het fenomeen integraal management voor hen betekent: zij zijn niet alleen verantwoordelijk voor de productie of dienstverlening, maar ook voor de daarvoor benodigde ondersteunende zaken, inclusief informatiebeveiliging. Veel tijd hoeft dat de managers niet te kosten, maar enige inzet is wel noodzakelijk. De belangrijkste actie van een manager is het aanwijzen of aantrekken van één of meer capabele deskundigen die niet alleen advies geven, maar de manager ook werk op het gebied van informatiebeveiliging uit handen nemen. Deze deskundigen hebben bovendien tot taak om met gevraagd, maar zeker ook met ongevraagd advies de risicoperceptie van hun manager te verbeteren, zodat diens aandacht voor informatiebeveiliging toeneemt.
De organisatorische positionering van de deskundigen die de manager op het terrein van informatiebeveiliging ondersteunen, kent een aantal mogelijkheden. Voor het maken van een

weloverwogen keuze spelen met name de voorkeur van de manager en eventuele regelgeving een doorslaggevende rol.
Naast de invulling van integraal management en top-down sturing van informatiebeveiliging moet er binnen de organisatie ook voldoende draagvlak voor informatiebeveiliging zijn. Hiervoor is verregaande integratie van informatiebeveiliging in de bedrijfsprocessen nodig, ook op operationeel niveau. Bovendien moeten externe invloeden zoveel mogelijk in kaart gebracht en geharmoniseerd worden.
Het op peil brengen van informatiebeveiliging mag overigens niet beschouwd worden als een eenmalige inspanning. Sterker nog: de voornaamste inspanning om een goede informatiebeveiliging te krijgen en te houden, wordt geleverd nadat de beveiligingsmaatregelen geïmplementeerd zijn. Het is dus zaak om informatiebeveiliging continu onder de aandacht te houden. Daarnaast veranderen organisaties en hun omgeving voortdurend. Daarom moeten de verschillende aspecten van de bedrijfsvoering, waaronder informatiebeveiliging, regelmatig geëvalueerd en zo nodig worden aangepast. Voor elke aanpassing in de informatiebeveiliging moet weer voldoende draagvlak bestaan. En ook hierbij moet de integratie van informatiebeveiliging voorop staan.

Literatuur

[BuJa, 1999] H. Buurma & C.W.J.M. Jacobs, *Integraal management in overheid en publieke sector*, Lemma, Utrecht, 1999.

[Goor, 2002] A.D. van Goor, *Informatiebeveiliging: 'grenzeloos'*, Informatiebeveiliging, nr. 5, 2002, pag. 18-21.

[Noord, 2001] F. van Noord, *Beveiliging: gepland veranderen van gedrag*, Informatiebeveiliging, nr. 4, 2001, pag. 20-23.

[ORS, 2005] P. Overbeek, E. Roos Lindgreen & M. Spruit, *Informatiebeveiliging onder controle*, Pearson, Amsterdam, 2005.

[OvRo, 2002] P. Overbeek & E. Roos Lindgreen, *Informatiebeveiliging: wat mag u ervan verwachten?*, Management & Informatie, nr. 1, 2002, pag. 50-56.

[PSV, 2005] S. Planken, L. Schurink & W. Vrouwenvelder, *Integratie van beveiliging bij het ministerie van Verkeer en Waterstaat*, Informatiebeveiliging, nr. 6, 2005, pag. 11-15.

[SpGr, 2004] M.E.M. Spruit & M. de Graaf, *Een twee-sporenaanpak voor informatiebeveiliging*, Management Executive, nr. 1, 2004, pag. 34-37.

[Spruit, 2004] M.E.M. Spruit, *Informatiebeveiliging en bewustzijn*, Informatiebeveiliging Jaarboek 2004/2005, Ten Hagen en Stam, Den Haag, 2004, pag. 95-101.