VERMIJD EEN BLINDSPOT: RISICO'S VAN SCHADUW IT

Eind 2017 begin 2018 heb ik onderzoek gedaan naar het fenomeen 'schaduw IT' (SIT) en hoe de negatieve effecten met behulp van IT governance (ITG) kunnen worden beheerst.

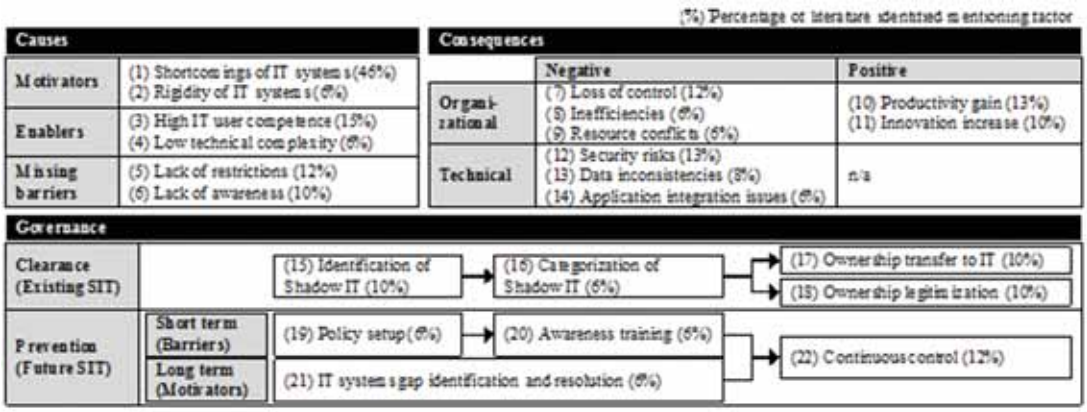
Allereerst is het van belang om een goed beeld te krijgen wat schaduw IT dan precies is: Schaduw IT (SIT) is de naam voor software en hardware die in een organisatie voorkomt zonder dat de formele IT-organisatie daarbij betrokken is (Kopper & Westner, 2016).

Er zijn grof genomen vier verschijningsvormen van SIT te vinden in de literatuur:

- Clouddiensten zoals SAAS-oplossingen; Office365, Dropbox en OneDrive.
- Zelf ontwikkelde applicaties zoals Microsoft Access databases en Excel-sheets.
- Zelf aangeschafte en vervolgens geïnstalleerde applicaties op de door IT aangeboden middelen.
- Zelf aangeschafte hardware of mobile apparatuur zoals smartphones en tablets.

Vele organisaties worstelen met het vraagstuk waarom SIT ontstaat en of SIT wel of niet leidt tot risico's. In een poging inzicht te geven in de beheersing van de risico's van SIT met behulp van het toepassen van governance, is er onderzoek uitgevoerd. De centrale onderzoeksvraag van dit onderzoek luidde als volgt: in hoeverre kan een (IT-) governance bijdragen aan het beperken van de risico's van schaduw IT?

Het fenomeen SIT is met name onderzocht bij streng gereguleerde organisaties, zoals banken- en verzekeringswezen en er is nog weinig bekend over de



Figuur 1 - Framework for causes, consequences, and governance of Shadow IT (Kopper & Westner, 2016)

toepassingen hiervan bij andere sectoren waaronder, onderzoek en onderwijs. Kopper en Westner hebben in 2016 een onderzoek uitgevoerd bij een een aantal zeer gereguleerde organisaties (zoals banken en industrie in Duitstalige landen) en hebben een framework ontwikkeld met een model voor de governance van SIT. Het framework bevat de oorzaken, gevolgen van de SIT voor een organisatie en de governance benaderingen.

In het governance model van het framework van figuur 1 worden er twee benaderingen weergegeven: de 'Clearance' (Existing SIT) en 'Prevention' (Future SIT). Bij de laatstgenoemde benadering wordt er gebruik gemaakt van het opwerpen van barrières en de motivatoren achter de keuzes voor SIT worden aangepakt. De onderzoekers gaan er ook vanuit dat het totaal uitbannen van SIT binnen een organisatie niet mogelijk is en ook niet wenselijk is. De meeste onderzoeken naar de positieve gevolgen van SIT wijzen uit dat met name de SIT wordt toegepast om te vernieuwen (innovatie) en op het vlak van productiviteit toegevoegde waarde heeft (György, Cleven, Uebernickel, & Brenner, 2012).

Risico's van SIT

Verlies van grip op IT en controle op data is een belangrijk risico voor organisaties. In de door SURF (ICT-samenwerkingsorganisatie van het onderwijs en onderzoek in Nederland) opgestelde dreigingsanalyse wordt het verlies van data aangemerkt als belangrijkste risico voor onderzoek en bedrijfsvoering (SURF, 2016). Daarnaast zijn er binnen universiteiten verschillende onderzoeksgroepen die gebruik maken van privacygevoelige gegevens. Het lekken van deze gegevens kan grote gevolgen hebben voor de subjecten en kunnen flinke boetes opleveren voor de bestuurders.

De meeste organisaties zijn ook risico-avers als het gaat om verlies van data (privacygevoelige data), omdat dit uiteindelijk zeer grote gevolgen voor het imago kan hebben van bijvoorbeeld een universiteit. Imagoschade kan invloed hebben op de toestroom van studenten en inkomsten uit researchopdrachten (valorisatie). Zeker gezien de waarde die studenten en onderzoekers hechten aan privacy en informatiebeveiliging.

Ing. Léon Wiskie MBI CISSP CCSP is een zelfstandig professional op het gebied van IT en informatiebeveiliging. Hij heeft dit artikel geschreven op basis van zijn thesis voor de masteropleiding Business Information, waar hij risicobeheersing rond schaduw IT heeft onderzocht.
Leon is te bereiken via leon.wiskie@wiskieit.nl of LinkedIn www.linkedin.com/in/leonwiskie

De grootste risico's van SIT zijn:
- verlies van grip op IT en controle op data (loss of control);
- informatiebeveiligingsrisico's (security risks).

Beheersing van SIT door governance

In dit onderzoek is IT governance gedefineerd als:
1. verzorgen van alignment IT-dienstenaanbod op de behoefte van de business;
2. effectieve en efficiënte besturing van de organisatie;
3. beperken van risico's met betrekking tot IT-investeringen: waarde creëren voor de organisatie maar ook waarde behouden voor de organisatie door controle en nemen van maatregelen.

Een belangrijke pijler is risicomanagement: het effectief toepassen ervan maakt het mogelijk doelen te realiseren en falen van IT te beperken

Om SIT onder controle te krijgen, kan men IT governance inzetten als beheersmiddel. Concreet betekent dit dat SIT onder de risicomanagement processen gecontroleerd kan worden door het overdragen naar de IT-afdeling of dat de business managers de risico's accepteren en dragen. Verder kan de organisatie korte termijn maatregelen treffen door extra barrières op te werpen om nieuwe SIT tegen te gaan en door de awareness van medewerkers vergroten. Als lange termijn oplossing kan men de motiverende factoren voor SIT wegnemen, door betere samenwerking tussen business en IT. Tenslotte is het toepassen van detectie en monitoring een belangrijk onderdeel van preventie.

Casestudy

Voor het empirisch deel van het onderzoek is er gebruik gemaakt van een casestudy, met als onderzoekseenheid een universiteit in Nederland dat bestond uit interviews met experts binnen de organisatie en bestudering van de bedrijfsdocumentatie.

In de casestudy is er gebruik gemaakt van de onderstaande empirische deelvragen:
1. Welk risicoprofiel is acceptabel en welke wet- en regelgeving is voor de universiteit relevant?
2. Wat is de beheersing van de risico's van SIT bij de universiteit?
3. Wat is de volwassenheid van de relevante ITG processen en is er een samenhang met de beheersing van SIT bij de universiteit?

Op basis hiervan kunnen de volgende uitspraken gedaan worden die tenminste geldig zijn voor de casestudy organisatie:
- Het toepassen van governance kan de risico's van de SIT beperken. Er is een blindspot ontstaan door het gebruik van SIT.
- Er wordt onvoldoende gecontroleerd op naleving van geldend beleid en toepassing van maatregelen op de niet door IT beheerde systemen.

Naar aanleiding van dit onderzoek kunnen in ieder geval de volgende aanbevelingen worden gedaan:
- vermijden van een blindspot door het toepassen van IT-assetmanagement;
- toepassen van meer interne controle en audits om compliance aan te kunnen tonen.

Naar aanleiding van het onderzoek zijn er daarnaast minimaal twee aanbevelingen die gedaan kunnen worden die in ieder geval van toepassing zijn op de case organisatie.
1. IT-assetmanagement: zeker door het toenemend gebruik van BYOD- en Cloud-toepassingen is het van belang dat er een beeld ontstaat van de het totale IT-landschap en waar bepaalde data zich bevindt.
2. Door het toepassen van risicomanagement kan er dan gekeken worden naar de bedreigingen per asset. Daarnaast is het van belang om eerdergenoemde data te classificeren en beleid op te stellen waar bepaalde data binnen of de buiten de organisatie mag worden bewerkt. Dit maakt het mogelijk om technische en organisatorische maatregelen te treffen die in overeenstemming zijn met de risicoacceptatiegraad van de organisatie.

Uiteraard is dit onderzoek toegespitst op een specifieke organisatie maar waarschijnlijk is het goed toepasbaar bij andere organisaties die met dezelfde problematiek worstelen. Het doel van de governance van SIT is het vermijden van een `blindspot': een vergeten of decentraal beheerde IT-voorziening waardoor organisaties aan meer risico worden blootgesteld dan acceptabel is.

Referenties

- Györy, A., Cleven, A., Uebernickel, F., & Brenner, W. (2012). Exploring the shadows: IT governance approaches to user-driven innovation. Ecis 2012 Proceedings.
- Kopper, A., & Westner, M. (2016). Deriving a Framework for Causes, Concequences, and governance of Shadow IT form literature.
- SURF. (2016). cyberdreigingsbeeld 2016 Sector onderwijs en onderzoek.