Informatiebeveiliging en Finance & Control – van kopzorg tot hoofdzaak?

Rob Fijneman

SAMENVATTING Informatiebeveiliging blijft de gemoederen bezighouden. Bij incidenten wordt direct om actie gevraagd. Het grootschalig verlies van gegevens bij de Britse overheid en het regelmatig niet beschikbaar zijn van een website van een financiële instelling leiden tot veel publiciteit. Voor de desbetreffende organisatie is het naast het oplopen van potentiële financiële schades steeds vaker een imagoprobleem. Kwetsbaarheden nemen toe en vragen om samenhangende oplossingen. Dit artikel schetst een aantal ontwikkelingen rondom informatiebeveiliging en pleit voor een integrale aanpak binnen de *Governance Risk & Compliance*-agenda (GRC-agenda).

RELEVANTIE VOOR DE PRAKTIJK De toenemende mogelijkheden van informatietechnologie en de snelheid van verandering leiden tot zorgen op bestuursniveau. In combinatie met de roep om transparantie en de noodzaak tot het afleggen van verantwoording roept dit artikel op om informatiebeveiliging als integraal onderdeel van de *compliance*-agenda uit te werken. Daarbij kan de afdeling Finance & Control een belangrijke rol (gaan) vervullen.

1 Inleiding

Hoe veilig is de informatievoorziening in onze organisatie? Dit is een vraag die elke directie zich regelmatig zal stellen. De vraag is niet nieuw, sinds de introductie van informatietechnologie (IT) is dit een discussiethema. In de beginjaren van IT stelde de vermaarde professor Herschberg al dat beveiliging van IT een parallel vertoont met een vergiet. Steeds zijn er weer gaten die gedicht moeten worden. De kunst was volgens Herschberg om het patroon te ontdekken, zodat ook preventief kon worden gehandeld. Deze wijsheid geldt feitelijk nog steeds.

De dynamiek van de discussie is wel toegenomen. De IT-veranderingen dienen zich in hoog tempo aan, waarbij elke nieuwe technologie ook weer om een antwoord vraagt. De Gartner-groep heeft een *security exposure*schema gepubliceerd, waarvan de tijdslijnen niet hoopgevend zijn. Kort gezegd stelt Gartner dat in de eerste zes maanden na de introductie van een nieuwe technologie er beveiligingsgebreken worden ontdekt. Na twaalf maanden wordt actief door eindgebruikers hierover nagedacht, na 18 maanden worden de eerste pilots met verbeterde beveiliging gestart. Tussen de 24 en 36 maanden ontstaat een stabiele situatie en precies op dat moment wordt er weer een nieuwe technologie geïntroduceerd. Dit lijkt iets om moedeloos van te worden, zeker als de IT-capaciteit, zoals de wet van Moore stelt, iedere 18 maanden wezenlijk verandert. Volgens de wet van Moore verdubbelt de IT-capaciteit iedere 18 maanden, waarbij de IT-mogelijkheden feitelijk ook weer zijn vernieuwd. De vraag is of een *deadlock* kan worden voorkomen?

Dit artikel besteedt aandacht aan informatiebeveiliging in het licht van een aantal ontwikkelingen. Op de eerste plaats de continue IT-vernieuwingen zoals hiervoor al kort aangeduid. Uit recente discussies met raden van bestuur komen daarnaast zorgen naar voren als:

- Hoe weten we of de *intellectual property* voldoende is beschermd?
- Hoe weet ik zeker dat gevoelige *merger-* en *acquisition*-informatie aan de juiste personen wordt verstuurd? Een adresboek in Outlook kan onoverzichtelijk zijn, een *closed user group* zou al meer zekerheid geven.
- Hoe voorkomen we dat gevoelige informatie op straat terechtkomt? In de United Kingdom (UK) hebben in 2007 en aan het begin van 2008 grootschalige incidenten plaatsgevonden met USB-sticks en nalatigheid van personen in het omgaan met informatie die het thema *data leackage* hoog op de agenda hebben geplaatst.
- Hoe past informatiebeveiliging in de gehele *compliance*-agenda? Is het een apart onderwerp of is het integraal onderdeel van de kwaliteitsmaatregelen? Recente publicaties spreken steeds vaker over een *single view of risk* en het integreren van compliancemaatregelen.
- Hoe organiseren we informatiebeveiliging zeker bij toenemende *internet-centric* IT-oplossingen en deels ook bij toenemende uitbesteding van IT-diensten?
- Hoe gaan we om met privacygevoelige aspecten? Het handelen in creditcardgegevens op internet heeft het

College Bescherming Persoonsgegevens (CBP) in het najaar van 2008 de rode vlag doen hijsen.

Dit artikel beoogt niet alle onderwerpen van informatiebeveiliging aan de orde te stellen, laat staan op te lossen. Wel is het bedoeld om vanuit diverse bronnen de aandacht op informatiebeveiliging te vestigen en ook te zorgen dat de Finance & Control-afdeling of anderzijds verantwoordelijken deze onderwerpen actief op hun agenda plaatsen. Dit is niet een onderwerp voor de *chief information officer* (CIO) of IT-manager alleen, logischerwijs hoort het een plaats te hebben in het *in control*-proces van de gehele onderneming. Finance & control vormt daarbij een belangrijke speler, deels als *facilitator*, maar ook als deeleigenaar binnen het financiële proces.

Dit artikel start met het kort aanduiden van te beheersen objecten in en rondom IT (paragraaf 2), vervolgens wordt ingegaan op normen voor informatiebeveiliging (paragraaf 3). In paragraaf 4 wordt informatiebeveiliging gepositioneerd binnen de compliance-agenda om aansluitend in paragraaf 5 de managementverantwoordelijkheden te benoemen. In paragraaf 6 komt de specifieke rol van Finance & Control-afdelingen aan de orde. Dit resulteert in paragraaf 7 in een samenvatting en conclusie.

2 Informatiebeveiliging: welke objecten zijn in beeld?

IT manifesteert zich op diverse manieren. Een veelgebruikte indeling is die naar infrastructuur (netwerken, computersystemen) en applicaties. De informatie die vroeger overzichtelijk in ordners stond, bevindt zich nu onzichtbaar op vele plaatsen in het netwerk, op harde schijven in al dan niet mobiele computers en in toenemende mate zelfs in organisers, mobiele telefoons en *memorysticks*. Het overzicht waar welke informatie zich bevindt, is moeilijk te verkrijgen. Het applicatielandschap moet daarbij ook in beeld worden gebracht.
Om te komen tot een stelsel van beveiliging is inzicht en overzicht nodig. Alleen op basis van helder beschreven objecten kan een risicobeeld ontstaan en kan vervolgens de discussie over te treffen beveiligingsmaatregelen worden gestart. Er is veel gepubliceerd over aanpakken voor informatiebeveiliging. Dit artikel zal niet ingaan op alle fasen om te komen tot een integrale beveiliging, maar slechts enkele aspecten belichten.

Bij de beveiliging van applicaties wordt veel aandacht besteed aan authenticatie en autorisatie. Bij authenticatie wordt gesproken over digitale certificaten, al dan niet in combinatie met *smartcards* en biometrie. Roos Lindgreen (2002) concludeerde dat digitale certificaten nog lang geen gemeengoed waren, een conclusie die ook nu nog onverminderd kan worden getrokken. Autorisaties moeten in complexe enterprise resource planning-applicaties (ERP-applicaties) worden verwerkt en teveel organisaties hebben nog conflicten in geïmplementeerde functiescheidingen. Een ander aandachtspunt is het versleutelen van vertrouwelijke gegevens, dit is meer en meer een *commodity*. Verder leeft de zorg over de blijvende integriteit van applicaties, denk daarbij aan zaken als virussen en dergelijke.

De beveiliging van technische infrastructuur start met de uitdagende vraag: wat is de in gebruik zijnde topologie? Een *case study* beschreven door Kornelisse en De Wolf (Kornelisse, 2006) toont aan dat het inventariseren van *servers* in een netwerk al tot opvallende zaken kan leiden. In het kader van een IT-audit werd een IT-auditor gevraagd sporenonderzoek te verrichten in een netwerk. Een reguliere startvraag is om de topologie van het netwerk op te vragen. Dit gebeurde ook in dit onderzoek, echter de IT-auditor kreeg snel het vermoeden dat het schema incompleet was. Door de inzet van *auditsoftware* ging de IT-auditor het dataverkeer op het netwerk volgen en via het spoor van netwerkadressen kreeg hij geleidelijk aan een beeld van de systemen die tot het netwerk behoorden. Het netwerk bleek allerlei onverwachte componenten te bevatten, deels ook illegaal aangesloten op het netwerk. Dit leidde ook tot overtredingen van de gestelde informatiebeveiliging. De betreffende organisatie was zeker niet 'in control'. Hoewel dit wellicht een extreem voorbeeld is, is dit zeker niet uniek. Een compleet overzicht van de IT-inventaris is zelden beschikbaar, wel opmerkelijk niet alleen vanuit oogpunt van informatiebeveiliging, maar ook vanuit de perspectieven kostenbeheersing en compliance. Denk bijvoorbeeld aan het voldoen aan licentiecontracten met leveranciers. Ook hiervoor is een IT-inventaris noodzakelijk.

Informatiebeveiliging wordt gedefinieerd als een stelsel van maatregelen dat tot doel heeft de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te waarborgen. (Overbeek en Ter Laak, 2006) Dit is breed gedefinieerd, soms heeft de beveiligingsdiscussie in een organisatie alleen betrekking op vertrouwelijkheid. Door de onderlinge verwevenheid van maatregelen is het echter logisch om het begrip breed te definiëren. Bij de introductie van IT werd beveiliging vooral vertaald in fysieke maatregelen: computersystemen werden in aparte ruimtes geplaatst. Vandaag de dag is beveiliging een subtiel spel tussen activiteiten in de organisatie (processen en procedures), de technische beveiliging, de menselijke component en fysieke beveiliging.

3 Normen voor informatiebeveiliging

Bij het beoordelen van beveiligingsmaatregelen wordt steeds vaker gebruikgemaakt van *standards of due care*: normen, methoden, richtlijnen en dergelijke die door de

markt zelf zijn ontwikkeld en die in de loop der jaren als *de facto*-standaarden voor het inrichten van beveiliging zijn gaan gelden (Overbeek en Ter Laak, 2006)

Een bekend voorbeeld is de Code voor Informatiebeveiliging, die is omgezet in een ISO standaard (ISO 17799). Gestart als een *best practice*-initiatief tussen een aantal gerenommeerde bedrijven, is dit doorontwikkeld tot een de facto-standaard. Hoewel er in de praktijk bezwaren worden geuit tegen de ISO-standaard, bevat het een overzicht van te gebruiken maatregelen op het onderwerp beveiliging. Deze maatregelen bestrijken het eerder genoemde spectrum van organisatie, techniek, de menselijke factor en fysieke beveiliging. Het aanbrengen van details heeft niet plaatsgevonden tot op het niveau van technische parameters of specifieke geprogrammeerde controles in bijvoorbeeld ERP-systemen, maar de standaard vormt een leidraad c.q. biedt een structuur om maatregelen verder te details aan te brengen.

Een andere normenset is opgenomen in de Information Technology Infrastructure Library (ITIL). ITIL, een verzameling richtlijnen voor het beheer van informatiesystemen, bevat diverse modules voor het beheer van IT-processen waaronder *security management*. Het proces van beveiliging staat hierbij centraal. Het gaat bijvoorbeeld om de vragen: waar moet de *security officer* worden gepositioneerd en waar moeten andere governance-aspecten van beveiliging worden behandeld?

Sinds het begin van deze eeuw maakt COBIT (Control Objectives for Information Technology, www.itgi.org.) een snelle opmars. COBIT werd geïntroduceerd als een de facto-standaard bij de implementatie van Sarbanes-Oxley. Het IT Governance Institute ontwikkelde richtlijnen om COBIT te implementeren en daarmee de gehele IT-cyclus te voorzien van beheersnormen en -maatregelen. De beveiligingsaandachtspunten vormen hiervan een integraal onderdeel. Ook niet-SOX-plichtige bedrijven namen vervolgens dankbaar deze structuur over.
Daarnaast worden door leveranciers van IT-componenten en -*tools* iedere dag nieuwe standaarden ontwikkeld, ook op het gebied van beveiliging. De vraag is natuurlijk: welke techniek moet worden voorzien van welke beveiligingsmaatregelen?

Er zijn veel normen en standaarden en het is dus vooral een keuzeproces. Het initieel uitwerken van beveiligingsnormen is minder een probleem, een keuze maken uit voorliggende beveiligingsmaatregelen des te meer. Het balanceren tussen risico's en investeringen in beveiliging blijft dagelijkse kost, dit is een *perpetuum mobile*, aangezien iedere nieuwe IT-techniek ook weer nieuwe beveiligingsrisico's introduceert. Het is geen kwestie van goede of foute normensets. De laatste jaren is wel merkbaar dat door de aansluiting op *corporate governance* (en het daarbij gebruikte COSO-model) de structuur van COBIT duidelijk terrein wint. COBIT biedt een integraal *framework* en vormt daarmee een basis om informatiebeveiliging niet geïsoleerd te behandelen.

4 Compliance-agenda

Informatiebeveiliging zou geen losstaand onderwerp moeten zijn. Toch is de uitdaging hoe het geheel van complianceeisen aan elkaar te koppelen is. Compliance is vooral het beantwoorden van de vraag of een organisatie voldoet aan alle gestelde interne en externe regels. Interne controles in en rondom processen moeten zekerheden geven en gelet op de integratie tussen processen en IT bevinden velen van deze controles zich op het gebied van IT. Het beoordelen van beveiligingsmaatregelen vormt daarmee een onderdeel van het beoordelen van de interne controles.

Veel organisaties hebben een omvangrijke complianceagenda die kan bestaan uit:

- het voldoen aan financiële regelgeving zoals Sarbanes-Oxley of eisen van de Code Tabaksblat;
- het voldoen aan productkwaliteitseisen. Organisaties die bijvoorbeeld actief zijn in de zorgsector of leveranciers van producten aan de zorgsector, moeten in de Verenigde Staten voldoen aan eisen van de Food and Drug Agency (FDA). Ook organisaties die actief zijn in de chemische en farmaceutische sector kennen uitgebreide productnormeringen en kwaliteitseisen;
- het voldoen aan privacyeisen gelet op specifieke producten of diensten die in de markt worden gezet. Vooral producten voorzien van *embedded software* behoeven de aandacht;
- het voldoen aan informatiebeveiliging als voortvloeisel van de effecten van de Wet computercriminaliteit en/of de Wet bescherming persoonsgegevens of meer in het algemeen, omdat toezichthouders binnen de sector (denk aan De Nederlandsche Bank) specifieke eisen stellen aan informatiebeveiliging;
- voldoen aan eisen op het gebied van *corporate social responsibility*.

Deze opsomming is niet limitatief bedoeld; variaties en aanvullingen zijn er in vele vormen. Wel is een rode draad te ontdekken. Complianceprogramma's worden meestal als een project gestart. In projectvorm worden de normen en beheersmaatregelen uitgewerkt en wordt uitrol in de organisatie gestart. Teveel organisaties blijven steken in dit projectformaat. Het benoemen van verantwoordelijken in de lijn vindt moeizaam plaats, dit geldt ook voor het regulier monitoren van de uitkomsten van het complianceproject.
Daarnaast is zichtbaar dat voor de genoemde compliance-

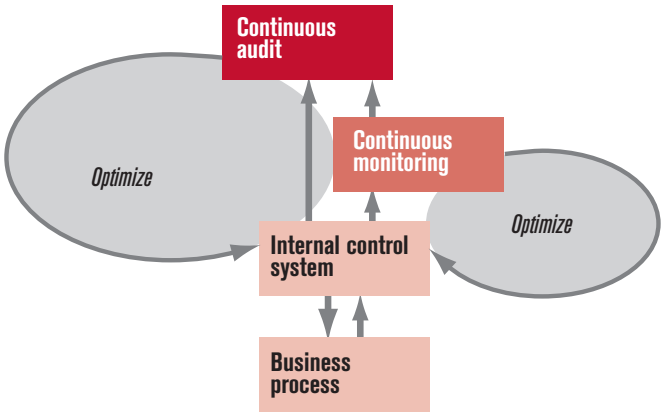
onderwerpen verschillende teams worden geïnstalleerd. De afdeling Finance & Control pakt de financiële compliance op, de afdeling Corporate IT start met de informatiebeveiligingsvraagstukken, de afdeling Legal is betrokken bij de privacyvraagstukken en het voldoen aan productnormen zoals de FDA wordt behandeld door de afdeling Productkwaliteit et cetera.

Wie voert de compliance-agenda en hoe wordt inefficiëntie in de aanpak voorkomen? Dit lijkt de uitdaging te vormen. Diverse organisaties evalueren momenteel hun aanpak op het onderwerp *Governance Risk & Compliance* (GRC).
De discussies gaan dan ook vooral over de *scope* van de GRC-agenda, waarbij het nastreven van een single view of risk belangrijk is en tevens het benutten van de mogelijkheden van diverse IT-tools. Leveranciers lanceren GRC-tools waarmee het inrichten en monitoren van beheersmaatregelen steeds meer geautomatiseerd kan plaatsvinden. Gartner-onderzoeken (2007) geven aan dat de compliance-gerelateerde IT-uitgaven sterk zullen toenemen. In 2006 bedroegen de uitgaven voor GRC-software naar schatting 354 miljoen dollar, een jaarlijkse groei van 28 procent is voorspeld, resulterend in 900 miljoen dollar in 2011.

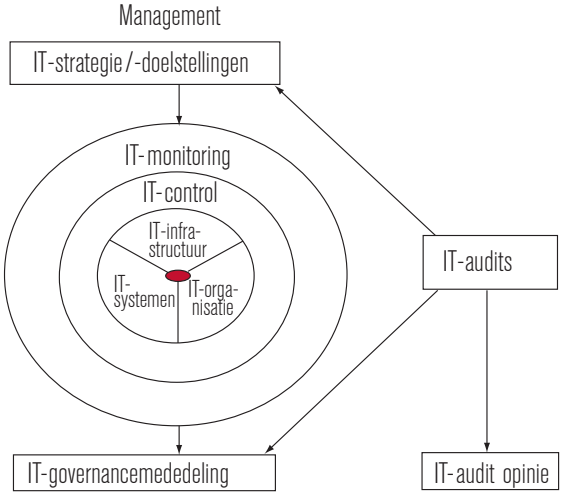
Begrippen als *continuous monitoring* en *continuous auditing* worden gebruikt en actief opgenomen in organisaties. Bij het geautomatiseerd vaststellen of IT-controls hebben gewerkt, wordt volgens Klumper en Francken (2008) bewijsmateriaal direct uit de onderliggende systemen verkregen. Klumper (2009) besteedt hier ook aandacht aan in relatie tot het COSO-model. Door ingestelde 'regels' kan worden vastgesteld dat er zich geen functiescheidingsconflicten hebben voorgedaan. Bewijsmateriaal kan worden verkregen door specifieke GRC-tools, maar ook door *data-mining*technieken. Het testen is ingebed in de processen van de organisatie. Als de organisatie zelf de werking van de ingerichte controls test, wordt dat continuous monitoring genoemd. Indien een interne of externe auditor de testen uitvoert, dan noemen we dat continuous auditing. Figuur 1 geeft de samenhang aan.

Deze ontwikkelingen hebben ook effect op het onderwerp informatiebeveiliging. Informatiebeveiliging wordt ingepast in andere compliance-agenda's. Tevens kan informatiebeveiliging ook centraler worden aangepakt. Slechts één voorbeeld wordt hierna genoemd. Parallel aan de GRC-discussie loopt de discussie over *Identity & Access Management* (IAM). IAM richt zich op het introduceren van een unieke en eenduidige toegang tot de IT-middelen en gegevens in een organisatie. Een zo te noemen *single view of autorisation*, waarbij een eenduidig eigenaarschap is uitgewerkt en tools beschikbaar zijn om uitgifte en beheer van autorisaties te regelen.

Figuur 1 Continous auditing versus continuous monitoring



Figuur 2 Structuur IT-governancemededeling



5 Management: neem uw verantwoordelijkheid

In 2004 werd onder de noemer 'Beat IT or Control IT' door Fijneman aandacht gevraagd voor onderwerp IT-governance. Hij bepleit dat het management het heft in eigen hand moet nemen. Informatiebeveiliging is een onderdeel van de IT-governance-agenda. IT-governance heeft als doel dat het management kan aantonen de juiste beheersing van de IT-infrastructuur, de IT-systemen en het netwerk te hebben gerealiseerd. Breder geformuleerd wordt wel gesteld, dat IT-governance het mechanisme is om de IT-werkprocessen efficiënt en effectief te regelen, zodat deze een bijdrage leveren aan de *business*wensen en daarover rekenschap kan worden afgelegd. Hierbij kan samenspel ontstaan tussen het management en auditors, zoals blijkt uit figuur 2.
Alle IT-componenten en -processen worden in deze opzet voorzien van beheersnormen, die meetbaar en controleer-

baar zijn. De IT-controls zijn concreet beschreven en het management heeft de IT-monitoringfunctie ook beschreven en gerealiseerd. De interne IT-auditor kan ingezet worden als *tool of management* om de juistheid van de IT-controls te monitoren. IT-audits kunnen worden uitgevoerd om de kwaliteit van de IT-controls te toetsen en daarmee ook de kwaliteit van de onderbouwing van de IT-governancemededeling. Een externe IT-auditor zou aansluitend zijn mening kunnen geven over de mededeling zelf.

6 Rol van Finance & Control

Er is veel in beweging en zoals eerder vermeld, blijft dit waarschijnlijk in en rondom IT ook het geval. De afdeling Finance & Control zou een professionele benadering van IT specifiek gericht op de beheersing van IT ook kunnen ondersteunen.

De IT-verantwoordelijken zijn gericht op het realiseren van de projectdoelen en het op efficiënte wijze realiseren van effectieve oplossingen. Tijd en ruimte voor beheersings- en beveiligingsdiscussies lijkt er regelmatig niet te zijn. De afdeling Finance & Control kan hier de helpende hand bieden door passend bij het *in control framework* van de organisatie ook het onderwerp informatiebeveiliging op de agenda te plaatsen.
Naast interne spelregels dwingen ook wet- en regelgeving organisaties daartoe. Medio jaren tachtig van de vorige eeuw ontstond al het begrip computervredebreuk als afgeleide van de discussies over de Wet computercriminaliteit. Sinds die tijd is te constateren dat de wetgever opgeschoven is van enig niveau van beveiliging naar een passend en zelfs een optimaal niveau van beveiliging. Organisaties worden verondersteld informatiebeveiliging uit te werken, passend bij de aard van hun processen en activiteiten, zodat via een risicoanalyse een verantwoord beveiligingsstelsel kan worden geïmplementeerd.

7 Samenvatting en conclusies

Het uitwerken van beveiliging is geen statisch proces. Iedere nieuwe IT-oplossing heeft weer nieuwe risico's en overigens gelukkig ook mogelijkheden tot het verbeteren van beveiliging. Het tijdens de projectfase actief beoordelen van deze mogelijkheden en risico's is een vereiste. Een *impact*analyse van beveiliging zou dan ook aan het management moeten worden voorgelegd.
Moderne technieken kunnen deze analyse ondersteunen. De termen continuous monitoring en auditing zijn al genoemd in dit artikel. IT-tools zijn beschikbaar om ook diverse informatiebeveiligingsscans te ondersteunen. Traditioneel worden deze tools vooral ingezet rondom het beoordelen van functiescheidingen; sommige organisaties gebruiken daarvoor intrigerende projectnamen als X-Ray. De gehele organisatie wordt gescand en eventuele onvolkomenheden worden gesignaleerd en desnoods individueel verder onderzocht. Dit vertoont veel overeenkomsten met het incheckproces bij vliegvelden vandaag de dag. Voor de individuele gebruiker levert dit potentieel wel irritaties op, de kunst is dus om toe te lichten waarom het grotere geheel (in dit geval de organisatie) er toch veiliger van wordt.
Verder is het zaak om proactief met leveranciers in contact te blijven over de ontwikkeling van beveiligingstools. Standaarden zouden sneller mogen worden gerealiseerd, het tempo waarin wordt geüniformeerd valt nog tegen. Leveranciers blijven aanhikken tegen de kosten en de commerciële voordelen van de tools.

Is het nu alleen een kwestie van het steeds verder invoeren van IT-tools en het verder automatiseren van IT-controls? Worden daarmee de in de inleiding gestelde managementvragen opgelost? De technische mogelijkheden helpen wel, echter informatiebeveiliging is en blijft in belangrijke mate ook mensenwerk. *Soft controls* behoeven meer en meer de aandacht. Een parallel met een recent uitgevoerd KPMG-onderzoek (2009) over *risk management* in de bancaire sector dringt zich op. Als één van de oorzaken van de huidige kredietcrisis werd het gebrek aan een risicocultuur genoemd. Risico's kunnen soms niet openlijk worden besproken. Het realiseren van een cultuur waarin ook een onderwerp als informatiebeveiliging op waarde wordt geschat, staat centraal. De eerlijkheid gebiedt dat beveiliging barrières geeft, die naarmate er lange tijd geen incidenten plaatsvinden als hinderlijk worden ervaren. Zo weet iedereen wel dat wachtwoorden nodig zijn, maar het onthouden daarvan op de vele verschillende IT-systemen valt niet mee. Er dreigt dan toch snel gemakzucht te ontstaan. Een incident zet het onderwerp vaak weer op scherp.

Het van incident naar incident managen is niet de gewenste aanpak en kan vandaag de dag ook niet meer op IT-gebied. Organisaties hebben steeds vaker open grenzen en hebben hun IT-omgeving internet-centric ingericht of hebben vergaande plannen daartoe. Kort gezegd, betekent dit dat het bedrijfsnetwerk steeds meer een openbare weg gaat worden: klanten en leveranciers maken ook gebruik van deze weg, maar hebben andere bevoegdheden dan de medewerkers. De samenwerking moet soepel verlopen en toch moet ook een gevoel van veiligheid worden gerealiseerd. Een beveiligingsincident zet alle relaties op scherp en kan veel meer dan in het verleden direct invloed hebben op de bedrijfsprocessen en commerciële belangen van een organisatie. Een organisatie moet inherent veilig zijn en de juiste maatregelen treffen. Dit moet tevens aantoonbaar gebeuren. Communicatie met de businesspartners zal plaats moeten vinden. Indien vandaag de dag een rondgang wordt gemaakt langs websites is het nog niet gebruikelijk om een paragraaf aan te treffen over de beveiliging

daarvan. De verwachting is wel dat dit in de toekomst *usance* wordt. Organisaties zullen dan niet alleen een mededeling opnemen, dit is vrij statisch, maar juist ook moeten uitleggen op welke wijze zij omgaan met informatiebeveiliging. Gelet op de openheid van het netwerk zijn informatiebeveiligingsstandaarden dan wel zeer gewenst, destijds was dit al het achterliggende doel van de Code voor Informatiebeveiliging.

De afdeling Finance & Control zou als verbindende schakel in deze complexiteit een rol kunnen vervullen, dat is een mooie gedachte en hoeft geen utopie te zijn. Historisch gezien is dit de afdeling met de meeste kennis van beheersingsvraagstukken. Er moet dan wel kennis bijkomen om de IT-beveiliging aan te kunnen pakken. Deze kennis kan intern worden gemobiliseerd of in samenspraak met interne en/of externe auditors worden ingevuld. Het aardige is dat ontwikkelingen in verslaggeving zoals Extended Business Report Language (XBRL) een mooie basis bieden om de daarbij passende en noodzakelijke aanpassingen in informatiebeveiliging door te voeren. Mashaie (2008) heeft eerder XBRL als een katalysator voor continuous auditing gepositioneerd. Er is dan al een '*momentum* van verandering'. Dit maakt het verbeteren van informatiebeveiliging een gemakkelijker proces dan in een statische omgeving.

De afdeling Finance & Control is niet de eigenaar van informatiebeveiliging. Op onderdelen in het financiële proces wel, echter ook andere proceseigenaren en natuurlijk ook de IT-afdeling/CIO moeten actief betrokken zijn. Als een aanpak wordt opgezet, waarbij informatiebeveiliging niet geïsoleerd maar passend in de GRC-agenda wordt uitgewerkt, kan de kopzorg veranderen in een hoofdzaak. ■

Prof. dr. Rob Fijneman is voorzitter van KPMG IT Advisory in Nederland en de regio's Europe, Middle East en Africa. Sinds 2004 is Rob als hoogleraar IT-auditing verbonden aan de Universiteit van Tilburg. Zijn werkervaring is gericht op IT-governance en IT-assurancevraagstukken bij multinationals.

Literatuur

- Donkers H. en B. Beugelaar (2008), *IT Governance, Performance & Compliance,* Groningen: Uitgeverij Kleine Uil.
- Fijneman, R.G.A. (2005), *IT auditing: grenzeloos of gelimiteerd,* Universiteit van Tilburg.
- R.G.A. Fijneman (2004), Beat IT or Control IT, Kracht van de vernieuwing, visies op ICT, in: A. Shahim, *Kracht van de vernieuwing, visies op ICT,* Schoonhoven: Academic Services, pp. 171-201.
- Kornelisse, P. en R. de Wolf (2006), Beveiliging van IT-infrastructuur, in: R.G.A Fijneman, E.E.O. Roos Lindgreen en K.H.G.J.M. Ho (2006), *IT auditing en de praktijk,* Schoonhoven: Academic Services, pp. 31-36.
- Gartner Research (2007), *Magic quadrant for finance governance risk & compliance,* Management Software.
- Klumper, C. en M.A. Francken (2008), Embedded testing – uitrol naar IT controls?, *Compact,* vol. 35, no. 3, pp. 10-13
- Klumper, C. (2009), Toepassing van de monitoringcomponent van het COSO-raamwerk. Betere interne beheersing voor organisaties én belangrijke innovatie in het accountantsberoep, *Maandblad voor Accountancy en Bedrijfseconomie,* vol. 83, no. 3, 78-83.
- Mashaie, M. (2008), XBRL een catalysator voor continuous auditing, *Maandblad voor Accountancy en Bedrijfseconomie,* vol. 82, no. 7/8, juli/augustus, pp. 324-333.
- Roos Lindgreen, E.E.O. (2002), *Over informatietechnologie, accountancy en informatiebeveiliging,* Vossiuspers UvA.
- Website van IT Governance Institute met referentiemateriaal over COBIT- en IT-governance-aanpakken: www.itgi.org.