GvIB Expert Brief – November 2006
ISSN 1872-4876, Jaargang 2 – Nr. 3

November 2006

Return On Security Investment (ROSI): *Hoe te komen tot een bedrijfseconomische onderbouwing van uitgaven op het gebied van informatiebeveiliging?*

Paul Overbeek

Rieks Joosten

Aart Jochem

Renato Kuiper

Alf Moens

Jan Popping

Paul Ruijgrok

Jorg Voeten

Organisaties die investeren in informatietechnologie beseffen inmiddels dat dit gepaard gaat met investeringen in governance, risk management en informatiebeveiliging. De governancestructuur zorgt er voor dat er een risicoinschatting voor de organisatie en de bedrijfsprocessen plaatsvindt, die ten grondslag ligt aan de keuze van maatregelen. Maar zijn de maatregelen effectief te implementeren en leveren de investeringen (kosten) voldoende voordeel (baten) op voor de organisatie ten opzichte van niet of minder beveiligen?

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

Introductie Return on Security Investments (ROSI)

Op de vraag wat security kost en oplevert is vaak geen eenduidig antwoord te geven, ook omdat de waardebepaling van informatie zo lastig is. Wat is de waarde van intellectuele eigendommen en de kennis die in informatiesystemen is opgeslagen en wordt verwerkt? En als er dan iets mis gaat, hoe kwantificeer je imagoschade of aansprakelijkheid? Daarnaast is de realiteit van de aannames die ten grondslag liggen aan de risicoafweging niet altijd eenduidig te bepalen. Tevens is er de vraag in hoeverre de maatregelen een dreiging wegnemen? Wat zijn de kosten van implementatie van maatregelen eigenlijk, en wat zijn de kosten om ze operationeel te houden?
Centrale begrippen voor deze vragen zijn:

- Waarde van informatie;
- Verlies van waarde door een incident;
- Kans op een incident;
- Herstelkosten;
- Kosten van implementatie van maatregelen;
- Kosten om maatregelen operationeel te houden.

De vraag is wat investeringen in informatiebeveiliging opleveren. De vraag naar een bedrijfseconomische onderbouwing werd in de wereld van de informatiebeveiliging tot voor kort nauwelijks gesteld. Investeringsbeslissingen werden genomen op basis van ‘gevoel’, de mening van een autoriteit, en ‘wat doen anderen’. De expertgroep is zich er van bewust dat dit met een analyse van de return-on-investment niet direct zal veranderen, maar dat dit wel kan helpen om de relevante factoren aan te dragen ten behoeve van het beslissingsproces. De expertgroep ondervond grote meerwaarde in de discussie die ontstaat tussen de bedrijfs-economische functie en security management, alsmede in de noodzaak om elkaars denkwereld te begrijpen.

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 risico management 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 klanten.

De deelnemers in deze expertbrief hebben diverse achtergronden: financieel, IT, bedrijfskundig en beveiliging. Maar voorafgaand aan deze discussie hadden de deelnemers wellicht dezelfde scepsis als u nu. Maar zodra de groep met concrete cases aan de slag ging, veranderende de ‘ja maar’-houding, naar een ‘ja, misschien’. En er was nog iets opmerkelijks: veel van de deelnemers zijn gewend om aangesproken te worden op hun expertise en, inderdaad, die individuele professionaliteit. Zodra ROSI een normaal onderdeel wordt van een investeringsproces, raak je als ‘expert’ een stukje van je voetstuk kwijt, en word je meer onderdeel van een gewoon proces. ROSI betekent ook een beetje afscheid van die ‘oprechte sheriff’ die wel weet wat goed voor ons is, en ja, een beetje minder romantiek en meer zakelijkheid in het vak… Professionalisering doet ook een beetje pijn.

Figuur 1 De expertgroep.

Deze brief is geen eindproduct maar een aanzet tot discussie, en is bedoeld als een stap op weg naar verdere professionalisering in het vakgebied.

1. DOELSTELLING

De hoofdvraag is:

Hoe te komen tot een bedrijfseconomische onderbouwing van uitgaven op het gebied van informatiebeveiliging

De vraag is hoe een bedrijfseconomische onderbouwing er uit ziet. De expertgroep is zich er van bewust dat er andere dan bedrijfseconomische redenen voor de verantwoording van de investeringen. Daarom is niet voor alle investeringen een bedrijfseconomische onderbouwing mogelijk of nodig.

2. ONDERBOUWEN VAN INVESTERINGEN

Deze paragraaf schetst de problematiek van het onderbouwen van investeringen in informatiebeveiliging.

Vandaag de dag worden investeringsbeslissingen voor beveiliging veelal genomen op basis van gevoel, een analyse van de directe uitgaven, en het gedrag binnen een peer-groep (wat doen soortgelijke bedrijven). Op grond van subjectieve informatie wordt een beslissing genomen. ROSI helpt om de subjectieve informatie te objectiveren: geobjectiveerde beslissingsondersteunende informatie ten behoeve van een minder subjectieve beslissing.

De bedoeling is binnen een bepaalde context, bijvoorbeeld een specifieke organisatie, investeringsvoorstellen voor beveiliging uniform aan te bieden. Het verdient aanbeveling het standaard investeringsmodel binnen de organisatie zoveel mogelijk te volgen, eventueel aangevuld met een vaste set van meer subjectieve criteria. Dat maakt het mogelijk om voorstellen naast elkaar te zetten. Hoewel nog steeds deels subjectief, kunnen we hiermee investeringsvoorstellen beter vergelijken. De expertgroep stelt voor hier aan te sluiten bij de gangbare methodiek in een organisatie. Wordt, bijvoorbeeld, PRINCE2 gebruikt, dan wordt geadviseerd de structuur van de Business Case of de PID (Project Initiation Document) te volgen (zie voor projectbeheersing de expertbrief over dit onderwerp van begin 2007).

ROSI kan ingezet worden bij investeringsbeslissingen waar geen sprake is van een duidelijke ‘must have’, en wanneer je je niet alleen wilt verlaten op de kunst van het ‘prediken’ dat bij subjectieve voorstellen tot “TellSell”-achtige taferelen leidt.

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 teveel uit aan beveiliging. Incidenten horen er gewoon bij.” Daarbij komt dat de security professional zo min mogelijk incidenten lijkt na te streven. 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 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 gemaakt.

Een veel gehoord 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, en van het IT-budget mag weer een percentage aan beveiliging worden toegewezen. Gartner,

bijvoorbeeld, geeft aan dat het gebruikelijk is dat tussen de 5 en 10% 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.

In de vakliteratuur zijn er niet veel kostenmodellen voor beveiliging beschikbaar. Een bekend kostenmodel is die van de Annual Loss Expectancy (Jaarlijkse Verliesverwachting). Deze is als volgt opgebouwd:

R = K * S

Risico = Kans * Schade

Dit wordt ook uitgedrukt als

ALE = ∑ (ARO * SLE) = SUM (ARO * SLE)

ALE is de Annual Loss Exposure / expectancy
ARO is de Annual Rate of Occurrence van een specifiek incident
SLE is de Single Loss Exposure ofwel de schade-verwachting
ALE = Sommatie over alle incidenten van (Annual Rate of Occurence * Single Loss Exposure)

Ofwel:

ALE = SUM (kans op incident*schade)

De sommatie (SUM) is over alle incidenten per jaar. Schade is uitgedrukt als directe kosten plus herstelkosten.

Merk op dat de ALE eigenlijk over de gehele waardeketen moeten worden berekend. Een beveiligingincident bij het ene bedrijf, veroorzaakt mogelijk ook incidenten bij voorlopende en opvolgende bedrijven in de keten.

> Een bekend voorbeeld is dat van de armlastige grootgrutter die problemen ondervond met de invoering van een nieuw logistiek- en distributiesysteem. Enerzijds werden daardoor bestellingen niet tijdig geplaatst, dat naar de toeleverende bedrijven verstorend werkte en, vanwege de crashacties die vervolgens moesten worden uitgevoerd, kosten verhogend werkte. Anderzijds werden daardoor producten niet uitgeleverd aan de supermarkten die daardoor met lege schappen zaten en minder omzet draaiden.

Een probleem bij dit 'ketendenken' is dat de kosten op de ene plaats in de keten worden gemaakt, en de baten elders worden genoten. In termen van ROSI betekent dit dat de kostprijsverhoging vertaald moet kunnen worden in een hogere verkoopprijs, die door de ketenpartners, klanten, etc., graag wordt betaald. Met andere woorden: de toegevoegde waarde van beveiliging levert een herkenbare service op met een positieve bijdrage aan de winst.

Leveren beveiligingsmaatregelen genoeg op? Dat hangt af van de reductie van de ALE, uitgedrukt als $ALE_{oud} - ALE_{nieuw}$. Als alleen naar de financiële kant gekeken zou worden, dan moeten de jaarlijkse kosten van de maatregelen lager zijn dan de financiële opbrengsten daarvan, te weten de reductie van de ALE. De kosten worden gesplitst in eenmalige investeringen (K_{inv}), en jaarlijkse kosten voor het operationeel houden, K_{jaar}, (beheer, licenties). Laten we aannemen dat de investering in beveiligingsmaatregelen 3 jaar werkzaam is.

In formule:

$$\mathbf{K_{inv}/3 + K_{jaar} < ALE_{oud} - ALE_{nieuw}}$$

Bij het opstellen van een businesscase moet je je altijd afvragen: wat is het alternatief? Zijn er andere mogelijkheden om dezelfde risicoreductie te krijgen of een gewenst niveau te bereiken. Met andere woorden: welke opbrengsten zijn haalbaar als de investering alternatief wordt aangewend? Investeer ik een ton in een bewustzijnscampagne of in continuïteitsmaatregelen?

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 persé 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.
ROI is in de bedrijfseconomie de rendementsberekening die de winst als percentage van het geinvesteerde vermogen uitdrukt. Stel dat er een ROI van 20% uitkomt. Dat betekent dat voor iedere geïnvesteerde Euro er 1.20 Euro wordt 'verdiend' (of bespaard). Van belang is hierbij over welke periode wordt gekeken. De periode van de verdienste en de investering moeten gelijk zijn.

Het is daarbij handig om:

- of 1 jaar te nemen en dus de eenmalige investering K_{inv} over de levensduur J te nemen: $\mathbf{K_{inv} / J}$;
- of de hele levensduur J te nemen, de periode waarover er baten zijn, en dus de baten over die hele periode mee te nemen $\mathbf{(ALE_{oud} - ALE_{nieuw})*J}$;

Bijvoorbeeld:

Stel: investering 1M, baten 1M per jaar, levensduur 2 jaar.

- Berekening 1 jaar:
  (baten – afschrijving)/afschrijving = (1M – 0,5M)/0,5M = 100%
- Berekening over de afschrijvingsperiode:
  (baten * afschrijvingsperiode – investering)/investering =
  (1M*2 – 1M)/1M = 100%

Vaak wordt de ROI gebruikt om verschillende projecten naast elkaar te zetten. Een ROI van 10% 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 persé een slechte investering te zijn, alleen is er dan een andere onderbouwing dan een bedrijfseconomische.
De definitie van ROI en ROSI is als volgt:

$$\mathbf{ROSI = (Voordelen - Kosten) / Kosten}$$

Ofwel

$$\mathbf{ROSI = [\ (RiskExposure * \%RiskMitigation) - K_{inv}\ ] / K_{inv}}$$

En met de ALE er bij:

$$\mathbf{ROSI = [\ (ALE_{oud} - ALE_{nieuw}) - K_{inv}\ )\ ]\ /\ K_{inv}}$$

Tijd: 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 5 jaar worden genoten, dan wordt voor de berekening de investering ook over 5 jaar uitgesmeerd. Dat geldt altijd, ongeacht hoe de berekening van de ROI wordt uitgevoerd.

Om dit te illustreren, stel wederom:

$\mathbf{K_{inv}}$ = Eenmalige investering
$\mathbf{K_{jaar}}$ = Kosten per jaar
$\mathbf{ALE_{oud} - ALE_{nieuw}}$ = 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:

$$\mathbf{ROSI = [\ (ALE_{oud} - ALE_{nieuw})*J - K_{inv} - K_{jaar}*J)\ ]\ /\ [\ K_{inv} + K_{jaar}*J\ ]}$$

Wordt de berekening over 1 jaar genomen, dan is de formule:

$$\mathbf{ROSI = [\ (ALE_{oud} - ALE_{nieuw}) - K_{inv}/J - K_{jaar})\ ]\ /\ [\ K_{inv}/J + K_{jaar}\ ]}$$

Deze berekeningswijze 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.

Investeringen in IT worden meestal in enkele jaren afgeschreven. De factor tijd wordt veel beter meegewogen in de Netto Contante Waarde (NCW of NPV - Net Present Value). Omdat deze berekeningen echter complexer zijn, wordt ROI veel vaker gehanteerd. In 42% van de organisaties die investeringen financieel-economisch onderbouwen, wordt ROI gebruikt. In 19% van de organisaties wordt NCW gebruikt, in 21% IIR (Internal Rate of Return) [bron: ref 8]. Merk op dat het percentage organisaties dat investeringen systematisch onderbouwt sterk stijgt.

Veel security professionals verzuchten wel eens dat er kennelijk incidenten nodig zijn om draagvlak voor investeringen te verkrijgen. De expertgroep is hier geen voorstander van. Bij ‘incident gedreven’-investeringen is de businesscase alleen gebaseerd op impuls en emotie. Het pakket aan maatregelen blijkt dan veelal onevenwichtig te zijn, want het is alleen gericht op het specifieke incident. Mogelijkheden om met een slimmere investering een grotere risicoreductie te verkrijgen, blijven jammerlijk buiten beeld.

Het ontbreekt aan harde cijfers om bijvoorbeeld de effectiviteit van maatregelen te onderbouwen. Er zijn geen goede (statistische) overzichten van wat er allemaal mis gaat. Volgens de expertgroep is dat probleem overkomelijk. Het is goed mogelijk met schattingen te werken, en dan gevoeligheid van de uitkomsten te relateren aan de betrouwbaarheid van die schattingen. Er wordt dan een bandbreedte aangegeven waarbinnen een businesscase betrouwbaar is. Ook is het mogelijk om de businesscase op basis van later verkregen kennis aan te scherpen en kan worden geëvalueerd of de businesscase nog valide is.

3. WAT IS ROI, WAT IS ROSI

Deze paragraaf gaat dieper in op de volgende vragen:

- Wat zijn Security Investments en is er een essentieel verschil met ander investeringen?
- Waarom zou return on *security* investments anders zijn dan een gewone ROI?
- Hebben we te maken met een specifiek begrippenkader?

De eerste vraag is: zijn er specifieke investeringen aan te merken als ‘security investments’. 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 ‘is het gerelateerd aan het wegnemen of opvangen van ongewenste gebeurtenissen’, en niet 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 beschouwd worden 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 er mee ondersteund worden. Je moet dus wel aan “de business” uit kunnen leggen waarom je de investering doet…

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 netwerk device met louter routing functionaliteit (zoals een switch) en een firewall als de beveiligingsinvestering worden gezien? De expertgroep is van mening dat deze fijnmazige differentiatie niet doelmatig is.

Natuurlijk zijn er wel investeringen die duidelijk beveiligingsinvesteringen zijn: professionele beveiligingsmedewerkers, anti-virus programmatuur, uitwijkvoorzieningen, RBAC,.. etc. Indien een investering specifiek is gericht op het voorzien in, of herstellen van vertrouwelijkheid, integriteit en/of beschikbaarheid van informatie en systemen, dan is sprake van een beveiligingsinvestering.
Controle of auditing wordt in deze definitie dan niet als beveiligingsinvestering gezien. Deze functie geeft inzicht in opzet/bestaan/werking van de beheersmaatregelen. Als er al een

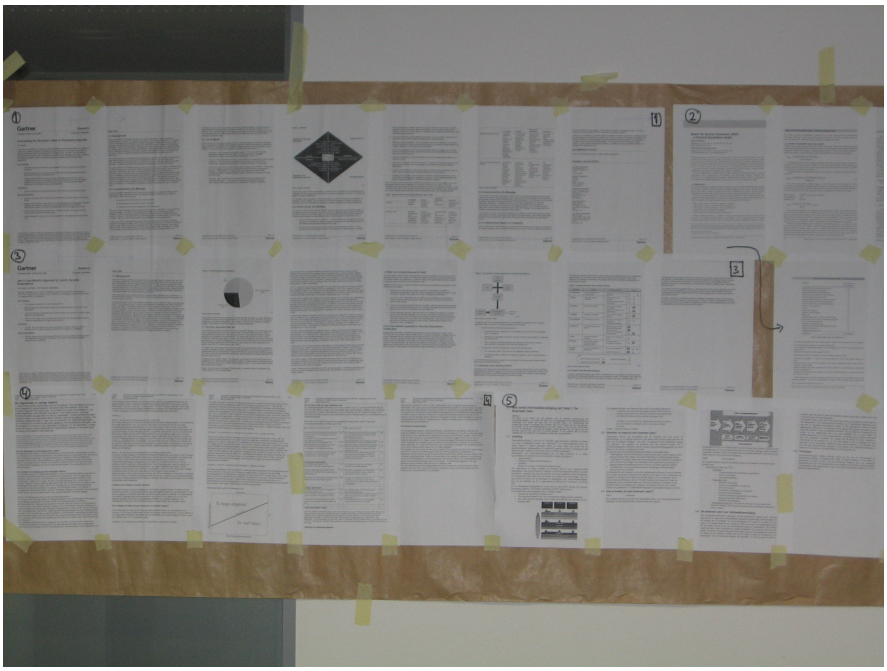
preventieve werking vanuit gaat, dat is deze secondair. Een herstellende werking van controle of auditing is mogelijk, maar indirect als gevolg van correctieve acties.

De expertgroep concludeert dat het niet altijd mogelijk is investeringen eenduidig als beveiligingsinvesteringen aan te merken. De investeringen betreffen veelal functionaliteit die tevens een effect hebben op beveiliging.

Het accent ligt 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 email-voorziening zonder anti-virusmaatregelen 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 profit generator 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 dan per afnemer aantoonbaar moeten werken. Beveiliging als profit generator vereist derhalve een ingerichte, meer volwassen beveiligingsorganisatie (zie hierover de Expertbrief over de organisatie van informatiebeveiliging van begin 2007).

Is dit scenario realistisch? Ja! Een van de grootste telecom-providers ter wereld worstelde lange tijd met het ad hoc karakter van beveiligingsafspraken met haar klanten. Beveiliging kostte, ook vanwege dit ad hoc karakter, alleen maar geld en vereiste te veel en te versplinterde managementaandacht. Deze telecom-provider heeft het roer omgegooid en een information security management proces ingericht alsmede het basisbeveiligingsniveau door de hele organisatie ingevoerd. Daarover wordt zekerheid ('assurance') gegeven middels SAS-70 en Third Party Announcements. Bovendien is deze aanbieder volkomen transparant is de realisatie van KPI's voor beveiliging naar de klanten. Interessant is bovendien dat, nu deze telecom-provider zijn eigen huis op orde heeft, ze ook aan kan bieden klanten te ondersteunen bij het op orde brengen van hun stuk van de verantwoordelijkheden. De telecom-provider heeft hierdoor minder 'specials' en de 'specials' die er zijn, leveren geld op.

Een ROI voor investeringen in beveiliging is niet altijd nodig. Een ROI is niet persé noodzakelijk wanneer er externe of interne wet- en regelgeving is, of als er een overduidelijke consensus in de markt is, of als intern beleid het vereist. In andere gevallen is onderbouwing nodig, en dat blijkt steeds vaker het geval te zijn. ROSI reikt de juiste parameters aan om op te beslissen, en maakt het eenvoudiger om alternatieven naast elkaar te zetten. Voor een deel blijft sprake van subjectiviteit of emotie, maar dat deel wordt wel heel helder en voor de verschillende alternatieven hetzelfde. Er is meer sprake van geobjectiveerde subjectiviteit, of, zo u wilt, gerationaliseerde emoties.



Figuur 2 ROSI input documentatie

4. ONDERBOUWINGSMODEL

Deze paragraaf gaat in op de volgende onderwerpen:

- Welke beslissingscriteria zijn er?
- Hoe ziet een kostenmodel er uit?
- Is benchmarking mogelijk?
- Hoe zijn security-voordelen te kwantificeren?

In het onderbouwingsmodel voor ROSI wordt onderscheid gemaakt naar de kosten- en de opbrengstenkant. Dat levert de volgende beslissingscriteria op:
Kosten:

- Directe investering;
- Instandhoudingskosten (beheer, management);

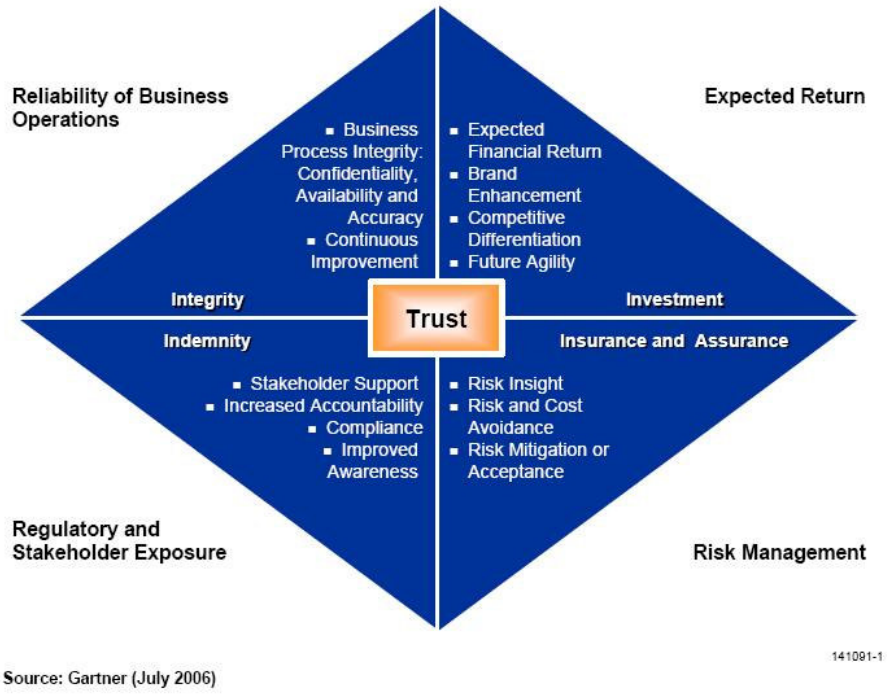
Opbrengsten

- Objectief: hogere verkoop, minder incidenten, minder uitval, minder claims, minder urenverlies, lagere herstelkosten, minder personeel nodig;
- Subjectief: imago, maatschappelijk vertrouwen, politieke impact, verbetering beveiligingscultuur.

Als lezer zult u nu waarschijnlijk denken: hoezo een onderscheid naar subjectief en objectief? De expertgroep is van mening dat er meer posten geobjectiveerd kunnen worden, dan momenteel gebruikelijk is. Dat helpt de discussie op de juiste beslissingscriteria te brengen. Je kunt dan bijvoorbeeld makkelijker investeringsvoorstellen naast elkaar zetten, die hetzelfde doel nastreven. Het ene investeringsvoorstel richt zich dan bijvoorbeeld op preventieve maatregelen met een duurder pakket aan investeringen, maar volledige eliminatie van incidenten, het andere investeringsvoorstel richt zich op het opvangen van incidenten met een goedkoper pakket aan correctieve maatregelen.

De opbrengstenkant kan ook op andere manieren ingedeeld worden. Gartner [bron: ref 1] maakt de volgende 4-I's indeling:

- Investment: besparing, wat levert het op;
- Integrity: verbetering operationele beveiliging;
- Insurance: verzekering van risico-vermindering;
- Indemnity: vrijwaring, met name van wettelijke aansprakelijkheid en verantwoordelijkheid.



Figuur 3 Gartners 4 I-model.

De parameters aan de opbrengstenkant kunnen verder worden gedimensioneerd naar de plaatsen waar 'winst' wordt geboekt. Gartner geeft de volgende parameters:

- Bescherming van merk, product en bedrijfsimago;
- Ondersteuning van de marketing en verkoop;
- Verbeterde beschikbaarheid en responsetijden;
- Verbetering veerkracht en aanpassingsvermogen;
- Verbetering kostenbeheersing;
- Het volgen van trends in de markt;
- Lessons-learned, incidenten uit het verleden;
- Voldoen aan nieuwe wet- en regelgeving

Gebruik 4 I-model voor ROSI

Voor de financiële onderbouwing in ROSI lijkt Indemnity niet geschikt. Investment uiteraard wel, dit levert de onderbouwing voor de te realiseren kostenbesparing bij een gelijkblijvend beveiligingsniveau. Bij Integrity probeer je de baten van verbeterde operationele beveiliging te schatten en af te zetten tegen de investering (zie ook de case 'uitwijkcentrum'; deze wordt beschreven vanuit het Integrity-perspectief). In het Insurance-perspectief wordt de

vermindering van kosten vanwege afname van risico's verwerkt (zie bijvoorbeeld de case 'awareness').

Wat in de praktijk van groot belang is, is dat de beveiligingsmensen leren in de onderbouwing veel meer aan te sluiten bij de taal van de business. Praat niet over wormen of virussen, maar over verlies van productie. 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.

Een ander vermeend probleem bij ROSI is de noodzaak om kansen op incidenten nauwkeurig te moeten kunnen schatten, immers, kengetallen over incidenten zijn onnauwkeurig en beperkt. De expertgroep wil ROSI juist zo opzetten dat de bandbreedtes, voor kansen en kosten van incidenten, waarbinnen een investering zinvol is, helder worden. Duidelijk moet zijn welke aannames zijn gedaan en hoe (on)zeker deze zijn. De doorwerking van de onzekerheid in de resultaten van de ROI wordt zichtbaar in de bandbreedtes van kosten en baten. Deze bandbreedtes zouden twee perspectieven, die dikwijls als conflicterend worden ervaren, bij elkaar brengen. Het eerste perspectief is 'we doen te weinig', gevoed vanuit het risicoperspectief; het tweede perspectief is 'wanneer is het genoeg', gevoed vanuit het investeringsperspectief.

Benchmarking is daarbij een optie: hoeveel problemen zijn er ten opzichte van de concurrentie. Welk gedeelte van de dienstverlening is gecertificeerd. Wat zijn de specifieke investeringen in IT-beveiliging als percentage van het IT-budget (3-5% voor een organisatie met normale risico's).
Toch helpt het als er enig zicht is op kansen van incidenten. Zo weten we dat de kans op verlies van een laptop zo'n 2% per jaar is. We weten ook dat de kans op verlies van een USB-stick 200% is. Kans op brand is tussen de 1 maal per 10 en 50 jaar. Hoe nauwkeurig moet het zijn? De expertgroep stelt voor een classificatie van kansen op incidenten te gebruiken als volgt: gebeurt meerdere malen per dag, dagelijks, wekelijks, maandelijks, jaarlijks, eenmaal per zoveel jaar, nooit.

De besluitvorming rond een investeringsaanvraag kan op verschillende gronden plaatsvinden en zal afhangen van het type organisatie. De expertgroep onderkent tenminste de volgende methoden:

- Methode 1. In de pas lopen met anderen: benchmarken: 5-10% van het IT-budget
- Methode 2. Bedrijfseconomisch onderbouwd: zolang de ROI > x%
- Methode 3. Passend bij het beleid van de organisatie of het karakter: Tot een bepaald beveiligingsniveau is bereikt: maximaal aantal incidenten, minimaal niveau beschikbaarheid, voldoen aan een bepaalde standaarden, etc.

5. ROSI in praktijk

Bij de inbedding van ROSI in de organisatie komen allerlei praktische vragen naar voren.

ROSI inbedden
De eerste vraag is hoe handig gebruik te maken van ROSI. Het is cruciaal om aan te sluiten bij de criteria die door de beslisser(s) worden gehanteerd. Als voor deze besluitvorming processen zijn ingericht, ligt het voor de hand hierbij aan te sluiten en daar ROSI in in te bedden. Aanhaken bij het change-management proces is een optie. Of, als dat er is, aanhaken

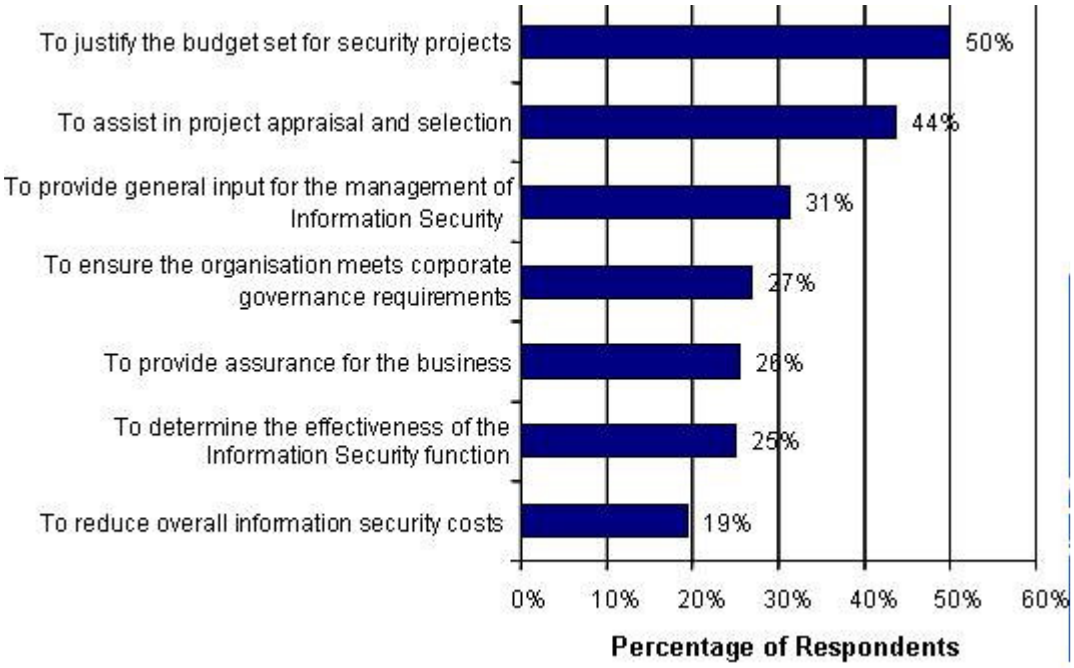
bij het reguliere investeringsproces. Sommige organisaties hebben een vast sjabloon voor het doen van investeringsbeslissingen, bijvoorbeeld door het opstellen van een businesscase. Organisaties die gebruik maken van PRINCE2 hanteren het Project Initiation Document, PID, waarin de businesscase en aanvullende projectinformatie is weergegeven. Vanuit PRINCE2 wordt aanbevolen specifieke onderwerpen in de PID op te nemen. De PID kan worden gebruikt voor IT-gerelateerde beveiligingsinvesteringen.
Het advies van de expertgroep is waar mogelijk de normale procedures voor investeringsvoorstellen in de "information-governance" te volgen, inclusief de daarbij horende formaten en standaarden.

Een veel gehanteerde systematiek is investeringsvoorstellen te voorzien van een classificatie, bijvoorbeeld: nieuw product/service, nieuwe markt, efficiëntie voordeel, regulier onderhoud, intern. De eerst genoemde investeringsvoorstellen hebben in tijden van kostenreductie betere kansen dan investeringen die als 'onderhoud' of 'intern' zijn geclassificeerd.

ROSI in verschillende types van organisaties
De expertgroep is van mening dat voor organisaties die zich in de lagere volwassenheidsfasen bevinden er meer 'must have'-investeringen zijn. Zo ligt het voor de hand eerst de grootste gaten te dichten, zoals back-up, incident-afhandeling en beheer van toegang en vervolgens een basisbeveiligingsniveau, zoals de "Code voor Informatiebeveiliging". Daarna heeft de organisatie een betere grip op de behoefte aan beheersing. Gebruik van ROSI is dan meer voor de hand liggend: kosten en bandbreedtes voor kansen zijn beter bekend.

Een ander onderscheid tussen 'must have' en 'added value'-investeringen hangt samen met de aard van de organisatie en het belang van de informatie. Enkele gedachten:

- Voor overheid/non-profit-organisaties is het aspect 'vertrouwen van de burgers / publieke opinie / maatschappelijke betekenis' van bijzonder belang. Investeringen die daarin ondersteunen, zullen een streepje voor hebben op andere gelijksoortige investeringen. Te overwegen is in het investeringsproces te classificeren naar het effect van de investering, bijvoorbeeld: gericht op de klanten, gericht op interne gebruiker, gericht op beheer,… Of naar beveiligingsaspect: vertrouwelijkheid, integriteit of beschikbaarheid.
- Misschien is voor overheidsorganisaties imago-bescherming, de overheid als betrouwbare partij voor onze informatie, wel eerder een 'must have' dan voor delen van het bedrijfsleven.
- In aansluiting op voorgaande: er zijn organisaties, zoals overheid/non-profit maar ook leveranciers van vertrouwensdiensten of andere 'organisaties van maatschappelijk nut', die een betrouwbaar imago moeten cultiveren. Een incident in de ene uithoek van de organisatie zal invloed hebben op het vertrouwen in de totale organisatie, ook ten aanzien van diensten die bij het incident in het geheel niet betrokken waren. Zo was er een service provider, die betrokken is bij het genereren van digitale handtekeningen, waarbij de website gehacked was. Hoewel het incident geen enkele invloed had op de primaire dienstverlening, was de reactie van het publiek: als de organisatie op dat ene aspect onveilig was, dan zal dat voor andere diensten van de organisatie ook wel gelden. Een discussie over de ROSI voor een specifiek onderdeel van de totale dienstverlening heeft in dit voorbeeld dan ook geen zin. De ROSI moet hier worden bepaald in het licht van het rendement voor de gehele organisatie. Feitelijk betekent een positieve uitslag van de investeringsaanvraag dat het basis niveau van beveiliging wordt opgehoogd.



Figuur 4 ISF: Redenen om ROSI in te zetten.

Zie voor de onderbouwing van beveiligingsinvesteringen ook figuur 4. Hierin zijn de belangrijkste argumenten volgens ISF samengevat [ref2, ref3].

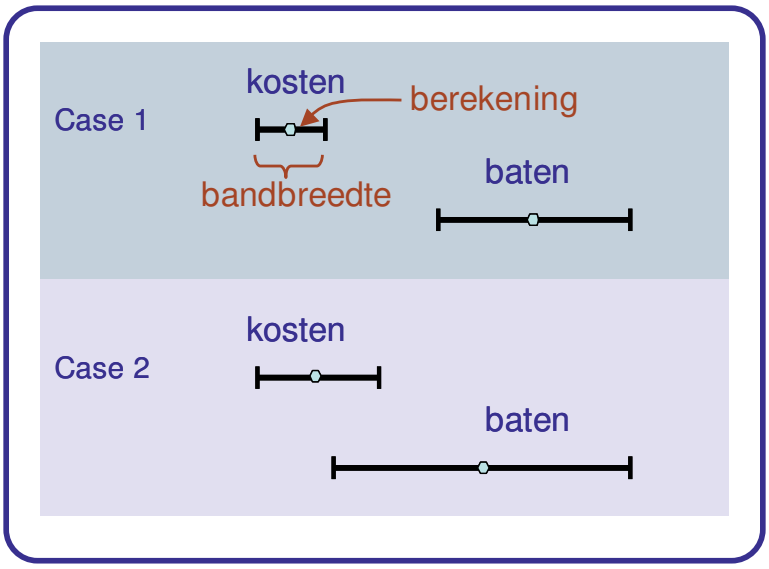
Businesscase & ROSI
Het is aan te bevelen ook bij beveiligingsinvesteringen zoveel mogelijk het traject van de normale businessplanning te volgen. In een businesscase komen doorgaans de volgende aspecten aan de orde:

- Beschrijving van de relevantie voor de business en toegevoegde waarde voor de dienstverlening / de klanten;
- Plaatsing in de strategie van het bedrijf;
- Keuze mogelijkheden: andere (technologische) mogelijkheden en overzicht van onderzochte afgewezen oplossingen;
- Inschatting benodigde middelen (voor de verschillende mogelijkheden);
- Schets van het projectplan;
- Risico's gepaard gaande met de investering;
- Overzicht financiële kosten en opbrengsten.

In de eerste twee punten is ruimte voor meer subjectieve parameters. In het laatste punt komt de ROI, bij beveiligingsinvesteringen de ROSI, naar voren. De definitie van ROI en ROSI is als volgt:

ROI = (Voordelen minus Kosten) / Kosten

De ROI wordt bepaald over een specifieke periode, meestal een jaar. Merk op dat in ROSI alleen variabelen naar voren komen die bedrijfseconomisch te waarderen zijn. Aangezien die variabelen veelal een element van risicoschatting in zich hebben, wordt gewerkt met bandbreedtes.



Figuur 5 Twee cases waarvoor de onzekerheden en risico's zijn aangegeven als een bandbreedte in de kosten en baten van de ROI. Case 1 laat geen twijfel over, case 2 des te meer.

In de cases worden verschillende voorbeelden uitgewerkt. De expertgroep ondervond dat het opstellen van de ROSI dwingt onderscheid te maken tussen objectieve en subjectieve criteria, en zo de zekerheden en onzekerheden duidelijk bloot legt. De échte besliscriteria worden helder. Er zijn verschillende types businesscases. Daar waar het kan, helpt ROSI inzicht te verschaffen in de 'knoppen' waaraan kan worden gedraaid: ROSI zorg voor een meer zakelijke discussie en afweging van alle mogelijkheden als voorbereiding van een investeringsbeslissing

6. Hoe verder - hoe goed is ROSI?

Een onderscheid tussen ROSI en ROI is dat de opbrengstenkant van ROSI zich achteraf niet of moeilijk laat meten. Voor het overige kan de realisatie van de ROSI zich op de zelfde wijze laten meten als de ROI. De discussie over hoe de ROSI achteraf te valideren is, is overigens nu niet aan de orde. Er moet eerst praktijk ervaring mee worden opgedaan.

Een ander punt is wat de randvoorwaarden zijn om ROSI effectief te implementeren. Er moet binnen de organisatie wel enige basis voor beheersing zijn. De expertgroep heeft een vereenvoudigd groeifasenmodel voor beveiliging als uitgangspunt genomen waarin de volgende fases zijn onderkend: onbeheerst, technologie-georienteerd, beheerst, service-georienteerd, klant-georienteerd, markt-georienteerd [ref 7]. In een onbeheerste situatie is het gebruik van ROSI even zinvol als het gebruik van een lancet in een slachthuis. In de 'technologie-georiënteerde'-fase, waarin investeringen op ad hoc basis naar aanleiding van incidenten worden gedaan, is het gebruik van ROSI niet zinvol. In de 'beheerste fase' kan ROSI een zinvolle onderbouwing geven bij het opstellen van het basis beveiligingsniveau, maar in die fase wordt toch voornamelijk gekeken naar 'wat te doen gebruikelijk is' of wat standaarden voorschrijven. Vanaf de service-georiënteerde fase acht de expertgroep de inzet van ROSI nuttig. De expertgroep adviseert om eerst ROSI als methode te gebruiken. Bij een voortgezette professionalisering van de security processen kan dan overwogen worden een andere methode, bijvoorbeeld NCW, als uitgangspunt te nemen.

ROSI heeft het beste effect als de security professional in staat is zijn de boodschap aan te laten sluiten bij de belevingswereld van de beslissers. Security professionals zouden zich hierin kunnen scholen dan wel zich in de praktijk door andere (financiële) deskundigen laten bijstaan.
ROSI is relevant omdat dit past in de verdere professionalisering van beveiliging, risico-analyse en compliance. Informatie en IT zijn belangrijke productiemiddelen, waar een normale bedrijfseconomische discussie op van toepassing moet zijn.

De expertgroep heeft een aantal cases aangedragen die ROSI meer tastbaar maken. De expertgroep zou graag deze cases verder willen aanscherpen, en is op zoek naar andere cases die het gebruik van ROSI illustreren.

Stellingen en adviezen:

- ROSI dwingt de ICT-functie de investeringen in businesstermen te onderbouwen. Security is uiteindelijk een business beslissing;
- In de businesscase: Wees niet bang voor onzekerheid maar maak deze expliciet. Toets de businesscase op de onzekerheden in je cijfermateriaal. Probeer ratio en gevoel te scheiden, maar wel in balans te houden;
- Standaardiseer het formaat voor businesscases, zodat ze eenvoudiger te vergelijken zijn;
- ROSI is een hulpmiddel om de discussie over de juiste parameters te krijgen;
- Andere methoden, zoals Netto-Contante waarde, kunnen ook geschikt zijn, bijvoorbeeld als deze methode beter is geaccepteerd in de organisatie;
- Elk kostenmodel is (alleen) geschikt in zijn context
- Laat beveiligingsinvesteringen zoveel mogelijk meeliften met andere investeringen onder het motto ‘more secure with every change’.
- Fouten worden duur betaald.

CASES

Case 1: Invoeren security architectuur:
Er is een investeringsvoorstel om een security architectuur in te voeren. Doelstelling is een reductie in kosten.
Stel, het invoeren van een security architectuur kost X miljoen Euro en blijft 4 jaar effectief.
We negeren zaken als reductie van beheersinspanningen en verhoging licentiekosten.

We berekenen ROSI als volgt:
Kosten/opbrengsten:

- De eenmalige investering X_{inv}.
- Verschil in ALE: R_{ale}

ROSI:

- $(4*R_{ale} - X_{inv}) / X_{inv} = ROSI$

Stel:

- X_{inv} = 2 M eur;
- R_{ale} = 1000 incidenten minder á EUR 1000 = 1 M Euro per jaar.
- ROSI = (4*1 – 2) / 2 = 100%

De terugverdientijd is 2 jaar: X_{inv} / R_{ale} per jaar = 2M / 1M = 2 jaar. De terugverdientijd is dus niet hetzelfde als ROSI.

Case 2: Investering in een Intrusion Detection System
Stel, een IDS kost X_{inv} per jaar, inclusief beheer. Per jaar worden Y intrusions gedetecteerd. Dat is X/Y per intrusion. Niet-ontdekte intrusions kosten Z.

Indien X/Y – Z positief is, dan is deze investering gerechtvaardigd.

De ROI is hier dus: (Z-X/Y)/(X/Y).

In dit geval is het interessant hoe de indringers hierop gaan reageren. Mogelijk vinden zij weer manieren om de IDS te omzeilen en is de investering ogenschijnlijk teniet gedaan.

Case 3: 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: $Aantal_{inc}$*nn%*Y.

Stel:

- Budget is 100.000 EUR
- Het security awareness programma reduceert 10% van een type incidenten gedurende 2 jaar (daarna is het awareness programma ‘uitgewerkt’).
- Een incident kost gemiddeld 1000 EUR.
- Per jaar 1000 incidenten.

Voordelen: 1000 incidenten/jaar * 10% * 2 jaar * 1000 EUR/incident = Eur 200.000
Kosten: EUR 100.000
ROSI: (Voordelen minus Kosten) / Kosten = 50%.

Vragen opdrachtgever:

- Wat zijn de bandbreedtes?
- Hoe reëel zijn die kosten per incident – waardoor worden die veroorzaakt?
- Hoe gaan we verzekeren dat we de voordelen gaan incasseren
- Hoe kom je aan 10% vermindering van een type incidenten?
- Neemt het rendement nog verder toe als we meer investeren.

Twee gesprek tussen opdrachtgever (OG) en beveiligingadviseur (BA) n.a.v. case 3:

- OG: Hoe weet je dat er 1000 incidenten per jaar minder zijn?
- BA: Afgelopen jaar zijn er 2000 incidenten geweest door onoplettendheid van medewerkers. We gaan ervan uit dat we de helft kunnen voorkomen. Zelfs al lukt het maar in 500 gevallen, dan bereiken we al het brake-even-point.
- OG: Hoe kom je aan die EUR 1000 per incident?
- BA: We hebben dat gemeten. Het zijn alleen de directe kosten, de arbeidsuren die nodig zijn om het incident te herstellen. Waarschijnlijk liggen de echte kosten dus nog hoger.
- OG: Hoe ga je ervoor zorgen dat we de besparingen daadwerkelijk realiseren?
- BA: Het herstellen van de incidenten gebeurt voor een deel door extern ingehuurde mensen. We kunnen van één van hen het contract opzeggen.
- OG: 50% rendement klinkt heel goed. Kunnen we met extra investeringen nog meer besparingen halen?
- BA: Als we over een jaar nog een herhalingscampagne doen, zal het effect mogelijk nog een jaar langer beklijven.

Case 4: Uitwijkcentrum (huur)
Inrichting: eenmalig 600 K (afschrijven over 3 jaar)
Huur en oefening: 200K (per jaar)
Interne kosten: 400 K (per jaar)
Baten: hersteltijd na verlies productiefaciliteit van 1 maand naar 1 dag
Kosten incident: 1 maand verlies van productie betekent dat het bedrijf failliet gaat.
Kans: eenmaal per 50 jaar

We nemen een periode van 3 jaar om de eenmalige kosten af te schrijven.
Kosten per jaar = 200.000 + 400.000 + 600.000/3 = 800.000
Stel, de omzet van het bedrijf is 10 miljoen, de beurswaarde is 15 miljoen EUR. Na het genoemde incident is de bedrijfswaarde Nihil. Het verlies is dus 15 miljoen Eur.
Per jaar is er een 2% kans dat het incident optreedt. ALE = Verwachte verlies als gevolg van de calamiteit is 2% van 15 miljoen EUR = 300K. De verwachting is dus dat we per jaar 800K aan kosten maken om 300K te besparen.
Niet doen?

Neem nu aan dat de omzet 30 miljoen is, en de beurswaarde 45 miljoen Eur. Per jaar is er een 2% kans dat het incident optreedt. ALE = Verwachte verlies als gevolg van de calamiteit is 2% van 45 miljoen EUR = 900K. De verwachting is dus dat we per jaar 800K aan kosten maken om 900K te besparen.
Meteen doen?

Beslisser:

- Een voordelig scenario bij een lage omzet (15 miljoen) is niets doen en bij een calamiteit de voorraden te verkopen en het bedrijf failliet te laten gaan.
- Wat als ik nou een voordeliger uitwijkscenario kies, en bijvoorbeeld genoegen neem met een maximale uitvalduur van drie dagen?
- Als mijn omzet stijgt bij gelijkblijvende kosten is er kennelijk een moment waarop een uitwijkvoorziening bedrijfseconomisch gerechtvaardigd is. Vanaf welke omzet is dat het geval?
- Zijn er andere maatregelen te nemen die de kans van 2% per jaar verminderen?

Case 5: Anti-virus programmatuur
Kosten per jaar: 200 EUR per werkplek.
Kosten verhelpen virus-besmetting: 1000 Eur per werkplek per keer
Verwacht aantal besmettingen zonder anti-virus programmatuur: 10 keer per jaar

ROSI: 10.000 - 200 / 200 = 4900%

Case 6: Storage Area Network aanleggen.
Doel is het waarborgen dat de bedrijfsinformatie altijd beschikbaar is, zodat medewerkers beschikking hebben over alle informatie om producten te verkopen.

- Implementatiekosten gedeeld door de levensduur in jaren: EUR 200.000
- Beheer EUR 50.000 per jaar.
- Kosten voor het niet beschikbaar zijn van de gegevens, als gevolg van ontbreken 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 3 dagen voordat de servers en daarin opgeslagen informatie weer beschikbaar is. Gederfde omzet 60.000 EUR per dag.
- Kans dat er een storing is, is naar schatting 3 keer per jaar.

ROSI: (3* (3*60.000)- (200.000+50.000)/ (200.000+ 50.000) = 116 %

LITERATUURLIJST

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

1. Articulating the Business Value of Information Security, Tom Scholtz., G00141091, 21 July 2006;
2. ISF –ROSI: Return on Security Investment- key findings presentation, july 2005;
3. ISF –ROSI: Return on Security Investment – Workshop report, july 2005;
4. The value of teaching and learning technology: Beyond ROSI, EDUcause quarterly, Jonathan D. Mott, Garin Granata, number 2, 2006;
5. Use a Cost-Benefit Approach to Justify Security Expenditure, Tom Scholtz, Jay Heiser, John Pescatore, Rich Mogull, G00136436, 30 November 2005;
6. Wat levert security op?, Thom Schiltmans, Informatiebeveiliging nummer 8, 2006;
7. Strategie voor de inrichting van riskmanagement: bouwen aan de piramide, P. Overbeek, VERA NIVRA NOREA-congres Update on ICT & Control(e), mei 2005;
8. bron: 2006 CSI/FBI Computer Crime and Security Survey;
9. KPN Integrated Compliance Framework: Living Effective and Demonstrable Compliance efficiently, Rieks Joosten (TNO), Jorg Voeten (KPMG).

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.

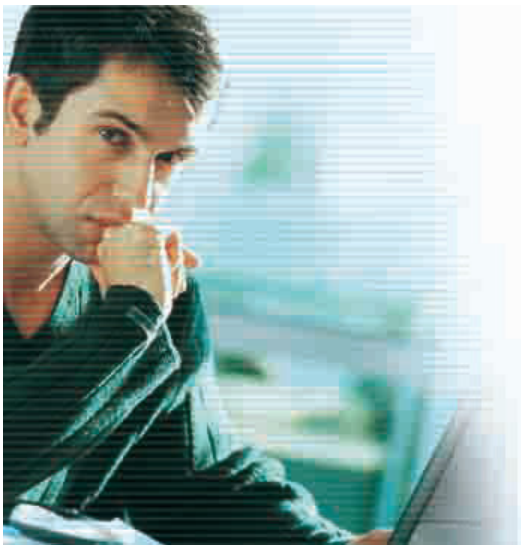
- Bij hergebruik of verspreiding dient de gebruiker de licentievoorwaarden van dit werk kenbaar te maken aan derden.
- De gebruiker mag uitsluitend afstand doen van een of meerdere van deze voorwaarden met voorafgaande toestemming van de rechthebbende.

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