GvIB Expert Brief – Juli 2006
ISSN 1872-4876, Jaargang 2 – Nr. 2

Juli 2006

Het inrichten van een beveiligingsorganisatie. Welke factoren zijn van invloed?

Henk Bel

Bart Bokhorst

Ed Bronner

Ben Elsinga

Theo Engelsma

Jule Hintzbergen

Andre Jannink

Andre Koot

Ernst Oud

Lex Pels

Thom Schiltmans

Frank van Vonderen

Paul Wielaard

De aanleiding van deze expertbrief is de groeiende behoefte aan meer inzicht in de optimale inrichting van de organisatie van de beveiligingsfunctie. Diverse publicaties, zoals ISO 17799 en Cobit, geven goed aan wat er geregeld moet worden ten aanzien van informatiebeveiliging. Echter wie moet wat regelen en hoe organiseer je dat het beste? Welk deel van informatiebeveiliging is een verantwoordelijkheid van de business en wat is de zorg van de ICT afdeling? Het in de praktijk effectief realiseren van informatiebeveiliging en het kiezen van de meest geschikte organisatievorm is niet triviaal. Deze expertgroep heeft zich gebogen over de vraag welke factoren van invloed zijn op de inrichting van een beveiligingsorganisatie en op welke manier.

http://www.gvib.nl/
✉ expertbrief@gvib.nl

2

INLEIDING EN SITUATIE SCHETS

Informatiebeveiliging wordt de laatste jaren bij steeds meer organisaties onderkend als relevant aspect voor de bedrijfsvoering. Met name de opkomst van standaarden en nieuwe wet- en regelgeving ten aanzien van compliance, zoals de Sarbanes Oxley wet, heeft sterk aan dit bewustzijn bijgedragen. Naast IT managers, zijn business managers zich meer bewust dat een goede beveiliging belangrijk is voor de betrouwbaarheid van business processen. Informatiebeveiliging wordt mede daardoor in toenemende mate gezien als een integraal onderdeel van business risk management en als belangrijk kwaliteitsaspect. Uiteindelijk zijn risico's voor de bedrijfsvoering dan ook de werkelijke rechtvaardiging voor investeringen in informatiebeveiliging.

Dit bewustzijn op zich is niet voldoende om ook daadwerkelijk een integrale invulling aan informatiebeveiliging te geven. Informatiebeveiliging blijft voor velen nog steeds een lastig onderwerp. Vaak wordt de 'hete kastanje' doorgespeeld aan een verantwoordelijke binnen een afdeling zonder daaraan het juiste mandaat te koppelen. Daarmee is dit lastige aspect 'belegd'. Gevolg is dat het probleem dan niet ligt bij de echte verantwoordelijke, waardoor effectief handelen en goede besluitvorming gehinderd kunnen worden.

In de praktijk is de informatiebeveiligingsfunctie (IB-functie) verschillend belegd, waarbij de huidige situatie vaak sterk is ingegeven door historische ontwikkelingen en bedrijfscultuur. Veel organisaties hebben een Corporate Information Security Officer (CISO) aangesteld. Taken en verantwoordelijkheden verschillen echter sterk. Een CISO als 'veiligheidsgeweten' van de business organisatie zal accenten leggen op beleid en risicoanalyses. Een CISO in een voornamelijk technische omgeving zal meer focus leggen op het realiseren van betrouwbare technische oplossingen.
Duidelijk is dat door het aanstellen van een verantwoordelijke CISO niet automatisch alle specifieke verantwoordelijkheden en taken van de IB-functie integraal in de organisatie zijn ingebed.
Bij de verdere invulling van informatiebeveiliging komen diverse vragen op, waaronder: Zijn informatiebeveiligingstaken een specialisme of zijn het primaire deeltaken die eenvoudig door medewerkers in reguliere processen meegenomen kunnen worden? Betreft het fulltime functies of parttime rollen en kunnen deze activiteiten worden ingehuurd of uitbesteed?

Een logische gevolgtrekking van het feit, dat informatiebeveiliging primair een business verantwoordelijkheid is, zou moeten zijn dat de IB-functie ook rapporteert aan de business. In de praktijk blijkt dit vaak niet het geval en dat is goed te begrijpen vanuit historisch perspectief. Dit leidt dan ook in veel gevallen tot een aantal knelpunten.

In dit artikel wordt gesproken over de organisatie van informatiebeveiliging. Hiermee wordt bedoeld alles wat met de informatieverwerking in een organisatie te maken heeft. Veiligheid van personen en andere safety aspecten vallen buiten de scope.
Deze expertbrief belicht het inrichten van de beveiligingsorganisatie en de plaats van de beveiligingsfuncties en rollen in een organisatie. Niet bedoeld wordt het proces van het organiseren van informatiebeveiliging of het verbeterproces op basis van bijvoorbeeld de Demming circle.
In deze expertbrief zullen voornamelijk de invloedsfactoren beschreven worden. Hoe deze factoren precies invloed hebben op de inrichting van de IB-functie, zal in een vervolg expertbrief worden beschreven.

DE ONDERZOEKSVRAGEN

Een informatiebeveiligingsorganisatie kan op veel verschillende manieren worden ingericht, variërend van een enkele CISO ondersteund door een aantal IT medewerkers met een informatiebeveiligingsrol als bijtaak tot een centraal team van specialisten die hun zorgtaken hebben door de gehele bedrijfsorganisatie. Informatiebeveiligingsorganisaties zijn soms sterk op techniek en infrastructuur gericht, terwijl andere zich nadrukkelijk met business risico management bezig houden.
De vraag is welke organisatievorm, rolverdeling en positie van de IB-functie in de organisatie het meest geschikt is voor het effectief inrichten van informatiebeveiliging en of dit universeel is of specifiek voor bijvoorbeeld een bepaalde bedrijfstak of bedrijfsomvang.

Op basis van de bovenstaande uitgangssituatie heeft de expertgroep zich gebogen over de volgende vraagstelling:

- Welke in- en externe factoren zijn van invloed op het inrichten van de IB-functie?
- Op welke wijze zijn deze factoren van invloed op de inrichting?
- Wat zijn de knelpunten en welke trends zijn te onderkennen?

Vragen die hiermee samenhangen zijn:

- Hoe krijg je informatiebeveiliging nu echt goed geregeld? Met het op papier formaliseren van de IB-functie heb je nog niet automatisch het juiste draagvlak.
- Is het mogelijk een ‘receptuur’ te ontwikkelen die op basis van een aantal parameters de meest optimale organisatie van de IB-functie aangeeft?

Een werkgroep als vervolg op een andere expertbrief heeft zich eerder al bezig gehouden met het beschrijven van informatiebeveiligingsfuncties. Er bestaat een risico van overlap met de activiteiten van deze expertgroep, aangezien deze werkgroep zich heeft gerealiseerd dat het beschrijven van functies niet gaat zonder daarbij een organisatie model voor ogen te hebben. Om het wiel niet opnieuw uit te hoeven vinden zal hieronder ook voortgebouwd worden op een deel van de voorlopige resultaten van deze werkgroep.

Naast in- en externe factoren die de inrichting van de IB-functie beïnvloeden is het ook van belang om de knelpunten in de huidige situatie in veel organisaties inzichtelijk te hebben. De belangrijkste knelpunten hebben vooral te maken met de huidige positie van de IB-functie in organisaties. Dit zal hieronder eerst worden toegelicht.

HISTORISCH PERSPECTIEF EN KNELPUNTEN

Om deze knelpunten inzichtelijk te krijgen is van belang te weten hoe deze ontstaan zijn. Daarom zal de ontwikkeling van de rol van de CISO als aanvoerder van de IB-functie kort worden beschreven.

De ontwikkeling van de rol van de CISO

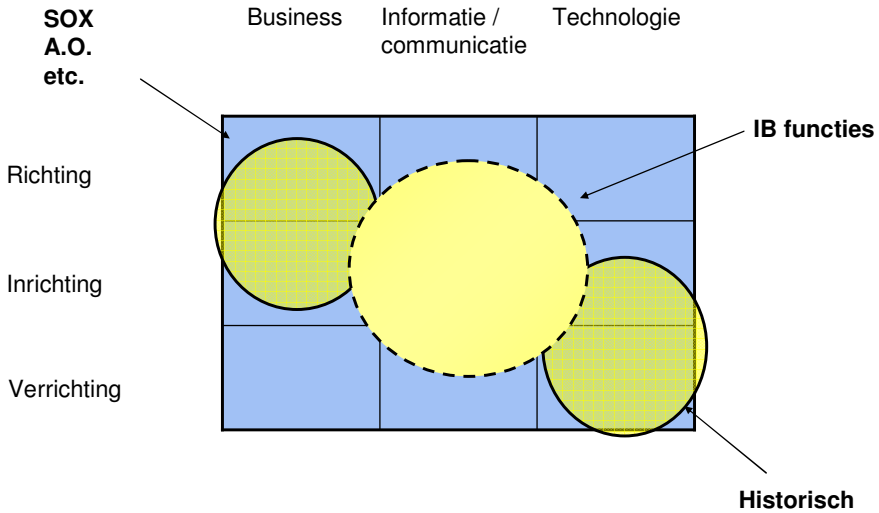
De rol van de CISO heeft in de loop van de tijd een sterke verandering ondergaan.
De klassieke informatiebeveiligingsmanager kwam voornamelijk voor in defensieomgevingen en andere hoogrisico omgevingen zoals bij banken en telecommunicatiebedrijven. In enkele organisaties met een hoog beveiligingsbewustzijn werd informatiebeveiliging al vroeg breed aangepakt. In de meeste organisaties echter kwam door

het toenemend aantal externe koppelingen via publieke netwerken de focus sterk te liggen op het bewaken van de grenzen door middel van firewalls en toegangsdiensten. Of te wel het regelen van technische kwesties om de vijand buiten te houden. Een bijna zuiver IT probleem dus. Ook toen de aandacht van de CISO meer verschoof naar interne aangelegenheden bleef de rol van de CISO een hoog technisch gehalte hebben.
De CISO sprak niet de taal van de business en het communiceren in termen van angst en onderzekerheden werd door business managers niet gewaardeerd. Pas de laatste jaren is door allerlei incidenten en met de opkomst van standaarden als ISO 17799 en compliance-eisen van uit wet- en regelgeving het belang van informatiebeveiliging voor de business managers duidelijker geworden. De CISO begon meer en meer te spreken in terminologie van de business, zoals Return On Investment, business continuïteit en betrouwbaarheid van de informatievoorziening. Informatiebeveiliging als onderdeel van business risk management. De verbreding van de aandachtsgebieden van security management leidde ook tot meer specialisatie en het onderkennen van verschillende informatiebeveiligingstaken op verschillende plaatsen in de organisatie.

De actuele positie van de CISO en knelpunten

Door de sterk technische focus uit het verleden rapporteren CISO's in veel organisaties nog steeds binnen de IT afdeling aan de IT manager of CIO. Veel organisaties realiseren zich dat de IB-functie nog te ver af staat van de business en worstelen met de vraag hoe informatiebeveiliging het beste geïntegreerd en georganiseerd kan worden.

Onderstaande figuur geeft een model weer om naar de positie van de IB-functie in de organisatie te kijken. Gebaseerd op een model van Rik Maes.



Op de verticale as zijn de bekende niveaus strategisch, tactisch en operationeel te herkennen, op de horizontale as is tussen de business en technologie kolommen een informatie en communicatie kolom opgenomen die informatie en communicatie als verbindende elementen tussen business en techniek weergeeft.

Dit figuur visualiseert nog eens dat op gebied van informatiebeveiliging behoefte is aan overbrugging van de kloof tussen business en technologie, maar ook dat informatiebeveiliging meer dan in het verleden onderdeel moet worden van strategische en tactische processen.

Knelpunten van de huidige situatie
Het feit dat de CISO nog vaak rapporteert aan de ICT manager of de CIO veroorzaakt een aantal knelpunten die bij de inrichting van de IB-functie geadresseerd moeten worden:

- Informatiebeveiliging wordt onvoldoende beleefd als een expliciete verantwoordelijkheid van het business management en als integraal onderdeel van het inrichten van business processen. Daarmee blijft informatiebeveiliging gezien worden als een ICT probleem met een grote kans op onvoldoende business alignment. Het risico bestaat hierbij dat de CISO als 'blaffende hond' veilig werken probeert te bewerkstelligen zonder voldoende mandaat;
- Informatiebeveiliging wordt nog te vaak ervaren als een hinderlijk en defensief 'blok aan het been' en niet als een kwaliteitsaspect dat kan bijdragen aan een positief bedrijfsimago. Bij de toenemende integratie van business processen en IT systemen tussen verschillende organisaties is informatiebeveiliging echter een belangrijke bouwsteen bij het creëren van vertrouwen tussen organisaties. Een potentiële business enabler!;
- De IT afdeling moet een oordeel vellen over de kwaliteit van zijn eigen IT systemen en infrastructuur. Als projecten onder druk komen te staan door gebrek aan mensen of middelen (tijd) kan informatiebeveiliging gemakkelijk ondergeschikt worden gemaakt aan het beschikbaar komen van functionaliteit zonder dat dit zichtbaar wordt;
- Er komt onvoldoende budget beschikbaar voor informatiebeveiliging;
- Het te gemakkelijk delegeren van informatiebeveiliging gaat ten koste van het beveiligingsbewustzijn van business medewerkers.

Een optimale integratie en inrichting van de IB-functie in de business helpt deze knelpunten op te lossen. De vraag is wat dan de meest optimale inrichting is.
Hieronder worden de belangrijkste interne en externe factoren belicht die deze inrichting beïnvloeden.

EXTERNE FACTOREN

Organisaties opereren in een extern krachtenveld met veel verschillende belanghebbenden en toenemende dreigingen. De belangen van de samenleving of van bepaalde belangengroepen worden veelal vastgelegd in standaarden of wet- en regelgeving.
Vaak staan organisaties niet langer op zichzelf, maar vormen ze onderdeel van verschillende samenwerkingsverbanden die hun business en IT processen gekoppeld hebben. Business process outsourcing en IT outsourcing bijvoorbeeld vragen om heldere interfaces en afspraken tussen organisaties.

De belangrijkste onderkende externe factoren zijn:

- Toenemende dreigingen
- Verplichtingen
- Ketenintegratie

Toenemende dreigingen

Hacking activiteiten op het Internet worden steeds vaker uitgevoerd door criminele organisaties. Organisaties waar 'iets te halen is' zijn het doelwit. Naar mate een organisatie gevoeliger is voor dit soort dreigingen zal zij haar IB-functie zwaarder moeten inrichten op gebied van preventie, detectie, monitoring en incident respons.

Verplichtingen

Voldoen aan wet- en regelgeving is een must om als organisatie te mogen opereren in het externe krachtenveld. Deze wet- en regelgeving is vaak geformuleerd in de 'taal' van de belanghebbenden en moet binnen een organisatie worden vertaald naar de consequenties voor informatiebeveiliging, zowel op tactisch als operationeel niveau.
Voorbeelden hiervan zijn SOX, Basel II, ROB, HIPAA en de WBP.
Afhankelijk van de markt waarin een organisatie opereert, zijn bepaalde compliance-eisen van toepassing. Dit vertaalt zich in een organisatie naar implementatie van specifieke maatregelen en een behoefte aan controle en rapportage op specifieke gebieden. De invloed van compliance op de inrichting van de IB-functie is hieronder deels aangegeven, maar moet zeker nog nader worden onderzocht en uitgewerkt.

Ketenintegratie

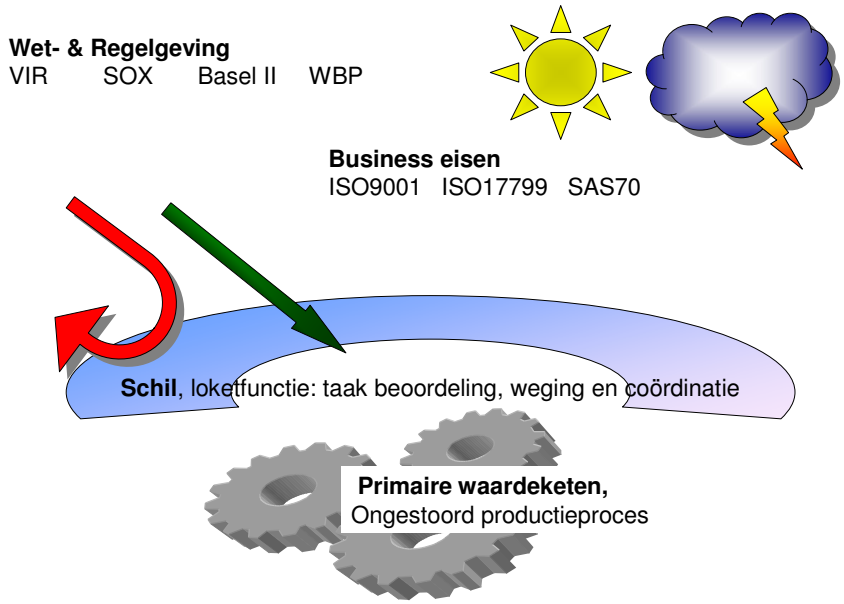
De trend tot verdere ketenintegratie tussen marktpartijen leidt tot een behoefte aan goede afspraken en maatregelen, zowel op business als op technisch niveau. De zekerheid over de betrouwbaarheid van informatie-uitwisseling en de vertrouwelijkheid van de communicatie wordt bepaald door het geheel aan afspraken en maatregelen. Afhankelijk van de situatie, de risico's en het onderlinge vertrouwen, kan het accent liggen op procedurele en contractuele maatregelen of op technische maatregelen. Om risico's kosten effectief en efficiënt af te dekken wordt vaak een combinatie van procedurele, contractuele en technische maatregelen genomen. Daarom is het gewenst dat de IB-functie een brede oriëntatie heeft. Enerzijds moet zij de business kunnen ondersteunen met adviezen over een goede balans tussen verschillende maatregelen. Anderzijds zal zij met externe partijen af moeten stemmen wat de mogelijkheden zijn en welke oplossingen voor de betrokken partijen het meest passend zijn. Soms is er vrijheid bilaterale afspraken te maken, maar vaak bestaat er behoefte aan branch brede, meer of minder verplichte, richtlijnen.

De invloed van compliance op de IB-organisatie.

Meestal zijn er vanuit verschillende invalshoeken compliance-eisen waaraan een organisatie moet voldoen, die ieder een bepaalde rapportage vereisen, maar die in wezen een groot aantal overlappende eisen kennen.
Organisatieonderdelen kunnen daardoor in een situatie komen waarbij ze verschillende rapportages moeten opleveren over veel vergelijkbare aspecten. Er ontstaat dan behoefte aan het opzetten van een gemeenschappelijk rapportage systeem, waaruit voor de verschillende compliance-normen afzonderlijke rapportages te halen zijn. Daarmee kan worden voorkomen dat de operationele organisatie meer met rapporteren bezig is dan met het productieproces zelf. Belangrijk is dat het productieproces in de primaire waardeketen van een organisatie zoveel mogelijk ongestoord kan verlopen.

Het creëren van een gemeenschappelijk rapportage systeem vraagt om coördinatie door een 'change organisatie' die alle invloeden van buitenaf beoordeelt, filtert en vertaalt naar een gemeenschappelijke set van eisen waarbij eenduidige terminologie wordt gebruikt.
Hierdoor zal er meer behoefte zijn aan integratie van informatiebeveiliging met andere bedrijfsprocessen, zoals enterprice risk management (ERM), operational risk management (ORM) en business continuity management (BCM). Gesteld kan worden dat door compliance-eisen de organisatie van informatiebeveiliging sterker moet samenwerken of integreren met organisatieonderdelen die zich met andere aspecten van risico management bezig houden.
De vraag hoe dit optimaal ingericht kan worden zal in een vervolg-expertbrief worden beantwoord.

Onderstaande figuur geeft de behoefte aan een filterende en coördinerende schil om de operationele processen nog eens beeldend weer.



INTERNE FACTOREN

Een belangrijke constatering van de expertgroep is dat in de discussie veel meer interne dan externe factoren geïdentificeerd werden.
Zonder al direct helder te hebben hoe deze interne factoren de inrichting van de security organisatie beïnvloeden, is de expertgroep van mening dat de volgende factoren van invloed zijn op de optimale inrichting:

- Drivers en draagvlak
- Volwassenheid van de organisatie
- Visie
- Cultuur
- Scope en definitie van IB functies
- Omvang organisatie
- Geografische spreiding

Drivers en draagvlak
Om informatiebeveiliging succesvol te integreren in de processen van een organisatie is het belangrijk op een natuurlijke manier aan te sluiten bij bestaande en geaccepteerde processen in de organisatie. Voorbeelden zijn risico management of kwaliteitsmanagement. Indien deze processen als belangrijk worden gezien, krijgt informatiebeveiliging bijna automatisch een positieve profilering en wordt het verkrijgen van commitment eenvoudiger.
Welke processen als belangrijk worden erkend is vaak afhankelijk van de belangen van een of meerdere belanghebbenden, ook wel stakeholders genoemd. Door in de communicatie aan te sluiten bij de terminologie van de stakeholders zullen ze sneller het belang herkennen en dit ondersteunen. Middelen en budget komen dan makkelijker ter beschikking. Het is immers in lijn met het eigen belang. Er kunnen meerdere stakeholders zijn en hun belangen kunnen veranderen door de tijd heen. Gebruik van het juiste momentum kan belangrijk zijn om de organisatie van informatiebeveiliging op een hoger plan te krijgen. Op dit moment kan bijvoorbeeld de noodzaak tot compliance met de Sarbanes Oxley wet een belangrijke hefboom zijn voor verbetering.
Het flexibel kunnen aanpassen aan belangen van stakeholders stelt ook eisen aan de flexibiliteit van mensen. Mensen moeten bij voorkeur breed georiënteerd zijn op gebied van informatiebeveiliging en moeten dezelfde boodschap op verschillende manieren kunnen verwoorden. Daarnaast is het gewenst dat ook prioriteiten of zelfs de organisatievorm flexibel aangepast kan worden. Het is overigens niet van zelfsprekend dat medewerkers deze flexibiliteit hebben aangezien veranderingen bedreigend kunnen zijn voor hun eigen positie.

Volwassenheid van de organisatie
Ervaring is nog steeds de beste leermeester. Organisaties zullen moeten ervaren wat wel en wat niet werkt en zullen op basis van een analyse van de oorzaken moeten leren en bijsturen. Dat kost tijd en vraagt geduld. Het is goed om een bepaald ambitieniveau te hebben. Belangrijk daarbij is om tegelijkertijd vast te stellen wat de voorwaarden zijn om dat ambitieniveau te halen. Een stap naar een volgend volwassenheidsniveau kan alleen gezet worden als een voorgaand niveau gerealiseerd is. Als er bijvoorbeeld geen basisniveau van beveiliging gerealiseerd is zullen IB-functionarissen zich voornamelijk bezig houden met incidentele situaties en ‘brandjes blussen’. Structuur en regelmaat aanbrengen blijft belangrijk, maar als ondertussen het gehele gebouw afbrandt is die structuur mogelijk overbodig geworden. Of als risicomanagement in de organisatie onvoldoende is ingericht wordt het lastig om hierop aan te sluiten bij de inrichting van informatiebeveiliging.

‘Kwaliteitstaken’ behoren integraal onderdeel te zijn van de bedrijfsprocessen. Naarmate management, primaire en ondersteunende medewerkers zelf zorgdragen voor de continuïteit en betrouwbaarheid van de informatievoorziening, zullen verbijzonderde informatiebeveiligingsfuncties overbodig worden. Dit impliceert dat elke manager of medewerker weet waarvoor hij of zij zorg moet dragen bij de uitvoering van de taak.
Tevens gaat deze gedachte uit van een voldoende kennisniveau van informatiebeveiliging bij alle medewerkers en voldoende tijd en middelen om de taak optimaal te kunnen uitvoeren. Aangezien dit vaak niet het geval is, blijft er toch behoefte aan IB-functionarissen die op de juiste plaatsen met de juiste kennis adviseren, ondersteunen en waar nodig correct gedrag afdwingen.
De volwassenheid van een organisatie bepaalt mede hoe en in hoeverre je informatiebeveiliging kunt integreren en verbijzonderd moet organiseren.

Visie
Het belang van informatiebeveiliging is afhankelijk van het primaire bedrijfsproces van een organisatie. Bij de meeste organisaties is ICT faciliterend voor de informatieverwerking van primaire processen. Er zijn echter ook organisaties die ICT als product of dienst leveren. Een goede beveiliging kan dan essentieel zijn om überhaupt de diensten te kunnen leveren. In alle gevallen echter hebben organisaties faciliterende ICT en in die zin zijn de belangen vergelijkbaar en onderscheiden ICT leverende organisaties zich niet wezenlijk van andere organisaties. Basis informatiebeveiliging is daarbij noodzaak en wordt doorgaans als defensieve maatregel gezien.
Informatiebeveiliging kan echter ook als offensief middel worden ingezet om een veiligheidsimago te creëren of door beveiligingstechnologie als business enabler te gebruiken. E-business bijvoorbeeld zou niet goed mogelijk zijn zonder adequate informatiebeveiliging.
Het belang van informatiebeveiliging voor het businessproces van een organisatie bepaalt mede de benodigde hoeveelheid IB capaciteit en de plaats van de IB-functie in de organisatie.

Cultuur
Naast bovengenoemde factoren kan de cultuur van een organisatie veel invloed hebben op de inrichting van informatiebeveiliging. Een autocratische of formele management stijl bijvoorbeeld zal snel leiden tot een top-down geleidde beveiligingsorganisatie, terwijl bij een informele organisatie veel bevoegdheden op lager niveau belegd kunnen worden. Waar ligt de macht in de organisatie? Bij de business of bij ICT? Vaak is dit sterk bepaald door historische factoren.
Ook de risicoperceptie van het management is belangrijk. Is de management stijl risicomijdend of juist kansenzoekend?
Informatiebeveiliging brengt technische maatregelen met zich mee, maar blijft in essentie voornamelijk mensenwerk. Een organisatie zal zijn beveiliging grotendeels moeten realiseren met de mensen die er al zijn. Wat is hun houding en hoeveel verantwoordelijkheid kunnen ze aan?
De stijl van zaken doen met andere organisaties zal ook medebepalend zijn. Doet een organisatie zaken op basis van vertrouwen of moet de zekerheid over business transacties worden afgedekt met technische controls en dikke contracten? Hoe meer controle, hoe minder vertrouwen en andersom.
Naar mate er meer behoefte is aan controle zal de IB-functie zwaarder moeten worden ingevuld.

Scope en definitie van IB-functies
De inrichting van informatiebeveiliging vraagt om een goede inventarisatie van alle beveiligingstaken die uitgevoerd moeten worden, variërende van opstellen van beleid tot bijvoorbeeld het zorgvuldig administreren van gebruikers. Beveiligingstaken zitten op meerdere niveaus en raken veel onderdelen in een organisatie. Het is verstandig taken integraal te inventariseren en waar mogelijk toe te kennen aan rollen in de reguliere organisatie.
Een risico is dat taakomschrijvingen, bij een gebrek aan integraal referentiekader voor de organisatie als geheel, te veel worden opgesteld op basis van lokale belangen. De invulling kan dan makkelijk afhankelijk worden van de belangen van de lokale leidinggevende, van datgene waar hij op afgerekend wordt, zijn scope en beperkte middelen. Ruimte voor lokale invulling is echter belangrijk. Hoe meer zelfsturend medewerkers zijn, hoe beter. Wat er

geregeld moet worden kan het beste zo veel mogelijk integraal worden vastgesteld, hoe dit moet worden ingevuld kan lokaal worden bepaald.
In hoeverre integratie van IB in de organisatie uiteindelijk kan leiden tot minder verbijzonderde beveiligingsfuncties is mede afhankelijk van factoren zoals omvang van de organisatie, kennisniveau, efficiency en de visie of informatiebeveiliging een specialistische functie moet zijn of dat beveiligingrollen onderdeel kunnen zijn van generieke functies.

Omvang organisatie
Dat de omvang van een organisatie mede bepalend is voor de inrichting van de IB-functie lijkt voor de hand liggend.
Een belangrijk uitgangspunt is dat er een goede scheiding is tussen uitvoering en controle. In een grote organisatie is dit makkelijker te realiseren dan in een kleine organisatie waar meerdere taken vaak in één persoon verenigd moeten worden
Naar mate een organisatie groeit en de hoeveelheid IB werk toeneemt, zal er vaak ook meer specialistisch werk zijn dat deels geheel binnen een ICT afdeling wordt uitgevoerd. In alle gevallen blijft de eindverantwoordelijkheid bij de business liggen. De business bepaalt de eisen en hoe sterk de controls (maatregelen) moeten zijn terwijl de ICT afdeling grotendeels zelf kan bepalen hoe de controls worden ingericht.
Bij een grote organisatie zal al snel ook een deel van de controle functie binnen de ICT afdeling zelf liggen en zeker daar waar het specialistisch werk betreft. Bij kleine organisaties ligt de verbijzonderde IB verantwoordelijkheid vaak bij één persoon, die direct aan de business zou moeten rapporteren, maar in de praktijk echter nog vaak via CIO of ICT manager rapporteert.
De eindverantwoordelijkheid om risico afwegingen te maken en restrisico's te accepteren blijft echter altijd bij de business.

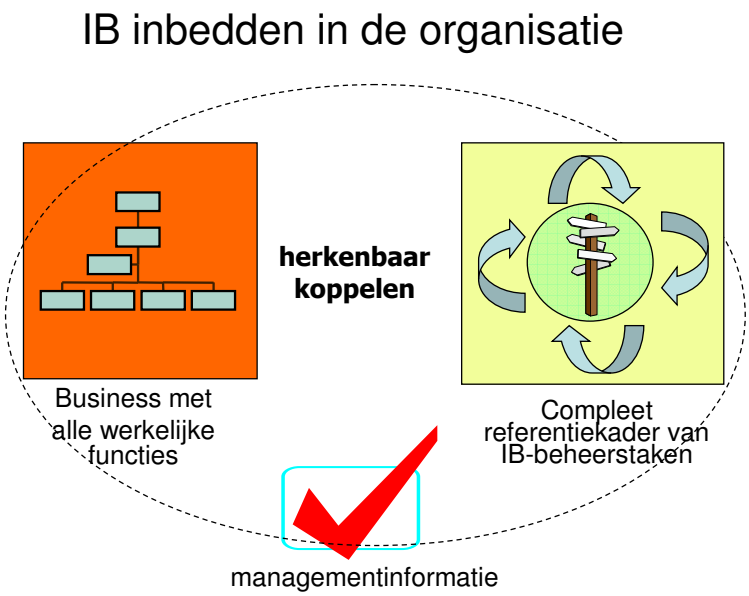
Geografische spreiding
In organisaties met grote geografische scheiding en vergelijkbare processen op verschillende locaties zal er meer behoefte zijn aan standaardisatie. Dan hoeft niet iedereen het wiel opnieuw uit te vinden. In vergelijkbare situaties moeten vergelijkbare maatregelen genomen worden. Standaardisatie kan op verschillende manieren geregeld worden, zowel door maatregelen hiërarchische op te leggen als door het bereiken van consensus tussen organisatieonderdelen. Deze keuze zal sterk bepaald worden cultuur en machtaspecten.
Een sterke geografische scheiding zal sneller leiden tot een decentrale IB-organisatie om daarmee lokale aspecten als taal, cultuur, tijdzoneproblematiek e.d. afdoende het hoofd te kunnen bieden. Goede centrale coördinatie van de IB-functie is daarbij echter essentieel.

Overige aspecten om rekening mee te houden

- Organisatieontwerp is vaak geen kennisgebied van de informatiebeveiliger, met als risico dat iemand 'buiten zijn stiel' gaat werken. Het werkelijk effectief inrichten van een organisatie is vaak lastiger dan het lijkt. Het niet onderkennen van krachtenvelden of persoonlijke belangen kan het optimaal inrichten van een IB-organisatie in de weg staan.
- Als het opzetten van een formele organisatie (even) niet lukt is het opzetten van een informele organisatie een goed alternatief. Houd er rekening mee dat een informele organisatie minder of geen mandaat heeft en dat er dus resultaten geboekt moeten worden op basis van persoonlijke invloed.
- Een virtuele organisatie van deskundigen ter ondersteuning is handig als je niet alle kennis zelf in huis hebt.

- Netwerk- en ketenorganisaties vragen om een samenwerkingsmodel voor informatiebeveiliging omdat een hiërarchische aansturing over verschillende organisaties doorgaans lastiger te realiseren is.
- Een security organisatie mag niet star zijn, maar moet flexibel zijn om te kunnen inspelen op nieuwe dreigingen, technologische ontwikkelingen of nieuwe regelgeving.
- Belangrijk voor het organisatiemodel is dat taken, verantwoordelijkheden en bevoegdheden goed worden afgestemd en helder zijn.
- Een IB-organisatie moet bij voorkeur multidisciplinair worden ingericht met voldoende inbedding in de business, zodat zowel de technische als niet-technische aspecten voldoende aandacht krijgen.

Het belang van een herkenbare koppeling tussen IB-taken en reguliere functies in een organisatie wordt in onderstaande figuur nog eens geïllustreerd.

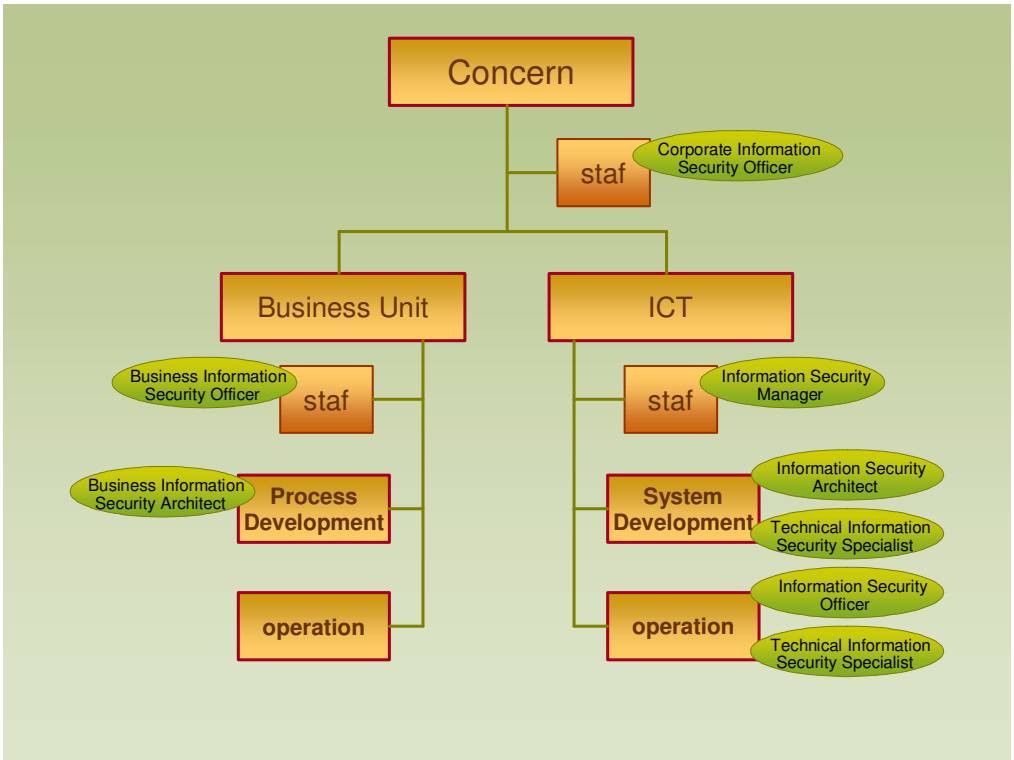


INRICHTINGSASPECTEN

Hierboven zijn factoren genoemd die de inrichting van de IB-functie beïnvloeden. De vraag is welke aspecten van de inrichting zij beïnvloeden en hoe. De te beïnvloeden aspecten zijn onder andere:

- Inbedding en structuur IB in de organisatie
- Omvang van de verbijzonderde IB-functie
- Afbakening rollen met taken, verantwoordelijkheden en bevoegdheden
- Rapportagelijnen
- Positie in de organisatie
- Bevoegdheden IB-organisatie en (lokale) functionarissen
- Scope IB-functie en relatie met aanpalende gebieden, zoals persoonlijke veiligheid, kwaliteitszorg, interne controle, BCM en risicomanagement.

Als referentiemodel voor de inrichting van een IB-organisatie wordt in dit artikel gerefereerd aan een voorlopig model zoals opgesteld door de GVIB/PI-werkgroep die zich bezig houdt met functies in de informatiebeveiliging.



De functies in dit model gelden voor grote en complexe organisaties. Voor kleinere organisaties is door de werkgroep aangegeven hoe functies samengevoegd kunnen worden. Verder zijn de relaties met verwante en/of overlappende functies in kaart gebracht. Voor meer details verwijzen wij naar de hierover nog uit te brengen publicatie.

Hoewel de exacte invloed van de hierboven geïdentificeerde invloedsfactoren nog niet door de expertgroep zijn vastgesteld, zijn er wel alvast een aantal factoren te onderkennen die leiden tot een meer formele of informele organisatie.

Formele organisatie	Informele organisatie
Bureaucratie	Dynamische organisatie
Autocratisch management	Decentraal management
Grote organisatie met geografische spreiding	Kleine organisatie
Risicomijdend management	Kanszoekend management
Accent op verbintenissen en controle	Accent op binding en vertrouwen
Volwassen organisatie (repeatable process)	Onvolwassen organisatie (heroes)

Volledigheid

Bij het inrichten van een organisatie is het belangrijk zo compleet mogelijk te zijn en met alle belangrijke factoren rekening te houden. Om dit goed in kaart te brengen is het van belang om:

- Goed te definiëren wat met informatiebeveiliging bedoeld wordt, welke beheersdoelen daar bij horen en wat in scope is.
- Helder te maken wat de samenhang is met andere begrippen, zoals kwaliteit, risicomanagement of compliance.
- Aan te sluiten bij de taal van de business
- Rekening te houden met externe stakeholders
- Een goede balans te vinden tussen vraag en aanbod (wat is nodig, wat is mogelijk)
- Communicatie tussen vraag en aanbod op WAT niveau te houden (niet hoe)
- Tekortkomingen bij het vastellen van het WAT niveau te voorkomen door gebruik te maken van best practices en standaarden
- Te zorgen voor volledigheid bij toewijzing van alle IB aspecten aan verantwoordelijken
- Verantwoordelijkheden toe te wijzen aan de eigenaar van het meest stabiele element in een organisatie (proces, organisatie, afdeling, functies), waardoor veranderingen in de organisatie zo min mogelijk invloed hebben op de IB-functie.
- Bepalen van een praktisch aggregatieniveau van eisen op het WAT niveau

CONCLUSIES EN VERVOLG

De expertgroep is er voor een groot deel in geslaagd antwoorden te vinden op de gestelde vragen.
De belangrijkste invloedsfactoren zijn geïdentificeerd en deels toegelicht. Gedeeltelijk is aangegeven op welke aspecten van de inrichting de verschillende factoren invloed hebben. Tevens is er een belangrijke trend geïdentificeerd dat organisaties in de ‘netwerk wereld’ steeds vaker onderdeel worden van een totale keten of hun activiteiten deels ‘outsourcen’. Hierbij verliezen organisaties in een bepaalde mate hun autonomie en is er noodzaak tot afstemming en samenwerking met andere partijen in de keten. Dit vraagt om flexibiliteit van de IB-functie.

De expertgroep heeft besloten een tweede sessie te wijden aan het nog onbeantwoorde deel van de vraagstelling, namelijk in welke richting en in welke mate de invloedsfactoren effect hebben op de inrichtingsaspecten.
Ideaal zou zijn om een model (‘receptuur’) te ontwikkelen waarbij op basis van een generiek geldend referentiekader en gedefinieerde parameters automatisch de optimale organisatievorm gepresenteerd zou kunnen worden.

Hierbij is het van belang om over zoveel mogelijk ervaringsgegevens te beschikken om op basis daarvan verbanden te kunnen ontdekken. Om de volgende sessie optimaal in te gaan vraagt de expertgroep om commentaar op dit artikel en om zoveel mogelijk input ten aanzien van geconstateerde verbanden. U kunt uw reacties sturen naar expertbrief@gvib.nl. Ook indien u deze expertbrief heeft kunnen waarderen stellen wij een e-mailtje op prijs!

14

LITERATUURLIJST

Voor het tot stand brengen van deze expertbrief heeft de werkgroep de volgende literatuur geraadpleegd:

Fred van Noord, *Top-down en bottom-up gaan hand in hand - BS7799 werkend krijgen in organisaties*

Gartner, *The evolving role of the Chief Information Security Officer*

Jentjes en van Dijk, *Groeien naar een integrale beveiliging bij RWS RIKZ*

Ton Thoma, *Waarborgen beveiliging bij uitbesteding*

Fred van Tol, *Project Informatiebeveiliging Defensie Interservice Commando*

Bart Bokhorst, *Functie in de informatiebeveiliging, deel 1*

Andre Koot, *Enhanced Security Management - Informatiebeveiliging verankerd in een dynamische Business Alignment theorie*

Rik Maes, *Reconsidering Information Management Through a Generic Framework*

A Hofman, *Adaptive Security: flexibele beveiliging in de netwerkeconomie*

A Jannink, *Kan AOR en Besfuta u helpen?*

GvIB, *Raamwerk AOR23 mrt'06 version GvIB*

APPENDIX GEBRUIKTE LICENTIEVORM

De expertbrief wordt gepubliceerd onder de volgende licentie:
http://creativecommons.org/licenses/by-sa/2.5/

Deze pagina ziet er op het moment van schrijven als volgt uit:

creative commons

COMMONS DEED

Naamsvermelding-GelijkDelen 2.5

De gebruiker mag:

- het werk kopiëren, verspreiden, tonen en op- en uitvoeren
- afgeleide werken maken
- gebruik maken van het werk voor commerciële doeleinden

Onder de volgende voorwaarden:

BY: **Naamsvermelding**. De gebruiker dient de naam of andere aanduiding van de maker te vermelden.

Gelijk delen. Indien de gebruiker het werk bewerkt kan het daaruit ontstane werk uitsluitend krachtens dezelfde licentie als de onderhavige licentie worden verspreid.

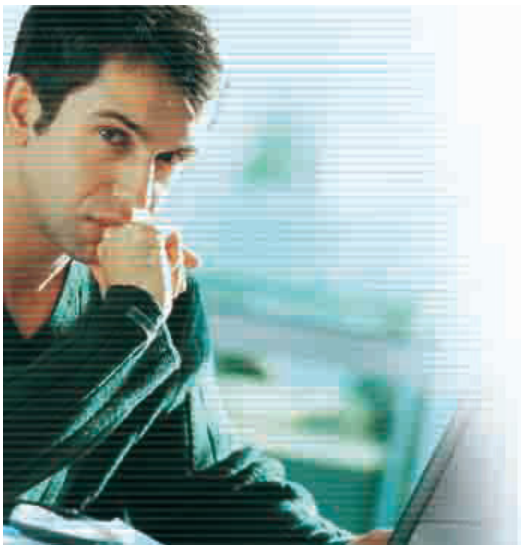
- Bij hergebruik of verspreiding dient de gebruiker de licentievoorwaarden van dit werk kenbaar te maken aan derden.
- De gebruiker mag uitsluitend afstand doen van een of meerdere van deze voorwaarden met voorafgaande toestemming van de rechthebbende.

Het voorgaande laat de wettelijke beperkingen op de intellectuele eigendomsrechten onverlet.

Dit is de vereenvoudigde (human-readable) versie van de volledige licentie.

Vrijwaring

WORDT LID VAN HET GVIB, SPEEL OP ZEKER EN BEVEILIG SAMEN...



Informatiebeveiliging is reeds jaren lang een noodzakelijk, spannend en dynamisch vakgebied. Vrijwel alle beroepen hebben meer dan ooit te maken met vertrouwelijkheid, beschikbaarheid en integriteit van informatie. of u nu als directeur, manager, adviseur of programmeur werkzaam bent. Het Genootschap van Informatie Beveiligers (GvIB) kan u behulpzaam zijn bij al uw vraagstukken op het gebied van informatiebeveiliging.

Wat is het Genootschap van Informatie Beveiligers?
Het GvIB is een open, breed samengesteld genootschap waarin professionals elkaar vinden om professioneel inhoud te geven aan informatiebeveiliging, door het uitwisselen van ideeën, informatie, kennis, inzichten en vooral veel praktijkervaring.

Wat willen wij bereiken?
Wij willen de fysieke, (systeem)technische & organisatorische beveiliging van gegevens en van de gegevensverwerkende middelen tegen inbreuken van binnenuit of buitenaf bevorderen. Ook willen wij de uitwisseling van kennis en ervaring en het netwerken van de in het vakgebied werkzame personen bevorderen. Bijvoorbeeld door middel van deze expertbrief.

De doelgroep
De doelgroep van het GvIB omvat iedereen, die door studie of beroepshalve te maken heeft met informatiebeveiliging, of hiervoor een bijzondere belangstelling heeft. Het snel groeiende ledenbestand kent vele disciplines zoals studenten, informatiearchitecten, technici, managers, organisatieadviseurs, juristen, beveiligingsfunctionarissen en ICT auditors. Onze leden komen voort uit alle mogelijke opleidingen, bedrijven, overheden, organisaties en leveranciers.

Voor de diverse soorten van lidmaatschap verwijzen wij u gaarne naar:

http://www.gvib.nl/afy_info_ID_1022.htm