# ADVANCED BUSINESS IMPACT ANALYSIS

## Verbeterd risico-management door gerichte impactbepaling

Alle bedrijven lopen risico's, waardoor er een kans bestaat dat bedrijven hun verplichtingen naar hun stakeholders - zoals klanten of aandeelhouders - niet meer kunnen nakomen en daardoor zelf schade leiden. Het is dus van vitaal belang dat bedrijven de relevante risico's identificeren en vervolgens managen. De stap in het risicomanagementproces waarin de impact van een bepaalde dreiging op het behalen van business doelstellingen wordt bepaald is de Business Impact Analysis (BIA). Aan de BIA zoals die tegenwoordig in de meeste organisaties wordt uitgevoerd kan nog veel verbeterd worden. Dat is de conclusie van een aantal interviews en een expertsessie met verscheidene information-security-consultants met meerjarige ervaring in het ondersteunen van organisaties met het uitvoeren van BIA's. De geconstateerde tekortkomingen resulteren in mogelijk onjuist ingeschatte impacts van cyberdreigingen, met het gevaar dat enerzijds werkelijk relevante risico's over het hoofd worden gezien en anderzijds het risico wordt gelopen om te investeren in onnodige veiligheidsmaatregelen.

In deel 1 van dit artikel benoemen we de geconstateerde onvolkomenheden. In deel 2 zullen we een aantal mogelijke verbeterpunten bespreken voor zowel de korte, als de wat langere termijn.

## Business Impact Analyse

Cyberincidenten kunnen een grote impact hebben op bedrijven. In 2013 werd een aantal gerenommeerde banken en bedrijven getroffen door Distributed Denial of Service (DDoS) aanvallen die gedurende enkele dagen het nieuws beheersten en hebben gezorgd voor veel onrust onder klanten. Voor bedrijven kunnen cyberincidenten een directe bedreiging zijn voor het voortbestaan van de onderneming, zoals bij DigiNotar. Bescherming tegen cyberdreiging en het kunnen afslaan van aanvallen is daarom erg belangrijk. Maar het nemen van mitigerende en defensieve maatregelen kost geld en andere resources. Om goed te kunnen onderbouwen welke maatregelen tegen welke risico's het beste genomen kunnen worden – en daarbij de investering waard zijn – moet er inzicht zijn in het effect van cyberincidenten en -dreigingen. Daarbij spelen vragen een rol als: Wat is het gevolg van cyberincidenten voor het bedrijf? Zorgt een veelvuldige DDoS aanval ervoor dat klanten naar de concurrent gaan? Wat doet verlies van klantgegevens met het imago van het bedrijf?
Het bepalen van de impact van een dreiging voor een organisatie, dat wil zeggen de totale schade die een organisatie naar verwachting oploopt als die dreiging ook werkelijk plaats vindt, is van belang omdat die schades altijd betrekking hebben op het niet of onvoldoende verwezenlijken van de - grotere of kleinere - doelstellingen van die organisatie, en dus diens succes mede bepalen.
De activiteit waarbij de (maximaal) te verwachten schades worden ingeschat voor een zekere organisatie met een zeker dreigingsprofiel, heet een Business Impact Analyse (BIA). Op basis van deze inschattingen bepaalt het management welke schade in het geval van optreden onacceptabel groot is en dus actie vereist.
Aan het uitvoeren van de BIA zoals die tegenwoordig in veel organisaties wordt uitgevoerd kan in onze ogen nog veel verbeterd worden.

## De context: IT-risicomanagement

Het globale risicomanagement(RM)-proces voor organisaties met IT-systemen staat beschreven in standaarden zoals de ISO 31000:2009 (Risk Management – Principles and Guidelines) en ISO 27005: 2008 (Information Security Risk Management).
Voor de BIA en Risk Assessment (RA) wordt echter nog vaak teruggegrepen op de traditionelere werkwijze - mogelijk omdat die bekend is c.q. al jaren gebruikt wordt - die (nog) terug te vinden is in de NIST SP 800-30. Deze traditionele BIA/RA richt zich op het identificeren van kwetsbaarheden en dreigingen van de IT-infrastructuur die door bedrijven wordt gebruikt om hun verplichtingen na te kunnen komen, en de hoogte van de impact die deze dreigingen zouden veroorzaken in het geval van optreden. Dat is gebaseerd op definities van 'Risk' zoals die staan in de NIST SP 800-30: "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." Hier ontbreekt dus de relatie naar de bedrijfsdoelstellingen zoals die tegenwoordig door ISO wel expliciet wordt gelegd.
Zulke definities leggen naar onze mening een zodanige nadruk op dreigingen en kwetsbaarheden dat het doel waar het allemaal om gaat, namelijk de onzekerheden in het halen van de bedrijfsdoelstellingen tot een acceptabel niveau reduceren, vaak uit het oog wordt verloren. Dit verklaart ook waarom veel Chief Information Security Officers (CISO's) er nog steeds veel moeite mee hebben om security op bestuurlijk niveau aan te kaarten: de directie is doorgaans niet geïnteresseerd in dreigingen en kwetsbaarheden, maar veel meer in wat dit voor de bedrijfsdoelstellingen betekent, welke impact het op bedrijf en bedrijfsvoering heeft, en welke schade ze kunnen veroorzaken. Waar deze link niet of onvoldoende wordt gelegd, zal informatiebeveiliging een ondergeschoven kindje blijven.

## Inschatten van Business Impact en Risico's

Hoe goed een organisatie zich tegen risico's heeft gewapend staat of valt met hoe de risicoanalyse wordt uitgevoerd. Een belangrijke stap bij het uitvoeren van een risicoanalyse is het inschatten van de impact en dreigingsrisico's om inzicht te verkrijgen in welke security-incidenten de grootste gevolgen (impact) voor de business kunnen hebben. Omdat men over het algemeen een beperkt budget heeft voor beveiligingsmaatregelen, worden de vervolgstappen van risicoanalyse vaak alleen uitgevoerd voor scenario's die tot hoge schade zullen leiden. Als de impact van bepaalde dreigingen wordt onderschat, zullen er tegen die dreigingen

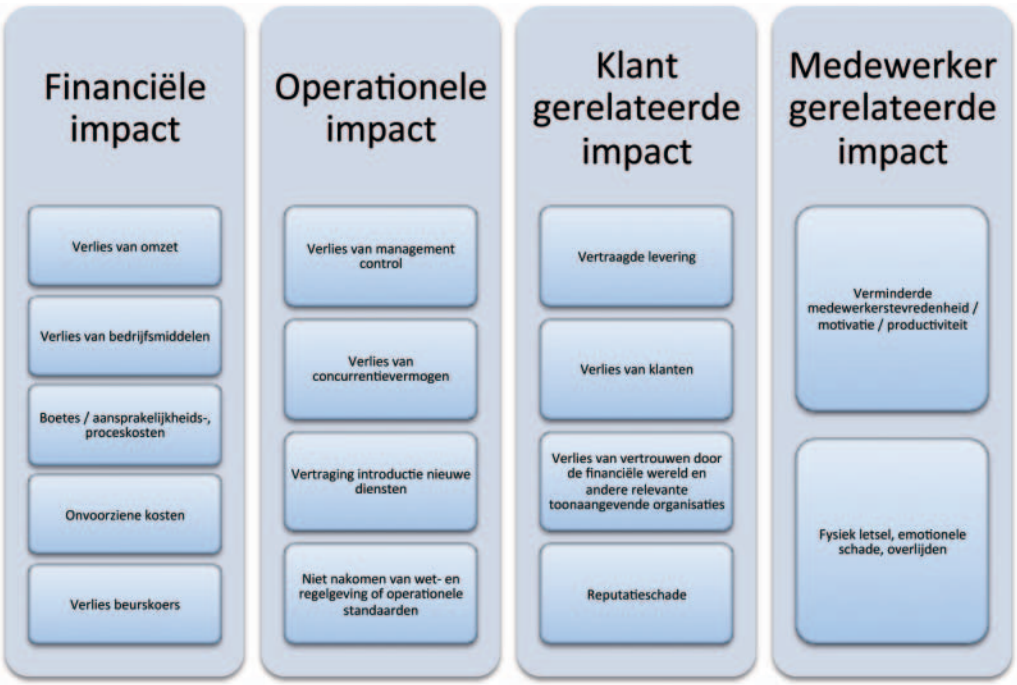
*Milena Janic promoveerde aan de Technische Universiteit Delft, op het gebied van performance van informatie- en communicatienetwerken en diensten. Zij werkt als consultant en onderzoekster bij de expertisegroep Information Security van TNO. Haar focus ligt op onderzoek en consultancy op het gebied van risicomanagement, identity- en access-management en privacy gerelateerde vraagstukken.*

geen maatregelen getroffen worden, hetgeen kan leiden tot potentieel hoge schade bij het toch optreden ervan. Ook overschatte impact leidt tot inefficiëntie, daar de onnodige maatregelen geïmplementeerd zullen worden en zo onnodige kosten introduceren. Vanwege dit belang zullen we wat dieper ingaan op hoe de impactinschattingen traditioneel worden uitgevoerd.

Gebaseerd op literatuurstudie en gesprekken met experts, concluderen wij dat - binnen de diversiteit aan bestaande methoden - de methodieken voor het uitvoeren van een impact- of risico-inschatting er in hoofdlijnen hetzelfde uitzien. Het doel is om voor een gegeven veiligheidsincident (-scenario) de impact op de business te bepalen. Een veel gebruikt middel om een schatting hiervan te kunnen maken, zijn expertmeningen. Deze worden uitgevraagd in een workshop, interviews, of enquêtes.

Om dit te illustreren gaan we uitgebreider in op de door het Information Security Forum (ISF) voorgestelde methodiek die de bedrijven die lid zijn van ISF gebruiken voor het uitvoeren van risicoanalyses. De Business Impact Analysis Assistant van ISF wordt uitgevoerd voor elke gedefinieerde scope binnen een organisatie. Deze BIA bestaat uit een van tevoren vastgelegde en in Excel gevatte vragenlijst die - meestal in een workshop - door degene die voor die scope verantwoordelijk is beantwoord dient te worden. In deze methodiek worden er voor verschillende processen en bedrijfsmiddelen binnen deze scope verschillende worst-case scenario's geïdentificeerd, die tot compromitteren van vertrouwelijkheid, integriteit of beschikbaarheid van informatie kunnen leiden. Vervolgens wordt er aan de hand van de vastgelegde vragen, behorende tot verschillende categorieën zoals operationeel, financieel, klant, of medewerker-gerelateerd, de impact van het optreden van deze scenario's op de business ingeschat. De vragenlijst is in principe generiek van aard, hoewel de organisaties zelf een versie kunnen opstellen die is aangepast op eigen doelstellingen en behoeftes. Voor scenario's en impact types die hoog en zeer hoog scoren worden workshops gehouden om de dreigingen te identificeren die tot deze scenario's leiden, en de kans van hun optreden in te schatten, zodat de totale risicowaarde bepaald kan worden.

In de ISF methodiek wordt uitgegaan van 15 impactsoorten, Business Impact Types (BIT) genoemd. Deze zijn weergegeven in Figuur 1. Voor elke impactsoort dient van tevoren de norm voor classificatie van impact te worden vastgesteld. Dit betekent dat wordt aangegeven voor welke waarderanges de impact als respectievelijk zeer hoog, hoog, middel, laag en zeer laag gekwalificeerd kan worden. Voor elk van de BITs wordt daarna ingeschat hoe hoog op de schaal van zeer hoog tot zeer laag de impact zou zijn bij het optreden van een geïdentificeerd worst-case scenario.




Figuur 1 - Business Impact Types zoals onderscheiden in de ISF methodiek

## Huidige BIA-knelpunten

In een expertsessie met security-consultants met meerjarige ervaring met het uitvoeren van BIA's in het algemeen, en de ISF-methodiek in het bijzonder, zijn de BIA als generieke processtap en de vragenlijst zoals het onderdeel van ISF, onder de loep genomen. Geconcludeerd kan worden dat de BIA zoals die nu wordt uitgevoerd een aantal belangrijke tekortkomingen kent, die we hierna bespreken.

## Tekortkomingen in scope-bepaling

Zowel ISO 27001 als ISO 31000 schrijven voor dat aan het begin van het risicomanagement proces een afbakening dient plaats te vinden van het gebied waarbinnen de risico's worden gemanaged: de scopebepaling. Deze standaarden geven echter geen richtlijnen over hoe de scopes bepaald dienen te worden. Het lijkt er overigens op dat in de ISO 27005 die nu wordt gereviseerd, uitdrukkelijk(er) aandacht aan dit probleem geschonken gaat worden, maar vooralsnog wordt impliciet verondersteld dat de meeste organisaties goed weten hoe men deze afbakening moet uitvoeren. De praktijk wijst uit dat er behoefte is aan een betere scope bepaling. Dit uit zich in een aantal aspecten:

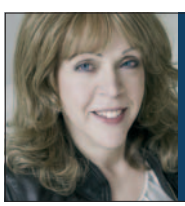
## Gebrek aan aansluiting bij de belangen van hogere organisatieniveaus (verticale afhankelijkheden)

De BIA-vragen worden beantwoord door of namens degene die voor een bepaalde scope verantwoordelijk is. In praktijk is dat meestal een dienst- of systeemverantwoordelijke. Niet zelden ontbreekt bij deze persoon echter het inzicht in wat op bestuurlijk niveau als relevante risico's wordt gezien. Op bestuurlijk niveau wordt vaak gesproken in termen van financiële bedrijfscontinuïteit, maar deze doelstellingen en daarmee gepaarde risico's worden vaak niet doorvertaald naar doelstellingen en targets van de scope-verantwoordelijke die de BIA uitvoert. Hierdoor kan het voor komen dat de ernst van het optreden van bepaalde scenario's wordt onderschat, waardoor de daarmee gepaarde risico's ongemitigeerd blijven. Anderzijds kan de impact van scenario's onterecht worden overschat, waardoor onnodige maatregelen getroffen worden voor risico's die er eigenlijk niet zo toe doen. Hierdoor worden onnodige kosten gemaakt. Er is gebrek aan inzicht in de afhankelijkheden tussen scopes (horizontale afhankelijkheden)
Doordat de scope van een BIA meestal beperkt wordt tot bijvoorbeeld een dienst, kan het voorkomen dat het optreden van een bepaald scenario wel enige, maar geen significante impact op de dienst in scope heeft. Daardoor zou zo'n scenario in daar op volgende risicoanalyses buiten beschouwing worden gelaten. Het is echter voorstelbaar dat het optreden van datzelfde scenario ook gevolgen kan hebben op business doelstellingen van andere diensten, doordat bijvoorbeeld hetzelfde systeem wordt getroffen, maar eveneens beperkt qua omvang, waardoor het ook in het resultaat en opvolging van de BIAs van die andere diensten niet wordt opgenomen. Door de scope van de BIA te bepalen zoals het momenteel wordt gedaan, kan het voorkomen dat scenario's over het hoofd worden gezien, en wel die scenario's die op elke individuele dienst beperkte impact hebben, maar door een cumulatief effect wel een significante impact hebben op de bedrijfsvoering van de organisatie als geheel.

## Tekortkoming met betrekking tot welke situaties te analyseren

*Ambiguïteit ten aanzien van worst-case-scenario.*

- Eerder is aangegeven dat de beantwoording van de vragen gedaan wordt voor het geval van het optreden van een worst-case-scenario. Er bestaan echter geen richtlijnen omtrent het definiëren van een worst-case. Dient de BIA te worden gedaan voor een absolute worst-case, waarvan de kans van optreden buitengewoon gering is zoals bijvoorbeeld dat alle systemen niet beschikbaar zijn voor een aanzienlijke tijdsperiode, zoals een week? Of dient de BIA uitgevoerd te worden in de context van een realistische worst-case, bijvoorbeeld op basis van karakteristieken van incidenten die in het verleden plaatsvonden?
- Bij inschatting van impacts wordt een aantal dimensies die de omvang van de impact bepalen niet expliciet aangegeven en meegenomen, zoals bijvoorbeeld de omvang van de incident, tijdsduur en andere karakteristieken van het incident. Zo is bijvoorbeeld de impact op de gezondheid van medewerkers afhankelijk van karakteristieken van incidenten, hoeveel systemen getroffen zijn, de tijdsduur daarvan, maar natuurlijk ook de aard van de mensen zelf. Met name bij de impactbepaling van incidenten die leiden tot verminderde vertrouwelijkheid en integriteit van informatie wordt niet gekeken naar de omvang en de duur van het incident.



*Eldine Verweij is als kwantitatief bedrijfseconoom afgestudeerd aan de Erasmus Universiteit Rotterdam en werkt als consultant en onderzoekster bij de expertisegroep Strategic Business Analysis van TNO. Haar focus ligt op onderzoek en consultancy met betrekking tot de economics van cybersecurity en kosteneffectiviteitsafwegingen binnen de informatiebeveiliging.*


- Bij de schatting van impact van niet beschikbaarheid van informatie wordt doorgaans wel nagedacht over de duur en de reikwijdte van het incident. Maar helaas wordt deze vraag ook vaak verkeerd geïnterpreteerd. De vraag wordt beantwoord, ervan uitgaande dat de dienst niet beschikbaar is in plaats van de informatie. Stel dat een cyberincident ervoor zorgt dat het facturatiesysteem niet meer werkt, maar dat de informatie om tot facturatie over te gaan, nog wel beschikbaar is. Dan zou ervoor kunnen worden gekozen om de facturatie uit te stellen of om tot handmatige facturatie over te gaan. Er kan nog steeds worden gefactureerd, alleen in een lager tempo. Als de informatie om tot facturatie over te gaan, niet beschikbaar is, kan de impact veel groter zijn. Dan kan er tijdelijk helemaal niet worden gefactureerd.

*Positie van een dienst in de product-life-cycle in relatie tot de BIA.*

- Huidige BIA-methodieken roepen ook vragen op als het gaat om de impactinschatting voor de diensten die aan beide uiteinden van een product-life-cycle zitten. Voor de diensten die helemaal aan het begin van de life-cycle zitten kan het zijn dat de impact van optreden van incidenten nog zeer beperkt is in absolute zin. Dit kan als gevolg hebben dat er onvoldoende maatregelen worden getroffen om de dienst af te schermen. Veel productmanagers worstelen tijdens het maken van de BIA met de vraag of ze rekening moeten houden met de huidige, of de toekomstige situatie. Moet er worden gekeken naar de impact van het incident op de huidige omzet of op die van de toekomstige verwachte omzet? Dezelfde redenering geldt voor de diensten die aan de

andere kant van het life-cycle-spectrum zitten, die dus in de nabije toekomst uitgefaseerd worden.

## Tekortkomingen met betrekking tot beantwoording van de BIA-vragen

*Er is beperkte aansluiting van vragen op de doelstellingen en targets van de scope-verantwoordelijke.*

- De vragenlijst bevat vaak vragen die eigenlijk betrekking hebben op doelstellingen die relevant zijn voor diverse verschillende organisatieniveaus. Daardoor worden bepaalde vragen door bepaalde scope-verantwoordelijken als "te ver van hun bed" ervaren, waardoor ze niet goed zelfstandig in te vullen zijn. Dit heeft als bijkomend nadeel dat men de betrokkenheid bij de BIA verliest. Zo is het, om een voorbeeld te geven, voor een dienstverantwoordelijke meestal lastig te bepalen of het optreden van één van de scenario's kan leiden tot verlies van aandeelhouderswaarde, en wat de ernst van dit verlies is. De vragen worden daarnaast door verschillende personen verschillend geïnterpreteerd, en verschillend ingevuld. Bijgevolg kunnen sommige impacts worden overschat, terwijl andere juist onderschat blijven.
- Een hiermee samenhangend aspect is dat een aantal BIA-impactfactoren specifiek gericht zijn op commerciële organisaties. Ze hebben geen algemene geldigheid. Voor een overheid zijn bijvoorbeeld verlies van omzet, verlies beurskoers en verlies van concurrentievermogen irrelevant. Ook is de lijst niet voor iedere organisatie compleet. Voor ziekenhuizen is bijvoorbeeld "patiëntveiligheid" verreweg de belangrijkste impactfactor, maar die komt in de lijst van BIA impactfactoren niet voor.
- Tot slot is het voor scope-verantwoordelijken vaak lastig om zich iets concreets voor te stellen bij wat het betekent als vertrouwelijkheid, integriteit of beschikbaarheid van informatie het gecompromitteerd is. Dit zijn vage begrippen, waarbij niet iedereen hetzelfde beeld heeft.

*Expertise en middelen om impact te kwantificeren ontbreken.*

- Ook voor de vragen die beter in lijn liggen met de doelstellingen en targets van de scope-verantwoordelijke, geldt dat de scope-verantwoordelijken het moeilijk vinden om de impact van verschillende scenario's te kwantificeren. Welk percentage klanten zou weggaan als een scenario optreedt? Wat is de hoogte van onvoorziene kosten die ermee zijn gemoeid?
- Doordat de scope verantwoordelijke onvoldoende kennis of data voorhanden heeft om impact van scenario's te berekenen worden deze vragen meestal op basis van buikgevoel beantwoord. Een voorbeeld is reputatieschade als gevolg van "gelekte" klantgegevens. De gedachte die scope-verantwoordelijken hebben is vaak: "imagoschade door in het nationale nieuws te komen zal wel tot veel schade voor de business leiden". Soms komt dat buikgevoel met de realiteit overeen, maar in vele gevallen ook niet. Vaak wordt vergeten dat de grootte van impact niet statisch is, maar dat de nieuwswaarde van cyberincidenten en daarmee de impact op reputatie in de loop van de tijd afneemt. Ook is er sprake van de zogeheten "beschikbaarheidsheuristiek". Dat wil zeggen dat mensen geneigd zijn om een situatie te beoordelen op basis van gegevens die in hun geheugen beschikbaar zijn. Daardoor laten ze zich gemakkelijk leiden door recente informatie, en laten ze na te zoeken naar oudere of minder vlot beschikbare informatie, of na te denken of de situatie voor hen wel relevant is. Een voorbeeld van het laatste zijn DDoS-aanvallen die in het nieuws komen, waardoor dit als een groot risico wordt gezien, ook door bedrijven die nauwelijks schade zullen ondervinden door een DDoS-aanval.

## Samenvatting

Het bepalen van de impact die een bepaalde dreiging kan hebben op de business is een belangrijk onderdeel van risicomanagement. De stap in het risicomanagement-proces waarin deze impact wordt bepaald is de Business Impact Analysis (BIA). Aan de BIA zoals die tegenwoordig in de meeste organisaties wordt uitgevoerd kan nog veel verbeterd worden. Zo is er bij degenen die de BIA uitvoeren vaak te weinig zicht op de belangen van hogere of aanpalende organisatieniveaus, met het gevolg dat belangrijke risicoscenario's over het hoofd worden gezien. Daarnaast worden dimensies als reikwijdte en tijdsduur van een incident vaak achterwege gelaten en leidt het vaststellen van een worst-case-scenario tot ambiguïteit. Tot slot is het bepalen van de impact van incidenten niet eenvoudig. Niet alleen door het ontbreken van data, maar ook door het feit dat er vaak een discrepantie bestaat tussen de scope van de verantwoordelijke persoon en de impactsoort, denk aan een IT-specialist die moet beoordelen wat de impact is van een data-breach op de aandeelhouderswaarde van een onderneming. De geconstateerde tekortkomingen resulteren in mogelijk onjuist ingeschatte impacts van cyberdreigingen, met het gevaar dat enerzijds werkelijk relevante risico's over het hoofd worden gezien en anderzijds loopt men het risico om te investeren in onnodige veiligheidsmaatregelen.

Volgende maand zal in deel 2 van dit artikel worden ingegaan op manieren om de geconstateerde tekortkomingen aan te pakken.