

Ronde tafelgesprek: Hoe kunnen SOX en Basel II bedrijven sterker maken?

ORM: Technology or Business?

Het wereldwijd succesvolle Nederlandse bedrijf Consul richt zich momenteel op een doorbraak in de VS. Het bedrijf beschouwt dit als een kernvoorwaarde voor de voortzetting van het huidige succes. De verkooporganisatie zal in de komende twee jaren dan ook verdubbelen, met name in de VS. Consul, ontstaan in de computer mainframe omgeving, beschikt over twintig jaar ervaring en know-how op het gebied van z/Os. Gedurende de laatste vijf jaar heeft het bedrijf zich toegelegd op de ontwikkeling van 'multi-platform' producten. Consul laat over deze periode een groeiende omzet zien, met een versnelling in de laatste twee jaren. Interessant hierin is de significante groei van omzet uit Consul InSight Security Manager en de constante inkomensstroom uit onderhoud en support.

Als gevolg van de sterke toename in regelgeving, zoals Basel II, HIPAA, Sarbanes-Oxley en ISO 17799, staan thema's als auditing, bedrijfsbeveiligingsbeleid en naleving hiervan bij veel bedrijven hoog op de agenda. Men vraagt zich af hoe dit het beste aangepakt kan worden. Er bestaan grote misverstanden en interpretatieverschillen bij zowel bedrijven als overheidsinstellingen, vaak veroorzaakt door de gekozen insteek. Het thema 'naleving van regelgeving' wordt namelijk vaak sterk vanuit de optiek van IT en IT-security specialisten benaderd. Het is echter belangrijk om deze zaken zeker ook vanuit een business control-perspectief te bezien. Daarmee komt men tot de ontdekking dat deze thema's juist als een business enabler kunnen worden beschouwd en niet langer uitsluitend als een kostenfactor.

Een grote uitdaging is het maken van een onderscheid tussen alle reële bedreigingen enerzijds en externe bedreigingen -waar veel over wordt gesproken en gepubliceerd- anderszijds. Denk bij dit laatste aan hackers die erin slagen om bij grote bedrijven binnen te dringen en bijvoorbeeld credit card fraude realiseren. Dergelijke inbreuken kan men met succes tegenwerken met firewalls en andere detectie oplossingen. Belangrijker is echter de dreiging van binnenuit. Denk aan fouten gemaakt door medewerkers, frauduleuze handelingen en diefstal van bedrijfsgeheimen of intellectueel eigendom. Veel bedrijven willen hier geen ruchtbaarheid aan geven, teneinde hun reputatie niet op het spel te zetten. Door dit stilzwijgen lijken de gevaren minder groot dan ze in werkelijkheid zijn. Toch kan iedereen zich wel enkele voorbeelden van interne fraude voor de geest halen. Denk aan de ondergang van de Barings bank. Of het door een Robeco medewerker verdonkeremanen van 10 miljoen gulden. Of recentelijk het 'kraken' van 10.000 VISA cards bij een toeleverancier van Interpay. Of het hacken van meer dan 40 miljoen credit card nummers, een gevolg van het feit dat een transactieverwerkend bedrijf zich niet aan de regels hield. De totale schade is niet te overzien.

De huidige situatie in de VS

In de Verenigde Staten is het niveau van 'security awareness' op dit moment zeer hoog. Dit is een gevolg van de Sarbanes-Oxley act, die bedrijven voorschrijft zich te wapenen tegen ongeoorloofd gedrag van medewerkers en directie. Overtredingen kunnen leiden tot straffen van maximaal \$5 miljoen of 20 jaar gevangenisstraf. Dit is voor directieleden een belangrijke stimulans om de verslaggeving van het bedrijf op orde te krijgen. In Nederland en andere Europese landen is deze dreiging minder aanwezig, behalve bij aan de Amerikaanse beurs genoteerde multinationals. Ook toeleveranciers van beursgenoteerde Amerikaanse bedrijven zullen strenger geselecteerd worden op basis van hun security maatregelen. Men hoopt zo een 'inktvlek'-effect teweeg te brengen: als een klein aantal bedrijven zich conformeert en aldus een sterke marktpositie verkrijgt, volgt de rest vanzelf. Echter, op dit moment kunnen toeleveranciers van bedrijven genoteerde aan de Amerikaanse beurs niet worden vervolgd voor het niet naleven van veiligheidsvoorschriften.

Er bestaat veel onduidelijkheid over de rol en doelstelling van de Sarbanes Oxley act in de Verenigde Staten. De doelstelling kan echter in een enkele regel worden samengevat: het brengen en geven van openheid en transparantie over investeringen die een bedrijf doet om investeerders en het publiek te beschermen tegen mismanagement. Als we ons losmaken van de regelgeving, die meestal ontstaat als een reactie op gebeurtenissen in de maatschappij –wie herinnert zich niet de grote schandalen in de Verenigde Staten van grote energie en internet bedrijven –Enron!- of in Europa-Ahold en Barings – blijkt ook dat deze gedwongen (maatregelen) tot het meten en documenteren van bedrijfsactiviteiten kunnen leiden tot een gigantische verbetering in business performance. Belangrijke aspecten bij de implementatie zijn het meten van alle relevante gegevens en activiteiten op bijvoorbeeld bedrijfsnetwerken, het openbaar maken van gegevens inclusief fouten of problemen, procesbesturing en bewaking, resources en infrastructuur. Naast Sarbanes Oxley is Basel II regelgeving in Nederland actueel, deze is echter uitsluitend bestemd voor de bank- en verzekeringswereld. Andere organisaties zijn niet gebonden door Basel II regelgeving, wel door regels voor bescherming van data en privé-gegevens.

Een academische kijk op het risico van IT-investeringen

Momenteel bestaan er voor internationale opererende bedrijven al zo'n 20 bekende regelgevingen die consequenties hebben voor bedrijfsvoering en auditing. Veel bedrijven denken dat het organiseren volgens de nieuwe regelgeving op te lossen is met investeringen in IT. Dit heeft weer tot gevolg dat directieleden op hun eenvoudige vragen vaak onbegrijpelijke antwoorden krijgen van IT-experts, waarmee zij weinig of niets kunnen. Het gros van dit soort investeringsbeslissingen wordt vaak genomen op basis van intuïtie en onwetendheid. Hoe anders valt te verklaren dat er jaarlijks voor \$ 300 miljard aan mislukte IT-projecten wereldwijd wordt uitgegeven: \$ 140 miljard in Europa en \$ 150 miljard in de Verenigde Staten? Het is uit onderzoek gebleken dat investeerders doorgaans negatief reageren op aankondigingen van grote IT-investeringen, die vaak misgaan en meer kosten dan ze opleveren. Onderzoek wijst uit dat aandeelhouders en beursanalisten zeer bewust zijn van de risico's die met IT investeringen samenhangen. Enkele voorbeelden van het effect van mislukte IT-activiteiten op bedrijfswaarde zijn ICI, die de waarde van het aandeel met 39% zag dalen en Hagemeyer, die een divisie met een winst van 86 miljoen naar een verlies van 28 miljoen zag gaan en van 22% naar 18% marktaandeel ging. Of bijvoorbeeld het faillissement van Van Heek-dochter Tweka, ontstaan door blunders met IT-investeringen en niet-functionerende logistieke processen.

Aan de Vrije Universiteit Amsterdam heeft professor Chris Verhoef een methode ontwikkeld om IT-investeringen meetbaar te maken en tot een verantwoorde business case te komen. Dankzij een jarenlange studie, toegepaste econometrie, risk management en geavanceerde wiskunde, heeft hij modellen ontwikkeld waarmee de risico's van investeringen in IT-projecten kunnen worden berekend. IT-ontwikkelingen en investeringen daarin brengen altijd onzekerheden met zich mee, maar dankzij deze modellen lukt het om de mate van risico voor een IT-project beter in te calculeren, door de wetmatigheden in de ontwikkeling van IT-systemen te gebruiken. Als je dit weet dan kun je de verplichtingen die via regelgeving aan het bedrijfsleven en overheden wordt opgelegd, omzetten in een voordeel. Het is mogelijk om data te gebruiken om bedrijfsanalyses uit te voeren die nieuwe kansen scheppen en tegelijkertijd aan de wetgeving te voldoen. Daarnaast is het mogelijk een op feiten gebaseerde IT-investering te doen, die het mogelijk maakt de toegevoegde waarde van een IT-project veel beter in te schatten en een indicatie van de ROI te krijgen.

Een ander knelpunt in de besluitvorming van IT-projecten is het feit dat veel bedrijven zich laten leiden door voorstellen die komen vanuit de IT-beveiligingsafdelingen. Dit laatste is helaas verre van optimaal omdat deze automatiseringsafdelingen meestal zijn opgesteld om bedrijfsprocessen te automatiseren of bedrijfsautomatisering te verbeteren. Vaak ontbreekt echter een belangrijk element in de keten, namelijk de capaciteit om vast te kunnen stellen waar het risico van de investering ligt en wat de werkelijke opbrengst zal zijn. De oorzaak hiervan ligt in het feit dat IT-experts doorgaans niet in bedrijfskundige processen denken, maar in technologie oplossingen. Wil een bedrijf dus een business model gebruiken om de IT-investeringsrelevantie op te zetten, dan dienen er ook bedrijfskundigen en wellicht risicomangers bij deze projecten te worden betrokken.

Uit analyses van IT-projecten in de laatste jaren uitgevoerd, blijkt dat de helft van de projecten twee keer het bedrag en twee keer meer tijd kostte dan was begroot en daarbij slechts de helft van het verwachte resultaat bracht. 30% van de projecten valt duurder uit, duren twee keer langer en brengen niets op. Slechts 20% van de IT-projecten leveren tegen voorziene kosten en binnen een voorzien tijdsbestek de afgesproken resultaten.

Beslissingen worden nog steeds sterk op basis van gevoel en intuïtie genomen, omdat risico voor de meeste mensen een emotionele factor is. Echter, als we doordenken dan blijkt dat het kwantificeren van risico's een veel verstandiger uitgangspunt is waarbij men op operationele basis kan afwegen welke risico's welke consequenties met zich mee zullen brengen. Daarin kan men een prioriteitsstelling aanbrengen en zien welke risico's een bedrijf zou willen nemen en welke risico's een bedrijf persé wil beheersen.

Risk management is sterk gerelateerd aan de dreiging x de kwaliteit x de kosten. Voorbeelden hiervan zijn natuurlijk de bekende anti-virusproducten. Organisaties die verder gaan en waar mensen bij betrokken zijn, richten zich op het maken van een beleid, het opstellen van procedures en het trainen van het personeel. Veel bedrijven beschouwen dergelijke acties vooral als een flinke kostenpost. Echter, een recent gangbare opvatting is dat het reduceren van risico kan leiden tot het verbeteren van de bottom line van een bedrijf.

De juiste mensen op de juiste plaats

Ten gevolge van de regelgeving worden mensen met een IT achtergrond benoemd tot security managers of ingezet in de jonge compliance officer functie. Dit zijn vaak mensen die geen bedrijfskundige achtergrond hebben. De essentie van een weloverwogen IT investering, optimaliseren van IT-beveiligingsinfrastructuur en een snel te implementeren inpassing van de diverse compliance-opdrachten te verwezenlijken is hiermee niet organisatorisch opgelost. Het lijkt derhalve niet onlogisch om CFO's hoofverantwoordelijk te maken voor implementatie van compliance processen in een organisatie. Een voorbeeld: om het systeem te verbeteren, denkt een IT specialist aan het verbeteren van een firewall, het aanbrengen van een softwarepatch en Access Control Software Change management. Een risk manager denkt eerder aan het opsplitsen van verantwoordelijkheden en het gedifferentieerd autoriseren van medewerkers. Daarnaast denkt een risk manager veel meer in businessprocessen. Nieuwe inzichten leiden ertoe dat experts op het gebied van IT beveiliging en organisatieprocessen steeds vaker adviseren dat bijvoorbeeld information security officers een MBA-opleiding zouden moeten volgen, of bedrijfseconomische bijscholing moeten krijgen. In Amerika heerst nog sterk de overweging dat technologie het probleem zou moeten kunnen oplossen. Dat is een groot misverstand, daar zijn vriend en vijand het inmiddels over eens. Volgens Kris Lovejoy, Chief Technology Officer van Consult risk management, onlangs uitgeroepen tot een van de top 25 CTO's wereldwijd door het Amerikaanse blad Infoworld, loopt Europa op dit gebied ongeveer tien jaar voor op Amerika. De oplossing ligt in een procesmatige aanpak waarin mensen, systemen, applicaties, processen en data en het meten daarvan in een feedbackloop zijn ondergebracht.

Basel II, Sarbanes-Oxley en andere bepalingen

Basel II en SOX dwingen bedrijven risico's te kwantificeren en te documenteren. Dit brengt een grotere transparantie met zich mee. In de bankwereld worden onder Basel I en II drie soorten benaderingen toegepast: de Basic Indicator Approach (BIA), de Standard Indicator Approach (SIA) en de Advanced Measurement Approach (AMA). Elke benadering is gekoppeld aan een vast voorgeschreven minimum reserveringspercentage als zekerheid. Het hoogste uiteraard bij de BIA tussen 15 en 18%, 8 tot 12 % voor de SIA en 8% voor de AMA implementatie van Basel II dient te zijn gerealiseerd voor één januari 2008. De specifieke punten met betrekking tot AMA zijn gebruik van interne data en externe verlies data, zelfbeoordeling en de meest essentiële risico-indicatoren. Het ligt hierbij voor de hand dat beveiliging een economische drijfveer voor de financiële wereld vormt.

Vanuit de bankwereld kennen we al duidelijk het kredietrisico en het marktrisico. Dit werd uitgebreid behandeld in Basel I. Sinds Basel II is hieraan het operationeel risicomanagement toegevoegd. Basel II biedt de financiële wereld een eenvoudige handreiking aan, door drie regels voor te stellen waarbij de financiële instelling een percentage tussen 8 en 18% moet reserveren voor niet te voorziene risico's. Daarnaast dient data drie jaar lang te worden gedocumenteerd, geregistreerd en gerapporteerd. SOX daarentegen is veel meer gericht op de bescherming van de aandeelhouder. Sectie 404 schrijft voor dat er een jaarlijkse review van interne kernprocessen en principes volgens een vast stramien moet worden uitgevoerd. Dit dient transparantie te brengen bij de financiële rapportages en het jaarverslag. SOX 404 beschrijft de rapportage, SOX 302 verlangt een kwartaalmatige benadering en SOX 409 wijst op een real time (maximaal 4 dagen) invulling van risicovolle incidenten.

Samenvattend kun je stellen dat SOX de financiële aspecten van de zakelijke rapportage afdekt, met als doel transparantie, en Basel II brengt het proces voor alle operaties in kaart om tot optimale capital deployment te komen. SOX dreigt met stevige straffen, maar Basel II werkt met beloning. Non-compliance levert bij SOX gevangenisstraffen op, bij Basel II levert compliance permissie op om minder grote reserveringen op te bouwen. Andere benaderingen die eerder hun toepassingen vonden zijn COSO, veelvuldig geadviseerd door de SEC. COSO oriënteert zich sterk op governance. GISO richt zich meer op controle en Itil richt zich meer op business services. De laatste ontwikkeling genaamd Cobit combineert een aantal van de voorgaande procedures. Financieel en Operationeel Riskmanagement dragen in het bijzonder bij aan het verhogen van de accuratesse van de business forecast.

ORM volgens Consul

De principes van Operational Risk Management liggen in deze hoofdpunten: het ontwikkelen van een doelmatige management-omgeving, risico management (identificatie, vaststelling, monitor en opheffen), rol van de supervisor en openbaarmaking. Consul adviseert IT-beveiliging volgens een vijf-stappen benadering aan te pakken:

1. Het identificeren van de mogelijke bronnen van risico en de daarbij verwachte waarschijnlijkheid en kosten ervan.
2. Het specificeren van het risico dat bij deze kan optreden: hoog risico of laag risico.
3. Selecteer de risico's volgens de risico cultuur binnen het bedrijf. Met andere woorden; hoe groot is de risicohonger, wat wil men accepteren en wat niet?
4. Zet daar tegen de beschikbare controlemaatregelen uit, wat wordt geaccepteerd, wat wordt afgewezen? Hoe maak je risico beheersbaar?
5. Het risicobeheer: monitoren, meten en feedback.

Het meten en documenteren van alle evenementen en incidenten is van extreem groot belang, de analyse daarna zo niet nog belangrijker. Op basis hiervan is het mogelijk om voorspellingen te doen en rationele beslissingen te maken over noodzakelijke investeringen. Er gaan veel stemmen op om de verantwoordelijkheid voor beveiligingsmanagement niet bij specialisten te leggen maar bij de Business Managers. Ook mag de IT auditor steeds vaker beslissen over bedrijfsinvesteringen voor IT, bijvoorbeeld de beschikbaarheid van budget. Dankzij SOX en andere reguleringen krijgt deze functie steeds meer zeggenschap.

Hoe te implementeren?

Probeer niet alle nieuwe regelgeving verticaal te implementeren. Dit heeft een verlamme werking op de organisatie en de mensen daarin, omdat men permanent met een variabel doel bezig is. Bij nadere analyse blijkt dat de meeste regelgevingen een gelijksoortige structuur hebben en een aantal vergelijkbare uitgangspunten. Hierdoor is het verstandiger om op een horizontale manier te werken en te denken, hetgeen wil zeggen een bepaalde bedrijfsprocesstructuur aanbrengen die met een aantal kleine aanpassingen kan worden uitgebreid om te voldoen aan de wensen van nieuwe regelgeving. Bijvoorbeeld: de in Amerika relevante VISA COSP requirements dienen vanaf 30 juni 2005 te zijn geïmplementeerd. Dit is een regulering die verband houdt met data privacy. Overigens hebben System Administrators vaak moeite met controle op henzelf. Men ervaart dit als een inbreuk op de eigen integriteit waardoor ze vaak opzien tegen persoonlijke controle.

Consul biedt een aantal oplossingen, waaronder de InSight Security Manager, die bedrijven helpt snel een beleid te formuleren en te implementeren. Verder is het mogelijk zelfs zonder policy met het product al een aantal 'röntgenopnamen' te maken van de IT-beveiliging. In feite haalt Consul de angel uit de compliance verplichting. Dit komt voor een groot deel doordat Consul het enige bedrijf is dat multi-platform oplossingen levert. Dat wil zeggen: Consul InSight Security Manager kan Windows, Linux, IAS, ZOS, Oracle, SAP etc zonder problemen monitoren en auditen. Daarnaast kan het systeem op een zeer eenvoudige manier via een 'correlation engine' het totale dataverkeer van alle servers van een bedrijf auditen en belangrijker nog, in een zeer eenvoudig leesbaar presentatie automatisch aanleveren. Hierdoor kan op het hoogste niveau in de organisatie in een zeer korte tijd een diepgaande inzicht worden verkregen in de IT-beveiliging van het gehele bedrijf (30-45 minuten). Wat voorheen dagen werk kostte met inzet van tientallen personen, kan nu met een druk op de knop in ultrakorte tijd worden gerealiseerd. Hetzelfde geldt voor het aanleveren van data voor een auditor sessie van de jaarstukken. Als je nog niet klaar bent om de totale risk management te doen, dan zul je met behulp van Consul InSight Security Manager implementatie kunnen starten en vaststellen hoe de security georganiseerd is en wat de risico's zijn en een doorlopend proces opzetten om de verbeteringen te realiseren.

Marc van Zadelhoff
V.P. Business Development Consul