Return on Security Investments – ROSI

Dr. ir. P.L. Overbeek RE en drs. J. Voeten RE

Investeringen in informatiebeveiliging roepen veelal discussie op. De vraag is dan wat deze investeringen opleveren, wat hun rendement is. Leveren deze investeringen (kosten) voldoende baten op die de investering rechtvaardigen? Wat zijn de kosten die samenhangen met minder investeren in informatiebeveiliging? Dit artikel is gebaseerd op de resultaten van de expertbrief 'Return on Security Investment (ROSI): Hoe te komen tot een bedrijfseconomische onderbouwing van uitgaven op het gebied van informatiebeveiliging?' van het Genootschap van Informatie Beveiligers en geeft een eerste aanzet tot de bedrijfseconomische onderbouwing van investeringen in informatiebeveiliging, alsmede richting aan de rol van de auditor hierbij.

Inleiding

In een wereld waarin hackers, computervirussen en cyberterrorisme regelmatig in het nieuws verschijnen, wordt informatiebeveiliging steeds belangrijker. Organisaties bedrijven in toenemende mate, al dan niet via het internet, 'business' met ketenpartners en zijn verbonden aan netwerken van derden. De informatievoorziening is de motor achter deze ontwikkeling, maar ook gevoelig voor risico's.

Informatievoorziening bestaat in deze context uit tastbare onderdelen, zoals hardware en software, en niet-tastbare onderdelen. Niet-tastbare onderdelen zijn onder meer de waarde van gegevens in databases en de kennis alsook intellectueel eigendom in de systemen. De niet-tastbare onderdelen zijn vaak moeilijk in geld uit te drukken ([Mizz05]). Als de waarde van de informatievoorziening moeilijk is te bepalen, hoe kan dan eenduidig worden bepaald of evenredige maatregelen zijn getroffen om deze waarde te beschermen? Voor bedrijven speelt de vraag wanneer een redelijk beveiligingsniveau is gerealiseerd en, misschien nog belangrijker, hoeveel tijd en geld nog in informatiebeveiliging moet worden gestoken ([Sonn02]). Als bedrijven willen kwantificeren hoeveel ze zouden moeten investeren in informatiebeveiliging dan is veel informatie nodig:

- Wat kost het gebrek aan informatiebeveiliging?
- Wat zijn de gevolgen van het gebrek aan informatiebeveiliging voor de productiviteit?
- Wat zijn de gevolgen van een catastrofale breuk in de informatiebeveiliging?
- Wat zijn en kosten de meest effectieve oplossingen, de te treffen maatregelen?

Dr. ir. P.L. Overbeek RE
is partner bij OIS Information Risk & Security Management en doceert aan de universiteiten van Eindhoven en Amsterdam.

Paul.Overbeek@OIS-NL.EU

Drs. J. Voeten RE
is adviseur bij KPMG IT Advisory en is specialist op het gebied van informatiebeveiliging, procesanalyse en gegevensanalyse bij zowel publieke als private organisaties. Daarnaast is hij hoofddocent voor de Post-HBO IT Audit-opleiding aan de Haagse Hogeschool.

voeten.jorg@kpmg.nl

Dit artikel is mede gebaseerd op een expertbrief van het GvIB. De auteurs nodigen u uit bij te dragen aan de discussie.

- Welke gevolgen hebben de getroffen maatregelen voor de productiviteit?
- In hoeverre nemen getroffen maatregelen een dreiging weg en verminderen ze het risico samengaand met de dreiging?
- Welke kosten gaan gepaard met het implementeren van een maatregel en wat kost het om deze operationeel te houden?

Corporate en IT-governance zorgen ervoor dat organisaties op basis van een risico-inschatting keuzen maken over het al dan niet implementeren van maatregelen voor beheersing en beveiliging. Een organisatie wil weten dat het financieel verantwoord is om een investering te doen. Zo ook investeringen in informatiebeveiliging. Een organisatie zal investeringen in informatiebeveiliging willen doen als de kosten van maatregelen lager zijn dan de reductie van het (financiële) risico. En dan nog moeten investeringen daar worden gedaan waar ze het best renderen.

De vraag naar een bedrijfseconomische onderbouwing van investeringen in beveiligingsmaatregelen werd in de wereld van de informatiebeveiliging tot voor kort nauwelijks gesteld. De drijfveer was angst, onzekerheid of twijfel. Investeringsbeslissingen werden genomen op basis van 'gevoel', de mening van een autoriteit, en 'wat doen anderen'. De verschuiving naar een betere onderbouwing van investeringen past in de groeiende volwassenheid van het vakgebied. Waar informatiebeveiliging in het verleden steunde op de individuele professionaliteit ('a few good men'), schuift informatiebeveiliging nu op langs risicomanagement in de richting van compliance management. In de beveiligingsfunctie komt daarmee het accent minder op IT te liggen, en meer op business risk management en compliance. Dat laatste wordt ook steeds meer geëist, niet alleen vanuit de steeds zwaarder wordende wet- en regelgeving, maar ook door ketenpartners of klanten ([Over06]).

Wat is ROSI en wat is het nut van ROSI?

Heden ten dage worden investeringen voor beveiliging veelal genomen op basis van gevoel, een analyse van de directe uitgaven, en het gedrag binnen een peergroep (wat doen soortgelijke bedrijven). Op grond van subjectieve informatie wordt een beslissing genomen. Van belang is om de subjectieve informatie te objectiveren, zodat geobjectiveerde beslissingsondersteunende informatie kan bijdragen aan een minder subjectieve beslissing.

Er is een natuurlijke spanning tussen de indieners van een investeringsvoorstel, in dit geval veelal security professionals, en de beslissers over het voorstel (de business). De voorstellen van de indiener, de security professional, zijn enigszins verdacht: 'Misschien geven we wel te veel uit aan beveiliging. Incidenten horen er gewoon bij.' Daarbij komt dat de security professional de indruk wekt enkel een zo laag mogelijk aantal incidenten na te streven, in plaats van een zakelijke afweging te maken. Het voorstel is te vaak gedreven door een technology push in plaats van een demand pull. Bij demand pull is de business leidend, en geeft deze aan wat de risk appetite is. De security professional kijkt welke investeringsvoorstellen gedaan moeten worden om het gewenste risiconiveau te realiseren. De relatie tussen een investering in beveiliging en reductie van *business*risico's wordt tot op heden te weinig gelegd.

Een veelgehoord vertrekpunt is dat uitgaven zijn begrensd aan de hand van een percentage van de omzet. Zo mag het IT-budget een maximaal percentage van de omzet bedragen. Van het IT-budget mag vervolgens weer een percentage aan beveiliging worden toegewezen. Gartner, bijvoorbeeld, geeft aan dat het gebruikelijk is dat tussen de vijf en tien procent van het IT-budget aan IT-beveiliging wordt besteed. Zo'n getal geeft wel een ankerpunt, maar is op zich geen onderbouwing. Daarnaast worden ook maatregelen getroffen buiten de IT die bijdragen aan een betere informatiebeveiliging. Denk hierbij bijvoorbeeld aan fysieke beveiliging of aan bewustwording.

De relatie tussen een investering in beveiliging en reductie van businessrisico's wordt tot op heden te weinig gelegd

Belangrijke vraag is: zijn er specifieke investeringen aan te merken als 'beveiligingsinvesteringen'? De meeste investeringen zijn gericht op meetbare of zichtbare doelen, bijvoorbeeld op functionaliteit of op een hogere efficiëntie van het beheer. Helaas wordt security niet altijd als functionaliteit beschouwd. Wat er specifiek is aan 'beveiligingsinvesteringen' is niet eenduidig af te bakenen. Een eerste afbakening is 'of een investering gerelateerd is aan het wegnemen of opvangen van ongewenste gebeurtenissen', en niet gericht op primaire functionaliteit. Die dualiteit maakt het moeilijk. Beveiliging is geen primair proces maar een ondersteunend, voorwaardenscheppend proces.

Stel, men maakt het mogelijk voor medewerkers om te gaan thuiswerken op basis van secure VPN. Moeten deze investeringen worden beschouwd als beveiligingsinvesteringen, als 'gewone' IT-investeringen of een combinatie van beide? Als er eerst onbeveiligde verbindingen mogelijk waren, en er wordt nu beveiliging aan toegevoegd, dat zou je kunnen verdedigen dat het een beveiligingsinvestering is. Als er echter eerst veilige inbelverbindingen waren en dezelfde veiligheid wordt nu over

een andere transmissievorm – VPN – geboden, dan zou het een gewone IT-investering zijn. Als de karakterisering van de investering afhangt van je vertrekpositie, is het onderscheid kennelijk niet erg fundamenteel. Wat wel relevant is, is dat de bedrijfsdoelstellingen ermee ondersteund worden. Men moet dus wel aan 'de business' uit kunnen leggen waarom een investering nodig of profijtelijk zou zijn.

Beveiliging als profitgenerator vereist een ingerichte, meer volwassen beveiligingsorganisatie

Of neem een firewall. Een deel van de kosten zit in de routingfunctionaliteit, en een ander deel is gericht op het filteren van gewenste/ongewenste activiteiten. Moet dan het verschil in kosten tussen een netwerkdevice met louter routingfunctionaliteit en een firewall als de beveiligingsinvestering worden gezien? Wij zijn van mening dat deze fijnmazige differentiatie niet doelmatig is.

Natuurlijk zijn er wel investeringen die duidelijk beveiligingsinvesteringen zijn: professionele beveiligingsmedewerkers, antivirusprogrammatuur, uitwijkvoorzieningen, RBAC, etc. Indien een investering specifiek is gericht op het voorzien in of het herstellen van vertrouwelijkheid, integriteit en/of beschikbaarheid van informatie en systemen, dan is er sprake van een beveiligingsinvestering.

Controle of auditing wordt in deze definitie dan niet als beveiligingsinvestering gezien. Deze functie geeft inzicht in de opzet, het bestaan of de werking van de beheersingsmaatregelen. Als er al een preventieve werking van uitgaat, dan is deze secondair. Een herstellende werking van controle of auditing is mogelijk, maar indirect als gevolg van correctieve acties. De investeringen betreffen veelal functionaliteit die tevens een effect heeft op beveiliging.

In de beoordeling van investeringsvoorstellen voor beveiliging ligt het accent momenteel eenzijdig op de kosten van beveiliging. Wat onderbelicht wordt, is de opbrengstkant van beveiliging. Beveiliging is uiteraard een *enabler* voor veel IT-diensten. Zo is een e-mailvoorziening zonder antivirusmaatregelen niet werkbaar. Ook is beveiliging een *differentiator* tussen service providers: aanbieders die bijvoorbeeld een certificaat 'Code voor Informatiebeveiliging' hebben, hebben een streepje voor op de concurrentie. Ook beveiligingskeurmerken van 'surf-op-safe' zijn differentiators. Maar wat onderbelicht is, is de mogelijkheid van beveiliging een profitgenerator te maken. Als een aanbieder een basisbeveiligingsniveau als standaard aanbiedt in het dienstenpakket, kan voor alle aanvullende wensen worden gefactureerd. Als bijvoorbeeld in het basisniveau een wekelijkse back-up zit, dan kan daarboven een dagelijkse back-up als extra worden aangeboden. In de markt bestaat bereidheid te betalen voor extra beveiligingsdiensten. Als aanbieder moet je daar op voorbereid zijn: er moet een basisbeveiligingsniveau zijn dat aantoonbaar werkt, en er moeten aanvullende beveiligingsdiensten zijn, die vervolgens per afnemer aantoonbaar moeten werken. Beveiliging als profitgenerator vereist derhalve een ingerichte, meer volwassen beveiligingsorganisatie.

ROSI-rekenmodellen en -casussen

Tot op heden is een beperkt aantal specifieke modellen beschikbaar voor de onderbouwing van investeringen in informatiebeveiliging. In een investeringsbeslissing geldt het uitgangspunt dat de investeringen in maatregelen geringer zijn dan de verliezen als gevolg van beveiligingsincidenten over een zekere tijdsperiode. Als we als tijdsperiode een jaar nemen is het verwachte verlies per jaar (Annual Loss Expectancy of Exposure (ALE)) de optelling van verwachte verliezen als gevolg van incidenten in dat jaar. Voor een incident is het risico op verlies de kans dat het incident zich voordoet en de schade die daarbij optreedt. In formule ([Over06]) voor een incident:

$$R = K \cdot S$$

Risico = Kans · Schade

Voor een jaar geldt dan:

$$ALE = SUM(K \cdot S)$$

Of anders geschreven:

$$ALE = \sum(ARO \cdot SLE) = SUM(ARO \cdot SLE)$$

Hierbij is ARO de Annual Rate of Occurrence van een specifiek incident en SLE de Single Loss Exposure ofwel de schadeverwachting.

Vraag hierbij is natuurlijk op welke wijze ALE voor een bedrijfsspecifieke situatie kan worden bepaald. Laten we beginnen met een model om de mogelijke schade te berekenen. Stel je voor dat binnen een organisatie het systeem dat gebruikt wordt ter ondersteuning van de primaire bedrijfsprocessen als gevolg van een incident buiten gebruik raakt. De schade bestaat mogelijk uit een drietal componenten, namelijk:

- de schade die direct opgelopen wordt als gevolg van beschadigingen aan het systeem;
- de gederfde omzet of verloren productiviteit als gevolg van het niet beschikbaar zijn van het systeem gedurende

een periode. Stel je voor dat honderd medewerkers, met een gemiddeld uurloon van € 20, niet kunnen werken over periode van drie dagen. De verloren productiviteit is dan al gauw (ervan uitgaande dat ze geen andere werkzaamheden kunnen oppakken) € 48.000;
- de kosten die gemaakt moeten worden om de schade te herstellen, bijvoorbeeld aantal manuren.

Wordt dit in een formule beschreven dan is de schade (in het vervolg de gemiddelde schade van een incident (SLE)):

$$SLE = L + A(t) + R(t)$$

Hierbij staat L voor de directe schade, A(t) voor de schade als gevolg van het niet beschikbaar zijn van het systeem gedurende periode t en R(t) voor de kosten (mandagen) die gemaakt zijn om het systeem te herstellen.

Ingevuld in de formule voor ALE ziet dit er als volgt uit:

$$ALE = \sum(ARO \cdot (L + A(t) + R(t)))$$

In de praktijk is het van groot belang dat de beveiligingsmensen leren in de onderbouwing meer aan te sluiten bij de taal van de business. Praat niet over wormen of virussen, maar over verlies van productie. Hierdoor zijn de gevolgen van een incident direct zichtbaar. Om in de taal van de business te kunnen praten is het noodzakelijk om de gevolgen van een incident te kunnen schatten. Zoek uit wat de key performance indicators zijn voor de business, en geef het effect van je beveiligingsinvestering aan op de KPI's van de business. Om de invloed van een incident op de productiviteit te bepalen is het noodzakelijk om kansen op incidenten te schatten. Kengetallen over incidenten zijn onnauwkeurig en accurate inschattingen zijn moeilijk te maken. Toch helpt het als er zicht is op kansen van incidenten, binnen een bandbreedte. De kans op verlies van een laptop is zo'n twee à drie procent per jaar. De gemiddelde kans op brand is eenmaal per tien tot vijftig jaar ([CSI06]). Hoe nauwkeurig moet de schatting zijn? Op basis van voortschrijdend inzicht kan de kansinschatting op een incident, maar evenzo ook de inschatting van het effect van maatregelen, worden verbeterd. Als voorbeeld: tabel 1 geeft een inschatting van de gemiddelde downtime als gevolg van een probleem met betrekking tot de informatievoorziening.

Er zijn diverse methoden voor de onderbouwing van investeringen. Investeringen hebben nut als door de investering de kans op een incident afneemt dan wel de gevolgen van het incident worden verminderd. Voor zich spreekt dat de gedane investeringen niet meer kosten met zich meebrengen dan de kosten als gevolg van incidenten in een jaar, in ieder geval als alleen naar de financiële aspecten wordt gekeken en niet naar andere aspecten zoals een verhoogd gevoel van veiligheid of het voldoen aan wettelijke verplichtingen. In formule

$$K_J < ALE$$

waarbij K_J alle investeringen zijn die in een jaar zijn gedaan.

Een dergelijke vergelijking kan ook over meerdere jaren worden gemaakt. Vraag is waar deze investeringen dan uit bestaan. Drie soorten investeringen kunnen worden onderscheiden:
- kosten (F) die in een tijdsperiode worden gemaakt om bekende kwetsbaarheden te verwijderen in bestaande besturingssystemen;
- investeringen in nieuwe beveiligingsmechanismen (B), denk hierbij bijvoorbeeld aan het aanschaffen van een firewall;
- kosten (M) om de beveiligingsmechanismen te voorzien van de laatste patches, virusdefinities, etc.

De totale investeringen zien er dan als volgt uit ([Mizz05]):

$$K_J = F + B + M$$

Deze kosten kunnen ook onderverdeeld worden in investeringen ($K_{INV} = B$) en jaarlijkse kosten voor onderhoud en beheer ($K_{JAAR} = F + M$).

Om te zien wat de investeringen opleveren kan worden gekeken naar de mate waarin ze de ALE kunnen verminderen. De afname in ALE kan worden uitgedrukt als

Problem	Average downtime (min)
• Application/System related crashes	10
• Email Filtering Sorting & Spam	15
• Bandwidth Efficiency/Throughput	10
• Inefficient/Ineffective Security Policies	10
• Enforcement of Security Policies	10
• System related Rollouts/Upgrades from IT	10
• OS/Application Security Patches	10
• Insecure/Inefficient Network Topology	15
• Viruses/Virus Scanning	10
• Worms	10
• Trojans/Key logging	10
• Spyware/System Trackers	10
• Popup Ads	10
• Hardware/Software Compatibility Issues	15
• Permissions based Security Problems (User/Pass)	15
• File System Disorganization	10
• Corrupt/Inaccessible Data	15
• Hacked/Stolen System Information/ Data	15
• Backup/Restoration	15
• Application Usage Issues	15

Tabel 1. Gemiddelde downtime per probleem ([Sonn02]).

$ALE_{OUD} - ALE_{NIEUW}$. Ingeval de getroffen maatregelen van een investering langer dan een jaar werkzaam zijn, kunnen de kosten over de werkbare periode gespreid worden. Laten we aannemen dat de investering in beveiligingsmaatregelen drie jaar werkzaam is.

In formule:

$$\frac{K_{INV}}{3} + K_{JAAR} < ALE_{OUD} - ALE_{NIEUW}$$

Of:

$$\frac{B}{3} + F + M < ALE_{OUD} - ALE_{NIEUW}$$

In de business case wordt onderzocht of een maatregel rendabel is en worden alternatieven naast elkaar gezet. Zijn er andere mogelijkheden om dezelfde risicoreductie te krijgen of een gewenst niveau te bereiken? Geld voor investeringen moet zo goed mogelijk worden aangewend en dus wordt onderzocht waar de opbrengsten van een investering het hoogst zijn. Wordt een ton geïnvesteerd in bijvoorbeeld een bewustzijnscampagne of in continuïteitsmaatregelen? Of wellicht is men tevreden met een andere mate van risicoreductie waarvoor minder investeringen zijn vereist.

Om een vergelijking te maken tussen investeringen kan gebruik worden gemaakt van ROI of ROSI. ROI betekent Return on Investment. ROSI is Return on *Security* Investment. ROSI is een verbijzondering van ROI. Het bijzondere van ROSI zit deels in het feit dat de baten niet per se opbrengsten zijn, maar ook uit kostenreductie kunnen bestaan, en het feit dat bij ROSI de waardering van meer subjectieve factoren (bewustwording, kans op incidenten) een belangrijkere rol speelt.

Een negatieve ROI hoeft niet per definitie een slechte investering te zijn

ROI is in de bedrijfseconomie de rendementsberekening die de winst als percentage van het geïnvesteerde vermogen uitdrukt. Stel dat er een ROI van twintig procent uit komt. Dat betekent dat op iedere geïnvesteerde euro er € 1,20 wordt verdiend of bespaard. Van belang is hierbij over welke periode wordt gekeken. De periode van de verdienste en de investering moeten gelijk zijn.

Als zoals gezegd RO(S)I wordt gebruikt om investeringen of projecten te vergelijken, dan worden de rendementen van projecten vergeleken. Een ROI van tien procent kan dan nog te laag zijn, omdat er veel projecten zijn met een hogere ROI. Sommige bedrijven gebruiken ook een cut-off-rendement. Een negatieve ROI hoeft niet per definitie een slechte investering te zijn, alleen is er dan een andere onderbouwing dan een bedrijfseconomische.

De definitie van ROI en ROSI is als volgt:

$$ROSI = \frac{Voordelen - Kosten}{Kosten}$$

Ofwel

$$ROSI = \frac{(RiskExposure \cdot \%RiskMitigation) - K_{INV}}{K_{INV}}$$

En met de ALE erbij:

$$ROSI = \frac{(ALE_{OUD} - ALE_{NIEUW}) - K_{INV}}{K_{INV}}$$

In de formules voor ROI en ROSI ontbreekt *de factor tijd*. Zoals gezegd moet bij de berekening van de ROI de investering worden uitgesmeerd over de periode dat de baten worden genoten. Bij ROI worden de voordelen en de kosten altijd over dezelfde periode genomen. Dus als de baten over vijf jaar worden genoten, dan wordt voor de berekening de investering ook over vijf jaar uitgesmeerd. Dat geldt altijd, ongeacht hoe de berekening van de ROI wordt uitgevoerd.

Om dit te illustreren, stel wederom:

K_{INV} = eenmalige investering

K_{JAAR} = kosten per jaar

$ALE_{OUD} - ALE_{NIEUW}$ = baten per jaar

J = aantal jaar dat de baten worden genoten, zonder dat aanvullende investeringen nodig zijn

Als de berekening over de gehele periode wordt genomen, dan volgt:

$$ROSI = \frac{(ALE_{OUD} - ALE_{NIEUW}) \cdot J - K_{INV} - K_{JAAR} \cdot J}{K_{INV} + K_{JAAR} \cdot J}$$

Wordt de berekening over één jaar genomen, dan is de formule:

$$ROSI = \frac{(ALE_{OUD} - ALE_{NIEUW}) - K_{INV}/J - K_{JAAR}}{K_{INV}/J + K_{JAAR}}$$

([Over06])

Deze berekeningswijzen geven uiteraard dezelfde uitkomsten.

De beslissing wordt voor de gehele periode genomen, en dus worden ook de effecten over de gehele periode genomen.

De berekening van de ROI staat dus geheel los van de boekhoudkundige afschrijving. Ook geeft de ROI geen inzicht in het moment waarop de kosten worden gemaakt, bijvoorbeeld alle kosten aan het begin, versus de periode waarover de baten worden genoten. Het kan bijvoorbeeld goed zijn dat een hoge investering in het begin nodig is, die over een lange periode rendeert en een hoge ROI tot gevolg heeft. In verband met de financiering geven veel organisaties in dat geval er de voorkeur aan door lease de investering uit te smeren. Veel organisaties bekijken het effect van een investering op een periode van één jaar, drie jaar of over de periode dat de investering baten oplevert.

Men moet in het achterhoofd houden dat er naast het gebruik van ROSI ook andere methoden worden gehanteerd om een besluit met betrekking tot een investeringsaanvraag te nemen. Bijvoorbeeld:
- in de pas lopen met anderen: benchmarken: vijf tot tien procent van het IT-budget;
- bedrijfseconomisch onderbouwd: zolang de ROI > x%;
- passend bij het beleid van de organisatie of het karakter. Tot een bepaald beveiligingsniveau is bereikt: maximaal aantal incidenten, minimaal niveau beschikbaarheid, voldoen aan bepaalde standaarden, etc.

Het bovenstaande is voornamelijk een theoretische onderbouwing. Op basis van twee voorbeelden willen we ROSI tastbaarder maken.

Voorbeeld 1: Storage Area Network aanleggen
Doel is het waarborgen dat de bedrijfsinformatie altijd beschikbaar is, zodat medewerkers de beschikking hebben over alle informatie om producten te verkopen.
- Implementatiekosten gedeeld door de levensduur in jaren: € 200.000.
- Beheer: € 50.000 per jaar.
- Kosten voor het niet beschikbaar zijn van de gegevens, als gevolg van het ontbreken van beschikbaarheidsmaatregelen, is in casu gederfde omzet omdat geen deals kunnen worden gesloten door het niet beschikbaar zijn van de informatie. Bij een storing in de serverruimte duurt het gemiddeld drie dagen voordat de servers en de daarin opgeslagen informatie weer beschikbaar zijn. Gederfde omzet: € 60.000 per dag.
- Kans dat er een storing is, is naar schatting drie keer per jaar.

ROSI: 3 · (3 · 60.000) – (200.000 + 50.000) / (200.000 + 50.000) = 116%

Terugverdientijd is 250.000 / 540.000 = 0,46.
Dus binnen een half jaar.

Voorbeeld 2: Awarenessprogramma
Er is een budget van X beschikbaar. Aanwending in een awarenessprogramma levert een reductie van het aantal incidenten op van n%, kosten per incident zijn gemiddeld Y. Opbrengst dus: $Aantal_{inc}$ · n% · Y.

Stel:
- Budget is € 100.000.
- Het security-awarenessprogramma reduceert tien procent van een type incidenten gedurende twee jaar (daarna is het awarenessprogramma 'uitgewerkt').
- Een incident kost gemiddeld € 1.000.
- Per jaar 1000 incidenten.

Voordelen: 1000 incidenten / jaar · 10% · 2 jaar · € 1.000 / incident = € 200.000.

Kosten: € 100.000.

ROSI: (Voordelen minus Kosten) / Kosten = 50%.

Wat is de rol van de auditor hierin?

De IT-auditor kan in de discussie over ROSI verschillende rollen spelen. De IT-auditor kan incidenteel een uitspraak doen over het nut van een bepaalde investering. Maar vaak is dat niet goed mogelijk in de beperkte context van zijn opdracht. De auditor kan wel het proces rond de investeringsaanvraag verifiëren en de business case toetsen. Een analyse van ROSI is een goed hulpmiddel.

Ook in relatie tot Cobit 4.0 zijn diverse raakvlakken met ROSI en de rol van de auditor te onderkennen. Dit komt reeds naar voren in de high-level control objectives:
- PO5 manage the IT investments, waarvoor geldt dat investeringscriteria moeten worden bepaald (zoals ROI, netto contante waarde, enz.);
- DS6 identify and allocate costs, waarin wordt gezegd dat IT-kosten moeten worden gemaakt in overeenstemming met goedgekeurde kostenmodellen ([ISAC06]).

ROSI helpt de discussie over investeringsbeslissingen voor beveiliging op een meer volwassen niveau te brengen. De échte argumenten komen op tafel, en subjec-

Bij ROSI komen de échte argumenten op tafel, en worden subjectieve criteria expliciet gemaakt

tieve criteria worden expliciet gemaakt. De auditor kan hierin een stimulerende en toetsende rol vervullen.

Literatuur

[CSI06] CSI/FBI, *Computer Crime and Security Survey*, 2006.

[ISAC06], *IS auditing guideline return on Security investments*, exposure draft, 2006.

[Mizz05] A. Mizzi, *Return on Information Security Investment. Are you spending enough? Are you spending too much?*, januari 2005.

[Over06] P. Overbeek, R. Joosten, A. Jochem, R. Kuiper, A. Moens, J. Popping, P. Ruijgrok en J. Voeten, *Return On Security Investment (ROSI): Hoe te komen tot een bedrijfseconomische onderbouwing van uitgaven op het gebied van informatiebeveiliging?*, GvIB Expert Brief, november 2006, www.gvib.nl.

[Sonn02] W. Sonnenreich, *Return on security investment (ROSI): a practical quantitative model*, 2002.