LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Skugg-IT möter GDPR

Icke sanktionerad IT i en omvärld med ökade krav på integritet.

Kandidatuppsats 15 hp, kurs SYSK02 i informationssystem

Författare: Erik Bråtendal
Per Jansson

Handledare: Odd Steen

Examinatorer: Umberto Fiaccadori
Magnus Wärja

Skugg-IT möter GDPR: Icke sanktionerad IT i en omvärld med ökade krav på integritet.

Författare: Erik Bråtendal och Per Jansson

Utgivare: Inst. för informatik, Ekonomihögskolan, Lunds universitet

Dokumenttyp: Kandidatuppsats

Antal sidor: 80

Nyckelord: Skugg-IT, Molntjänster, GDPR, BYOE, Informationssäkerhet, Personuppgifter, Personlig integritet, PUL.

Sammanfattning (Max. 200 ord):
Skugg-IT är ett fenomen som har förekommit i organisationer så länge IT har existerat. Skugg-IT innebär all användning av IT-artefakter av olika slag som inte är sanktionerad av IT-avdelningen. Tidigare har motivationen att ta tag i problematiken kopplat till skugg-IT varit begränsad. Detta har i sin tur bidragit till att organisationer inte vet vad för typ av information de lagrar och var den finns. I och med införandet av EU:s nya dataskyddsförordning kommer kraven på organisationer som hanterar personuppgifter om EU-medborgare att öka kraftigt. Vi undersöker hur skugg-IT i organisationer påverkas utav de förhöjda kraven på integritet och genomför kvalitativa intervjuer med praktiker i branschen som har stor erfarenhet av både skugg-IT samt GDPR. Det visar sig att problematiken kring skugg-IT blir större och det går från ett problem som har kunnat ignoreras till att det nu måste hanteras. Det bör ske proaktivt med ett välgrundat organisatoriskt informationssäkerhetsarbete som har fullt stöd i ledningen och där efterlevnads-ansvaret är solidariskt. Fokus bör ligga på informationen i sig och inte på vilka enheter eller molntjänster som används för att behandla informationen. Företagen kommer tjäna på att ha ett individperspektiv på problematiken då det är samma perspektiv som lagstiftningen i slutändan har.

Innehåll

Figurer

Tabeller

1 Introduktion

Användandet av molntjänster i organisationer har i dagsläget ökat till synnerligen höga siffror och visar inga tendenser på att avta. Enligt Netskope (Netskope 2016) använde personalen i början av 2016 i en given organisation, i genomsnitt 935 molnapplikationer. I ytterligare en rapport från ett senare skede från samma organisation visar att antalet molntjänster som organisationer i genomsnitt använder har ökat till 1030 (Netskope 2017). Den senaste undersökningen visar också att hälften av alla användare av en sanktionerad molnapplikation även använder sig av en personlig icke-sanktionerad instans av samma applikation (Netskope 2017). Om till exempel en organisation har 500 användare av en sanktionerad molnapplikation i sin miljö, så har företaget ytterligare 250 osanktionerade privata instanser av samma applikation. Skillnaden är att organisationen inte har någon som helst kontroll över dessa osanktionerade instanser, data kan lagras hur eller var som helst eftersom de existerar utanför ramarna för organisationens existerande avtal och informationsäkerhetsåtgärder. Detta är ett exempel på fenomen som kallas “skugg-IT” eller på engelska: “Shadow-IT”. Detta är inget som är begränsat till molntjänster utan finns i många olika former, dock är principen densamma. Skugg-IT har existerat och varit ett problem ända sedan den första disketten introducerades på en arbetsplats.

Icke-sanktionerad IT eller skugg-IT, är applikationer, enheter samt teknologier som inte är godkända av IT-avdelningen att användas i företagsmiljön men ändå används på den enskilda medarbetarens egna initiativ. Att detta överhuvudtaget sker kan bero på många saker, bland annat att användarna av en sanktionerad applikation hittar en gratis applikation som upplevs smidigare att använda än de organisationen erbjuder. Detta leder till att organisationen förlorar kontrollen över den enskildas handlingar och var datan som laddas upp lagras.

EU:s nya dataskyddsförordning (den allmänna dataskyddsförordningen eller GDPR) kommer träda i kraft i slutet av maj 2018 och ersätter alla nationella personuppgiftslagar för samtliga medlemsländer. Anledningen till att den kommer vara så omfattande är på grund av att den inte bara kommer gälla EU:s medlemsländer utan även alla länder som behandlar personuppgifter tillhörande EU-medborgare (Datainspektionen 2017a). I samma rapporter som tidigare nämndes (Netskope 2017, Netskope 2016), så var i början av 2016 enbart en fjärdedel av en given organisations applikationer kompatibla med den nya dataskyddsförordningen. Enligt den senaste rapporten från 2017, bara cirka 14 månader innan den nya förordningen träder i kraft, så har denna siffran ökat till cirka en tredjedel av dessa applikationer (33,7%). Detta är en låg siffra och bekräftar det som många andra undersökningar också identifierat, nämligen att en väldigt stor andel organisationer är i dagsläget inte redo för en strängare lagstiftning gällande personuppgiftshantering.
Något som inte får glömmas bort i förberedelserna inför den nya lagstiftningen är att det inte räcker att bara se över de sanktionerade IT-lösningarna utan att även se till att det inte föreligger ett problem med omfattande användning skugg-IT inom organisationen. Vi identifierade att det föreligger en brist på forskning just kring ämnet skugg-IT i relation till de ökade kraven på integritet vilket ligger till grund för denna uppsats.

1.1 Problemområde

Tidigare har det funnits svaga incitament för företag att ägna uppmärksamhet åt eventuell skugg-IT som florerat inom organisationen. Då personuppgiftsbehandlingen tidigare inte kunnat leda till några allvarliga konsekvenser (Datainspektionen 2017b). Men i och med införandet av EU:s nya dataskyddsförordning så ställs organisationer helt plötsligt under luppen och bristande personuppgiftsbehandling kan leda till allvarliga konsekvenser i form av stora sanktionsbelopp (Allmän dataskyddsförordning 2016/679 av den 27 april 2016) och ett nedsvärtat rykte ur ett konsumentperspektiv.

Enligt en undersökning gjord av Frost & Sullivan (2013) så erkände 80% av deras tillfrågade informanter att de använder icke-sanktionerade molnapplikationer i sitt dagliga arbete. Kombinationen av att användandet av molntjänster ökat (Netskope 2016, Netskope 2017) och det nya datalagringsdirektivet som introduceras i maj år 2018 så problematiseras användningen av skugg-IT ytterligare. Hårdare krav ställs på både molnleverantörer och den enskilda organisationen vid hantering av personuppgifter. I värsta fall kommer organisationen som inte behandlat personuppgifter enligt förordningen bli skyldiga att betala ett vite på fyra procent av organisationens globala omsättning (Allmän dataskyddsförordning 2016/679 av den 27 april 2016).

I den nuvarande gällande lagstiftningen (Personuppgiftslagen) så är organisationer, vid brott mot personuppgiftslagen skyldiga att betala ut ett eventuellt skadestånd till de utsatta personerna som blivit kränkta som resultat av deras bristande personuppgiftsbehandling (Datainspektionen 2017b). Högsta domstolen fastställer i en dom från 2013 att ersättningen för kränkningar i de fall som inte kan ses som allvarliga bör ligga under 5000 kr (Högsta domstolen 2013). Det har med andra ord hittills inte funnits några omfattande legala konsekvenser för organisationer att inte hantera personuppgifter på rätt sätt. Den nya dataskyddsförordningen tvingar organisationer att ta hänsyn till behandlingen av personuppgifter då bristande sådan nu har potential att påverka hela organisationen.

Ytterligare en problematisering som medföljer införandet av den nya dataskyddsförordningen är ansvarsförhållandena. I dagsläget är, enligt Datainspektionen, de organisationer som behandlar personuppgifter i tjänsten personuppgiftsansvariga och de företag som tillhandahåller exempelvis molntjänster som används för lagringen av dessa uppgifter är personuppgiftsbiträden (Datainspektionen 2011). Skulle ett dataintrång ske på grund av att någon av parterna inte vidtagit tillräckliga åtgärder för att förhindra detta, så är det för närvarande enbart den personuppgiftsansvarige som gör sig skyldig till brott mot personuppgiftslagen, inte personuppgiftsbiträdet, om inget annat har avtalats parterna sinsemellan. Det är dessutom den enskilda individen, det vill säga ägaren av personuppgifterna, som behöver initiera processen mot den personuppgiftsansvarige. Den personuppgiftsansvarige behöver inte kontinuerligt kunna bevisa att de följer de rådande lagarna (Datainspektionen 2017b).

Den nya dataskyddsförordningen kommer inte påverka själva definitionen av begreppen men däremot förändras rollernas ansvarsförhållande. Personuppgiftsbiträdet kommer få nya skyldigheter och dess eget ansvar i relation till personuppgifterna kommer öka kraftigt. I flertalet situationer kommer personuppgiftsbiträdet omfattas av samma skyldigheter som personuppgiftsansvarige (Datainspektionen 2017c). Skugg-IT är ett fenomen som har existerat länge, dock utan att ha uppmärksammats i någon större utsträckning (Yeadon 2016). Nu kan

dock den bristande kontrollen av skugg-IT få stora konsekvenser för organisationer och åtgärder måste vidtas.

1.2 Forskningsfråga

Hur påverkar ökade krav på personlig integritet skugg-IT i organisationer?

1.3 Syfte

Syftet är att ta reda på hur organisationer förhåller sig till sina icke-sanktionerade IT-lösningar och hur de påverkas av de ökade integritetskraven som införandet av den nya dataskyddsförordningen innebär.

1.4 Avgränsningar

- Vi kommer inte själva försöka tolka dataskyddsförordningen, utan endast använda sekundärkällor, till exempel Datainspektionen.

- Vi tar inte hänsyn till lagar som inte direkt påverkar oss i Sverige.

- I organisationer kan det hända att de förekommer användning av olagligt anskaffad mjukvara eller liknande, detta tas inte heller hänsyn till, utan vi diskuterar endast laglig skugg-IT.

- På samma sätt som skugg-IT kan leda till läckage av personuppgifter kan det hända att andra känsliga uppgifter, företagshemligheter och liknande, som kan påverka organisationen. Detta kommer inte att behandlas i vår uppsats.

1.5 Centrala begrepp

BYOE - *Bring your own everything.* Ett samlingsbegrepp för IT som anställda tar med till arbetet på eget initiativ.

Datainspektionen - Svensk statlig förvaltningsmyndighet som har till uppgift att verka för att människor skyddas mot att deras personliga integritet kränks på grund av felaktig behandling av personuppgifter. Datainspektionen har varit vår källa när det kommer till tolkning av lagtext då vi själva ej besitter tillräcklig juridisk kunskap.

Dataskyddsreformen - *På engelska General Data Protection Regulation (GDPR).* EU:s nya regelverk för hur personuppgifter om EU-medborgare bör lagras och hur deras integritet skall skyddas. Regelverket är en reform från ett direktiv till en förordning. Ett direktiv inom EU är bara riktlinjer, nationernas egna lagstiftningar gäller fortfarande över ett direktiv. En förordning är tvingande och står över de nationellt stiftade lagarna.

Informationssäkerhet - Åtgärder som vidtas för att förhindra att information läcker ut, förvanskas eller förstörs och för att informationen skall vara tillgänglig när den behövs.

Integritet - I uppsatsens sammanhang så definieras personlig integritet utefter definitionen; Personlig integritet är den enskildes rätt att kontrollera vem som kan få tillgång till dennes privata information.

Organisation - En gemensam samverkan för att uppnå ett mål. Exempelvis ett bolag eller en förening.

Personuppgift - Som personuppgift räknas enligt 3§ PUL (SFS 1998:204): *"all slags information som direkt eller indirekt kan användas för att identifiera en fysisk person som är i livet."*

2 Litteraturgenomgång

Här går vi igenom den tidigare forskning som är gjord på området samt begrepp som är relevanta för vår frågeställning och vårt problemområde. Teorin har framförallt hämtats från akademiska artiklar som belyser vårt problemområde från olika perspektiv samt påvisar hur icke-sanktionerad IT traditionellt sett har hanterats i organisationer.

De akademiska artiklar som skrivits på området skrevs innan dataskyddsreformen var aktuell och de har inte kunnat ta med de konsekvenser den nya förordningen kan ha. Däremot finns det gott om icke akademiska artiklar i form av teknikbloggar och branschtidningar. Den tidigare forskning som funnits har dock bidragit till god förståelse om vad som ligger bakom problematiken inom ramen för uppsatsens syfte.

2.1 Skugg-IT

Fenomenet skugg-IT har funnits så länge IT har använts i organisationer. Skugg-IT innefattar samtliga IT-artefakter som existerar i en organisation där användandet inte är kontrollerat och godkänt av en IT-avdelning eller liknande (Silic & Back 2014). Samma fenomen kan även definieras som användning av obehöriga applikationer i företagsmiljö och bearbetning samt lagring av företagsinformation på icke-godkända enheter (Walters 2013). Skugg-IT behöver inte heller utgöras av en enskild IT-artefakt utan kan vara så kallade skuggsystem som är ett helt informationssystem som existerar parallellt med de sanktionerade systemen (Behrens 2009). Detta kan till exempel uppstå om en avdelning i en organisation anser att de behöver ytterligare funktionalitet än den som erbjuds av deras vanliga system och bestämmer sig för att antingen utveckla eller införskaffa ett eget system.

Ämnet skugg-IT är i många fall svårt att studera tack vare dess informella karaktär och de är sällan uppenbara i organisationer vilket leder till att utredare har svårt att få tillgång till dem (Behrens 2009). Detta är anledningen till att vi hittat få studier kring ämnet.

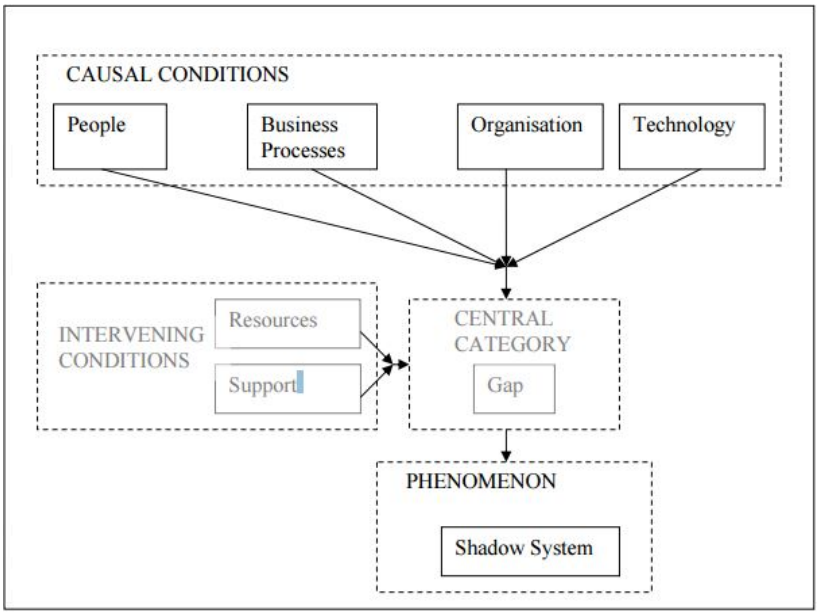
Den senaste tiden har skugg-IT fått allt mer fotfäste i organisationer och företeelsen får allt mer betydelse då ny teknik har introducerats (Silic & Back 2014), både på grund av det ökade användandet av diverse molntjänster och att personliga enheter börjat användas i professionella sammanhang (Frost & Sullivan 2013). Silic & Back (2014) delar in skugg-IT under tre olika rubriker: *Graynet* där de syftar på applikationer som använder tekniker för att undvika vanliga nätverksregler, som till exempel vid fildelning med hjälp av *peer-to-peer* teknik eller vissa chattprogram som installeras. *Content apps* som används för att skapa, modifiera och publicera olika typer av innehåll och *Utility tools* som hjälper användaren att utföra optimeringar eller liknande uppgifter. *Graynet*-applikationer utgör den största risken för en organisations informationssäkerhet men *Content apps* kan ha större påverkan då anställda använder applikationer som är orelaterade till deras arbetsuppgifter (Silic & Back 2014). Eftersom definitionen av begreppet är så brett som det är, verkar det dock enfaldigt att begränsa sig till detta dessa tre rubriker.

Att inte endast fokusera på de tekniska bitarna av skugg-IT och istället diskutera informationen som faktiskt hanteras i systemen är ett mer relevant perspektiv där den

informationen som lagras ges mer utrymme (Walters 2013). Det är i slutändan informationen som är det värdefulla i sammanhanget. Under tidigare skede gjordes försök att hantera skugg-IT genom att märka specifika lagringsenheter med organisationens namn för att påminna de anställda om vem informationen på enheten egentligen tillhör (Walters 2013).

2.1.1 Uppkomst av skugg-IT

Skugg-IT förekommer i organisationer där "gapet" mellan vad ett system utlovar och vad användarna av systemet faktiskt behöver är för stort (Behrens 2004). Detta illustreras nedan i en modell i figur 1. Detta är en av förklaringarna till varför skugg-IT uppstår och har ett tekniskt perspektiv. Hur stort "gapet" blir påverkades av de i modellen kallade *casual conditions* samt *intervening conditions*. *Casual conditions* innehåller faktorer som påverkar och avgjorde ifall någon form av Skugg-IT uppstod och *intervening conditions* avgjorde hur omfattande systemet blev utefter vilka resurser och vilken support som fanns tillgänglig (Behrens 2004). Om skuggsystemet exempelvis var av en mer sofistikerad karaktär och användarna av det hade tillgång till support ifall de behövde, så ökade detta skuggsystemets omfattning (Behrens 2004). Även mängden resurser som lades ned påverkade resultatet. Detta innefattar allt från hur systemet utvecklas till hur mycket pengar som läggs på ett färdigutvecklat alternativsystem.



Figur 1: Theoretical Scheme (Behrens & Sedera, 2004, p.13)

Även Silic & Back (2014) är av åsikten att Skugg-IT uppstår då den IT-lösningen som erbjuds inte är tillräcklig för att på ett bra sätt uppfylla verksamhetens mål.

Ett annat intressant perspektiv är hur organisationens kultur kan påverka uppkomsten av skugg-IT. I en artikel skriven av Jennifer Yeadon (2016) citeras Phil Hagen:

> *"I believe Shadow IT sprouted from what users perceived as a 'Culture of No' on the part of IT organizations. IT was seen as a roadblock to business, so people found a way around it."*
>
> - Phil Hagen (2016)

Detta innebär att allt eftersom teknologin utvecklades och anställda fick tillgång till ny modern teknologi så ville de ha med sig dessa till jobbet och använda i tjänsten. Men eftersom användarna visste att IT-avdelningen troligtvis skulle säga nej till användningen av dessa nya enheter och applikationer, så började dem helt enkelt användas utan IT-avdelningens samtycke. Istället för att försöka introducera dessa nya teknologier via organisationens etablerade kanaler, ignoreras dessa helt. Detta innebär att all form av validering undviks och de eventuella säkerhetsrisker som kan uppstå utvärderas inte (Yeadon 2016). Detta grundar sig i att de anställda vill använda verktyg som hjälper dem att utföra sitt arbete på ett bättre och snabbare sätt. Dock ignoreras ofta de negativa konsekvenser som användandet av Skugg-IT kan få. Många gånger vet det anställda dessutom inte att de gör något fel, framförallt på grund av att de policys som hanterar detta är ofta för svåra att förstå (Silic & Back 2014).

2.1.2 För- och nackdelar med skugg-IT

Skugg-IT existerar parallellt med organisationens övriga legitima IT-lösningar. Den största skillnaden är att den undgår den kontroll och övervakning som de sanktionerade systemen utsätts för. Ur ett tekniskt perspektiv så kan användandet av skugg-IT bland annat öka risken för inkonsekvent affärslogik, problem med minskad medgörlighet mellan system och ökad risk för att förlora data då datan lagras utspritt (Silic & Back 2014). Ett utbrett användande av skugg-IT leder även till att de officiellt sanktionerade systemen undermineras (Strong & Volkoff 2004) Användningen av skugg-IT har även lett till förhöjda krav och förhöjd IT-konsumtion hos anställda (Williams 2011). De anställda är vana vid att alltid använda de senaste teknologierna privat. Eftersom enskilda individer oftast inte ställer lika höga krav på säkerhet och inte behöver integrera teknologin i ett större sammanhang är det sällan något problem att snabbt anamma ny teknik. En organisation har dock betydligt mer faktorer att ta hänsyn till vid införandet av en ny teknologi. De måste bland annat fråga sig om den nya applikationen eller enheter uppfyller deras krav på säkerhet och hur väl de samspelar med redan existerande verktyg. Detta har resulterat i att många IT-avdelningar har problem med att hålla jämn takt rent utvecklingsmässigt (Williams 2011). Har inte IT-avdelningen resurser att leverera tillfredsställande verktyg till organisationen finns det risk att användningen av skugg-IT fortsätter att öka (Williams 2011).

Skugg-IT lägger även extra belastning på IT-avdelningen på andra sätt. Utöver deras vanliga arbetssysslor så kommer problemen som skugg-IT orsakar naturligt förväntas att tas hand om av dem då de anses vara experterna inom området (Walters 2013). I en undersökning där en femtedel av anställda på en mängd tillfrågade företag hade svarat att de använde en privat instans av Dropbox för att lagra företagsinformation trots att de visste att detta var emot organisationens säkerhetspolicys (Walters 2013). Det betyder att i vissa fall kan användningen av skugg-IT vara så hårt förankrat hos anställda att de medvetet utsätter organisationen för risker vilket kan leda till allvarliga följder för både organisationen och den ansvarige

anställde. I andra fall visade det sig även att de anställdas fortsatta användning av skugg-IT berodde på att de antingen inte förstod organisationens säkerhetspolicys eller inte visste om att de fanns (Silic & Back 2014).

För att få förståelse för varför skugg-IT är ett så pass utbrett fenomen bör även dess fördelar tas i beaktning. Skugg-IT är inte enbart så negativt som IT-personal ofta betonar det att vara, fördelarna har visat sig vara många (Behrens 2009). De nämner allt från att det är lättare att använda till en högre grad av tillgänglighet och framförallt att fördelarna var lätta att observera vilket gjorde att andra anställda kunde snabbt förstå hur systemet direkt kunde underlätta deras dagliga arbetsrutin (Behrens 2009).

Utöver de negativa aspekterna med användningen av skugg-IT, som exempelvis att IT-avdelningen helt har tappat kontroll och inte administrerar ett system som många anställda använder, har det visat sig att användandet av det gällande systemet påverkade både företagskulturen och företagspolitiken (Behrens 2009).

2.1.3 Hanteringen av skugg-IT

För att förhindra förekomsten av skugg-IT finns det ett antal åtgärder som kan vidtas. Trafiken på organisationens nät kan övervakas och åtkomst till vissa webbsidor kan begränsas. Dessutom kan användarnas behörighet på organisationens enheter reduceras så bara representanter från IT-avdelningen har rättighet att installera program (Silic & Back 2014). Undersökningen visade dock även att dessa restriktioner inte varit speciellt effektiva då många av åtgärderna varit lätta att kringgå (Silic & Back 2014). Ett av problemen som tidigare identifierats är att användarna inte har insett vilka konsekvenser användning av skugg-IT kan leda till. För att åtgärda detta kan existerade policys göras tydligare och mer fokus läggas på utbildning. Detta tillsammans med hårdare kontroll ska minska förekomsten av skugg-IT (Silic & Back 2014).

Ett annat perspektiv är att acceptera användandet av skugg-IT. Skugg-IT behöver inte endast vara något som en individ själv använder. Det kan vara ett system som är accepterat och används av delar av verksamheten men inte som är officiellt accepterad av organisationen (Silic & Backs 2014). Behrens (2009) presenterar ett exempel där ett skuggsystem använts i stor utsträckning i organisationen. Inledningsvis accepteras dess existens av ledningen. Till slut beslutades det dock att systemet skulle flyttas in i den redan centralt existerande IT-avdelningen. Ledningen ansåg att trots att skuggsystemet fungerade bra så var den överhängande risken med att ha ett så pass omfattande system utanför central styrning för stor. Det framkom också att individerna som satt i ledningens och deras inställning var avgörande i beslutet. Några beslutsfattare var uttalat emot användandet av systemet medans andra var för. Den individ som för tillfället hade makt bestämde om systemet skulle få användas eller ej. Detta belyser på två saker, dels att ledningens åsikter spelar stor roll i sammanhanget och eftersom att systemet integrerades i organisationens sanktionerade lösning bekräftas att skugg-IT kan användas för att förbättra den redan existerande IT-lösningen.

I slutet av studien presenteras fem olika punkter hur skugg-IT bör hanteras (Figur 2).

1. *Acknowledge the shadow system:* Every organization will have its informal side. This informal side will most likely harbour both social and/or technical shadow systems. They exist as a necessary function of the organization.
2. *Learn from the shadow system:* If there are shadow systems in an organization, ask why they are there. Many exist out of pure necessity: to get the job done. On the other hand, though, they might be masking a deeper deficiency with the formal systems themselves.
3. *Shadow systems are in the eye of the beholder:* Take off the blinkers of prejudice and stigma surrounding shadow systems and try to see them for what they really are. At times they may be bad to the core but they may also be diamonds in the rough.
4. *Don't try to control shadow systems:* Many shadow systems exist because the informal side of the organization is the place where they survive and thrive. Uprooting them from the creative and innovative side of the organization may cause them to wither and die.
5. *Encourage the good shadow systems:* Make the good shadow systems legitimate without uprooting them. Management at all levels should pay careful attention to capturing these innovations and fostering the unique conditions that initially gave rise to them. Because of the natural diversity both across and within organizations, capitalising on a system that grew from within is more likely to hold the key to true strategic and competitive advantage[3].

Figur 2: Lessons Learned (Behrens, 2009, p.128)

Metoderna fokuserar snarare på att dra nytt av och utnyttja fenomenet skugg-IT till skillnad från den vanliga infallsvinkeln där informationssäkerheten prioriteras i större utsträckning (Behrens 2009).

För att kontrollera användandet av skugg-IT kan även kontrollen av åtkomst utökas, användare verifieras i en större utsträckning och övervakningen av webbapplikationer som används i organisationen bör implementeras (Walters 2013). Genom att applicera dessa metoder och övervaka trafiken till anställdas webbläsare kan organisationens existerande policys upprätthållas och istället för att helt förbjuda användandet av molnapplikationer kan de anställda dra nytta av dess fördelarna samtidigt som organisationen kan kontrollera att deras data hanteras på rätt sätt (Walters 2013). Silic et al. skriver i artikeln *A new perspective on neutralization and deterrence: Predicting shadow IT usage* (2017) om skugg-IT och dess hot från insidan. De viktigaste punkterna summeras nedan:

- Flertalet undersökningar med IT-chefer och ledningspersonal kom fram till att det absolut största säkerhetshotet är nuvarande och före detta anställda i organisationen.
- Två teorier som är centrala i hanteringen av att anställda inte efterlever organisationens säkerhetspolicy, avskräcknings- och neutraliseringsteorin.
- Avskräckning kan exempelvis vara genom hot av både formella och informella sanktioner men forskningen inom området visar på motsägelsefulla resultat gällande framgången av denna metod.
- Anställda har i många fall visat sig fortsätta bryta mot säkerhetspolicys trots de eventuella konsekvenserna som kan uppstå, både av godartade och illvilliga anledningar.
- Detta har gett upphov till neutraliseringsteorin som förklarar detta genom att anställda försöker rationalisera eller motivera en omoralisk eller olaglig handling.

2.2 Informationssäkerhet

Skugg-IT är ett fenomen som utsätter en organisations data för risker. För denna uppsats så är det framförallt intressant ur ett integritetsperspektiv då det är detta som dataskyddsförordningen ämnar skydda. Vi har valt att adressera det genom att ta upp informationssäkerhet som helhet då det är på detta sättet som integriteten skyddas från en organisations perspektiv. Under ett informationssäkerhetsarbete sätts policys upp som bör behandla hur personuppgifter skall hanteras i organisationen.

Informationssäkerhetsarbetet för ett IT-system bör gå ut på att primärt åtgärda fyra saker: se till att information finns när vi behöver den (tillgänglighet), att vi kan lita på att den är korrekt och inte förstörd eller manipulerad (riktighet), att endast behöriga får ta del av den (konfidentialitet) samt att det går att följa hur och när informationen hanteras och kommuniceras (spårbarhet) (Informationssäkerhet.se 2015). Tack vare att den moderna ekonomin drivs av den informationsintensiva miljön vi idag lever i, så har informationssäkerhetsarbetet fått en mycket högre prioritet inom organisationer runt om i världen (Gordon & Loeb 2002). För att reducera risker och försäkra sig om att dessa fyra punkter alla är åtgärdade så har organisationer ofta förlitat sig på teknologiskt baserade lösningar (Bulgurcu et al. 2010). Även om dessa lösningar hjälper till att förbättra informationssäkerheten så eliminerar det sällan på egen hand riskerna (Bulgurcu et al. 2010). Nyckeln till ett framgångsrikt informationssäkerhetsarbete ligger i att även investera i organisatoriska åtgärder (Bulgurcu et al. 2010). Eftersom anställda anses vara den svagaste länken vad gäller informationssäkerhet så har anställdas eftergivenhet till informationssäkerhetspolicys framkommit som en av de viktigaste resurserna i informationssäkerhetsarbetet (Bulgurcu et al. 2010).

2.3 Bring Your Own Everything

Bring Your Own Everything (BYOE) är ett samlingsbegrepp som involverar ett flertal, vanligt förekommande, termer inom “Bring Your Own”-trenden. Eftersom fenomenet innebär att fler enheter introduceras i företagsmiljön så ökar komplexiteten kring informationssäkerhet genom att information kan lagras på ställen bortom organisationens sanktionerade system. Detta bidrar till att eventuella dataläckor eller intrång kan ske från fler åtkomstpunkter och det blir betydligt svårare att få en överblick över vart organisationens information lagras. Samlingsbegreppet är omfattande men vi tar enbart upp de som är mest relevanta för vårt område. Dessa är Bring Your Own Device (hädanefter BYOD) samt Bring Your Own Service (hädanefter BYOS) som också ibland benämns som Bring Your Own App (hädanefter BYOA).

BYOD är ett koncept som innebär att anställda tar med och använder privatägda IT-enheter i tjänsten och använder dessa för att komma åt företagsresurser men även för privat bruk (Ghosh et al. 2013). Konceptet är till stor fördel för anställda då det effektiviserar arbetet tack vare att de har all relevant företagsinformation lättillgänglig vart de än befinner sig. Eftersom de använder sina egna enheter även i jobbet så är dem redan vana att arbeta med dem vilket resulterar i en effektivisering av arbetet (Ghosh et al. 2013). För organisationen finns det också fördelar, omfamnas helt konceptet och låter de anställda använda sina egna enheter minskar kostnaderna för dels inköp av enheterna samt undviks kostnaden för att utbilda de anställda på organisationernas interna verktyg (Ghosh et al. 2013).

BYOS är en förlängning på *BYOD* och innebär att anställda inte bara använder privata enheter utan även egenvalda mjukvaror (Leeuwen 2014). Fenomenet förekommer även då anställda installerar egna mjukvaror på sina tilldelade enheter. Fördelarna med *BYOS* är väldigt lika de som finns i användningen av *BYOD,* bland annat slipper företag lägga pengar på dyra mjukvaror och utbilda de anställda i hur dem används (Leeuwen 2014). Givetvis finns det inte endast positiva aspekter. Om alla på kontoret själva skulle få välja vilka verktyg de vill arbeta med så blir det en omfattande utmanande att skydda informationen och kunna samarbeta i havet av olika applikationer (Leeuwen 2014). Det går inte heller att övervaka säkerheten i den valda mjukvaran eftersom ansvaret har skiftat från organisationen till de anställda som är användarna (Leeuwen 2014).

BYOA är en relativt ny trend som också gjorts möjlig av *BYOD* och är en förlängning av *BYOS.* Om anställda tror att de kan utföra sitt jobb snabbare och effektivare genom att använda sina egna enheter så kommer de helt enkelt stå för kostnaden för eventuella applikationer själva (Walters 2013).

2.3.1 Skugg-IT i relation till BYOE

Som vi tidigare påpekat är inte Skugg-IT är ett nytt fenomen, men det är tydligt att den moderna teknologiska utvecklingen har försvårat situationen ytterligare (Walters 2013). Bland annat ökar problematiken i och med *BYOD*. Anställda vill idag välja vilka enheter de vill utföra sitt arbete med och detta leder till att företagsinformation hanteras av fler enheter än vad som kan vara tänkt enligt företagspolicys. Problematiken uppstår när vi inte inser att samma mångfald som gäller för anställda att få välja vilken enhet de vill jobba med också appliceras på informationen som används i dessa enheter vilket i sin tur leder till ökad spridning av datan (Micallef 2015).

Vad gäller *BYOD* så förstärker det inverkan som skugg-IT har på en organisation. Bland annat blir det betydligt svårare att kontrollera informationen som flyttas över till de anställdas egna enheter. Informationen som överförs från organisationens interna system skulle till exempel automatiskt kunna laddas upp i den anställdes privata molnlagringsinstans. Detta leder till att organisationen helt förlorar kontrollen över informationen (Miller et al. 2012).

Problematiken ökar ytterligare med fenomenet *BYOS*. Om anställda hanterar personuppgifter i sitt dagliga arbete och de använder sig av verktyg de införskaffat sig på egen hand som inte har försetts av organisationen så bryter det också mot säkerhetspolicys. Det måste vara tydligt klargjort för anställda som arbetar med information som är skyddad av diverse förordningar att detta är strängt förbjudet (Walters 2013).

BYOA är ett resultat utav *BYOD* och *BYOS* vilket förenklar för användarna att sprida ut datan ytterligare då många applikationer använder sig av molnlagring. Detta har blivit ett så pass stort problem att företag överväger att sätta upp egna företagsstyrda applikations-butiker för att på

så sätt tillfredsställa de anställdas behov och samtidigt ta kontroll över vilka applikationer de använder (Donnelly 2013).

2.4 Molntjänster

För att öka förståelsen för hur skugg-IT i molnet kan uppstå så finner vi det av värde att undersöka hur molntjänster används i organisationer idag. Det finns många orsaker att molntjänster har blivit så populära inom företag. Molntjänster idag erbjuder en dynamisk allokering av resurser och är mycket skalbara vilket gör det enklare för företag att skala upp eller ned deras tjänster (Marston et al. 2011). Eftersom datorresurserna hanteras via mjukvara så kan distributionen ske snabbt när nya krav uppstår (Marston et al. 2011). En orsak till att molntjänster är populära bland mindre företag är eftersom de får tillgång till samma kraftfulla datorresurser som tidigare bara var tillgängligt för mycket större företag (Marston et al. 2011). På så sätt kan de mindre företagen få en lättare start då de inte behöver investera resurser att bygga upp en egen IT-infrastruktur med tillhörande IT-avdelning. Samma fördelar gäller även för företag i tredje världen som har lämnats efter i IT-revolutionen (Marston et al. 2011).

2.4.1 Problematik med molntjänster

I dagsläget är användandet av molntjänster inom organisationer högre än någonsin. Även användandet av icke-sanktionerade molntjänster följer trenden (Netskope 2017). Tidigare diskuterades det hur anställda snabbt anammar nya teknologier som underlättar deras egna arbete. Med detta i åtanke är det inte konstigt att fokus flyttas från traditionella teknologier som exempelvis användning av USB-stickor och skrivbordsapplikationer, till molnlagring och liknande. När molnbaserade applikationer används förändras förutsättningarna för hur informationen hanteras. Walters (2013) skriver:

> *“Because of the highly abstract and distributed nature of the cloud, data may reside in different geographies and even move around between physical locations depending on how data is replicated between data centres or hubs. This has legal implications when an organisation is required to comply with specific privacy laws or has to present digital evidence, and highlights a further risk associated with shadow IT “*
>
> (Walters 2013)

Här påvisas hur komplex informationshanteringen kan bli vid användandet av molntjänster. I samspel med den nuvarande ökningen av användandet så dyker det upp frågor kring molntjänsternas säkerhet. Tas det även i beaktande att anställda i organisationen använder icke-sanktionerade molntjänster, där det inte finns fördefinierade avtal för hur informationen skall hanteras ökar komplexiteten ytterligare.

Data-integritet är ett viktigt element i ett väl fungerande system och detta bör beaktas när information skickas iväg och skall sparas hos en molntjänstleverantör. Att bevara integriteten i

ett system är mycket svårare när tillgängligheten ökar och speciellt känsligt i fallet då det gäller personuppgifter.

Sammanfattningsvis har molntjänsters ökade popularitet har bidragit till en ökad teknisk komplexitet, men genom att involvera fler intressenter i informationshanteringen blir ansvarsförhållandena ytterligare en dimension i problematiken.

2.4.2 Skugg-IT i relation till molntjänster

Traditionellt sett har mycket fokus kopplat till skugg-IT lagts på fenomenen som BYOE och vilka applikationer det är som använts inom ramen för skugg-IT. I och med molntjänsternas ökade popularitet bör fokus flyttas från enheterna till informationen som lagras i dem (Walters 2013). Problematiken gällande Skugg-IT är i stor del de samma som för sanktionerade molntjänster, den största och mest avgörande skillnaden är att i fallet Skugg-IT så är det svårt att veta var informationen huserar då organisationerna inte administrerar eller ansvarar för de använda applikationerna.

Molntjänsternas ökade popularitet har lett till att anställda nu kan välja i ett överflöd av billiga och bekväma molnlagringstjänster (Micallef 2015). Detta innebär att det kontinuerligt skapas och lagras dokument i flertalet förvaringsplatser, på flera enheter både utanför och innanför företagets brandvägg (Micallef 2015). Denna praxis är nästintill alldaglig och antalet lagringsplatser bara fortsätter att öka (Micallef 2015). I en undersökning genomförd av IBM så svarade en tredjedel av anställda på “fortune 1000”-företag att de regelbundet sparar och sprider företagsinformation på externa icke-sanktionerade molnlagringsplattformar (Silic et al. 2017). En annan undersökning gällande molnanvändning riktad till IT-säkerhetspersonal så svarar 72% av dem att de inte har en aning om vilka skugg-IT-applikationer som används inom deras organisationer (Silic et al. 2017).

Om en organisation av någon anledning snabbt skulle behöva sammanställa stora mängder information, till exempel för en pågående rättegång, kan detta resultera i väldigt stora kostnader. IT-personal skulle då behöva lägga all sin tid på att lokalisera, hämta och sammanställa all denna information för presentation. För att komplicera situationen ytterligare så använder troligtvis en given användare sig av flera enheter, både privat och i tjänsten. Ofta används även dessa med flera olika identiteter för att kunna komma åt olika typer av tjänster på enheterna vilket leder till att datan sprids ut ytterligare (Walters 2013).

2.5 Dataskyddsreformen

Bakgrunden till varför företag måste ta tag i sitt informationssäkerhetsarbete och hantera den skugg-IT som existerar i organisationen finns i den nya dataskyddsförordningen. I maj 2018 börjar EU:s nya regelverk för personuppgiftshantering gälla i alla medlemsländer. Regelverkets mest centrala del är den allmänna dataskyddsförordningen som kommer att tillämpas generellt på behandling av personuppgifter (Datainspektionen 2017d). En förordning är en EU-lag som när den träder i kraft direkt blir en del av den nationella lagstiftningen. Förordningar tillämpas på samma sätt i alla länder, skulle någon nationell lag skilja sig mot förordningen är det fortfarande förordningen som gäller (EU-upplysningen 2016).

I och med implementeringen av dataskyddsreformen kommer förutsättningarna i den miljön skugg-IT verkar i att förändras. Mycket är fortfarande under utredning men några saker kan vi redan konstatera. Framförallt att kraven på organisationer, både de som ansvarar för och hanterar personuppgifter kommer att öka och att det konsekvenserna kan komma att bli betydligt allvarligare om inte förordningen följs.

För att öka den enskilda individens möjlighet att ha kontroll över sina egna personuppgifter samt öka kraven på organisationerna som hanterar dem har EU beslutat om att våren 2018 införa en ny dataskyddsförordning. Som personuppgift räknas enligt 3§ PUL (SFS 1998:204): *"all slags information som direkt eller indirekt kan användas för att identifiera en fysisk person som är i livet."* Den nya dataskyddsförordningen liknar till vissa delar den redan existerande svenska Personuppgiftslagen, som till exempel definitionen av begreppet personuppgift, personuppgiftsbiträde och personuppgiftsansvarig men vissa delar innebär ett utökat ansvar för organisationer som behandlar personuppgifter. Dataportabilitet är en av nyheterna som innebär att personer vars personuppgifter behandlas baserat på samtycke har rätt att kräva tillbaka sin data och på så sätt bli "bortglömd" av organisationen. Dessutom kommer det krävas att den enskilda organisationen anmäler förluster av personuppgifter inom 72 timmar till Datainspektionen. Den kanske mest betydande förändringen är den sanktionsavgift som kan ges organisationer som inte följer förordningen. Avgiften kommer att bedömas utifrån hur allvarlig överträdelsen är, vilka åtgärder som vidtagits för att undvika att bryta mot förordningen och om det var medvetet eller inte (Datainspektionen 2017e). Maximalt kan fyra procent av organisationens omsättning eller 20 miljoner Euro i en administrativ sanktionsavgift utkrävas (Allmän dataskyddsförordning 2016/679 av den 27 april 2016).

2.5.1 Personuppgiftsansvarig

Både begreppet personuppgiftsansvarig och personuppgiftsbiträden kommer ursprungligen från Personuppgiftslagen men kommer fortsätta att finnas inom ramen för dataskyddsförordningen, dock med vissa utökade åtaganden (Datainspektionen 2017f). Personuppgiftsansvarig är den som på något sätt hanterar personuppgifter inom ramen för sin verksamhet (Datainspektionen 2017g). Det syftar på den juridiska personen, alltså organisationen eller företag i sig och inte på en enskild individ. I undantagsfall, om till exempel en person har en enskild firma, kommer den personen bli personuppgiftsansvarig. Ansvaret den personuppgiftsansvarige har kan inte överlåtas på en annan part, dock kan själva hanteringen av personuppgifter överlåtas (Datainspektionen 2017g).

2.5.2 Personuppgiftsbiträde

Personuppgiftsbiträde är den organisation som hanterar personuppgifter på uppdrag av en personuppgiftsansvarig. Dessa två tillhör inte samma organisation utan detta förhållande uppstår till exempel då organisation X anlitar organisation Y för att lagra deras personuppgifter. Organisation X blir då personuppgiftsansvarig medan organisation Y blir personuppgiftsbiträde (Datainspektionen 2017g). För att reglera detta förhållandet måste ett skriftligt avtal, som den personuppgiftsansvarige är ansvarig för att upprätta, finnas. Detta avtal skall reglera att personuppgiftsbiträdet endast får hantera uppgifterna enligt den personuppgiftsansvariges instruktioner samt att de skall följa alla säkerhetsåtgärder som den personuppgiftsansvarige är skyldiga att vidta (Datainspektionen 2017g). Personuppgiftsbiträde finns även i PUL, men i och med införandet av dataskyddsreformen kommer denna rollen att innebär ett utökat ansvar för den som behandlar personuppgifter. Personuppgiftsbiträdet blir skyldiga att ta, som Datainspektionen uttrycker det: *"ett eget ansvar för att vidta lämpliga tekniska och organisatoriska åtgärder för att se till att säkerhetsnivån för er behandling är tillräcklig."* (Datainspektionen 2017c). Detta kan enligt dem innebära ett behov av att kryptera eller pseudo-anonymisera personuppgifterna samt säkerställa att systemen som används är tillräckligt säkra. Det innebär även att kraven på att samarbeta med den personuppgiftsansvarige ökar, bland annat genom ett krav på att informera dem om någon form av incident relaterat till personuppgifterna sker. Följs inte det här reglerna kan personuppgiftsbiträdet bli, precis som den personuppgiftsansvarige, skyldiga att betala böter på 20 miljoner euro eller fyra procent av organisationens omsättning (Allmän dataskyddsförordning 2016/679 av den 27 april 2016).

2.6 Teoretiskt ramverk

I det här kapitlet presenteras de mest centrala delarna av litteraturstudien. Dessa sammanfattas i en tabell som sedan utformas till ett ramverk för att ge läsaren en tydlig överblick över litteraturgenomgångens resultat.

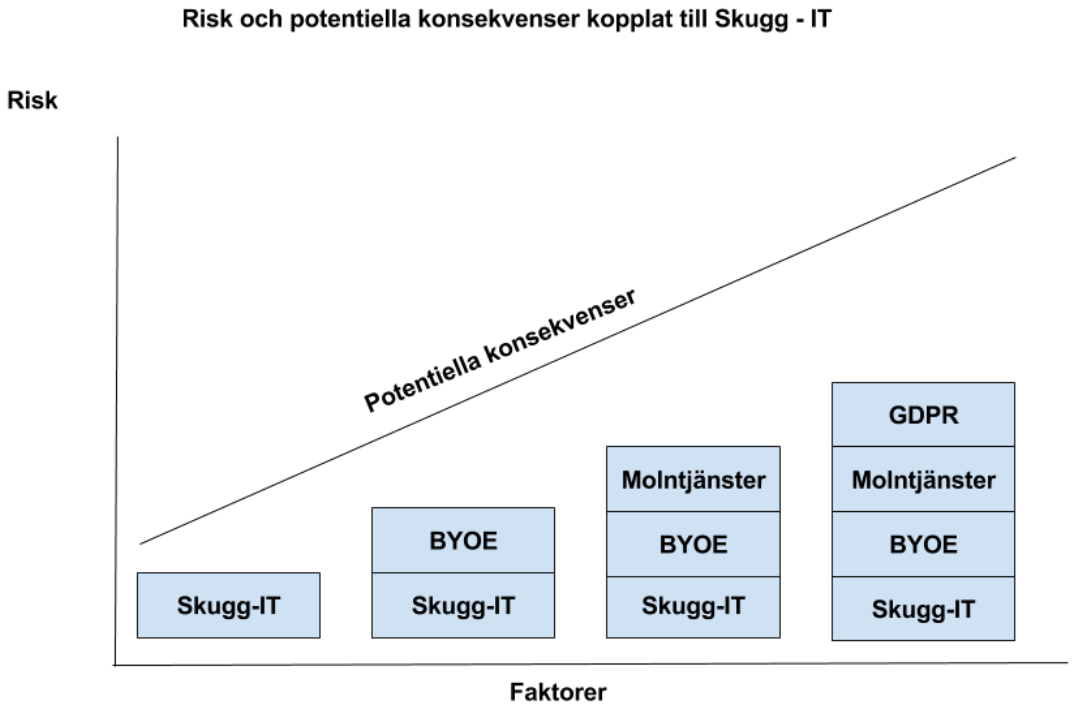
Litteraturstudien sammanfattas i ett teoretiskt ramverk där de mest centrala delarna finns representerade. Dessa sätts även in i en kontext för att påvisa hur dem är relaterade till varandra. Ramverket används som utgångspunkt i utformning av den empiriska studien för att säkerhetsställa dess förankring i litteraturen.

Inledningsvis presenteras en konceptuell modell (Figur 3) över hur komplexitet och potentiella konsekvenser har utvecklats i takt med att flera externa faktorer har tillkommit i miljön skugg-IT verkar i. Därefter sammanfattas de mest centrala delarna från litteraturstudien, dessa konkretiseras slutligen till vårt teoretiska ramverk (Figur 4).

I litteraturstudien har ett antal trender observerats. När fenomenet Skugg-IT började uppstå i organisationer var problemen kopplade till detta relativt begränsade. Den största ursprungliga problematiken var fortfarande att information kan komma på villovägar, framförallt genom att anställda lagrar information på olika lagringsmedier som de senare tappar bort (Walters 2013). I och med BYOE-trenden introduceras ytterligare en dimension som påverkar skugg-IT. Det blir allt vanligare för anställda att ta med egna enheter och applikationer för att använda på arbetsplatsen. Applikationerna som används för med sig ytterligare risker för att information på något sätt skall hamna i orätta händer och organisationens kontroll över den minskar (Silic & Back 2014). Nästa faktor som påverkat skugg-IT är användandet av molntjänster. Molntjänsters distribuerade karaktär gör det betydligt svårare att hålla reda på var informationen faktiskt lagras. Tidigare har riskerna varit mer begränsade men nu kan informationen som lagras finnas var som helst i världen (Walters 2013). Dessutom används molntjänster ofta i kombination med IT som omfattas av begreppet BYOE. Det är viktigt att påpeka att molntjänster i sig inte ökar komplexiteten i en organisations IT-lösning, utan många gånger kan de bidra till en minskad belastning då ansvaret för drift och liknande läggs på en extern leverantör. När vi menar att komplexiteten ökar i modellen är det enbart relaterat till komplexiteten som kan uppstår vid lagring och hantering av information inom ramen för vårt problemområde.

Den senaste faktorn som kommer att påverka skugg-IT är införandet av den nya dataskyddsförordningen. Detta är visserligen inget tekniskt fenomen likt molntjänster och BYOE, men fortfarande en faktor som kommer att påverka skugg-IT genom att förändra miljön inom vilken det verkar. Många detaljer är fortfarande inte helt klara kring hur dataskyddsförordningen exakt kommer att se ut i slutändan. Det är dock klart att kraven på hanteringen av personuppgifter kommer att öka, vilket räcker för att påvisa att omständigheterna förändrats.

Nedan presenteras en modell baserad på litteraturstudien över hur de olika faktorerna påverkar skugg-IT. Faktorerna innefattar inte fenomenen kopplat till sanktionerade lösningar utan bara kopplat till skugg- IT. Desto fler faktorer som spelar in, ju mer ökar både risken organisationen utsätts för och de eventuella konsekvenser som kan uppstå. Konsekvenser definieras som både de som kan uppstå på grund av skugg-IT i sig, och de legala konsekvenser som kan uppstå på grund av att EU:s dataskyddsförordning inte följs. I modellen representerar blocket benämnt "skugg-IT" den traditionella problematiken kopplat till fenomenet som identifierats i litteraturstudien, med andra ord de nackdelar som påvisas senare i ramverket i figur 4.



Figur 3: Risk och potentiella konsekvenser kopplat till Skugg-IT.

För varje faktor som adderas i modellen ökar både riskerna och de potentiella konsekvenserna kopplat till skugg-IT. Inledningsvis beror detta på att organisationerna riskerar förlorar kontroll över sin information och senare de legala konsekvenser som dataskyddsförordningen påför.

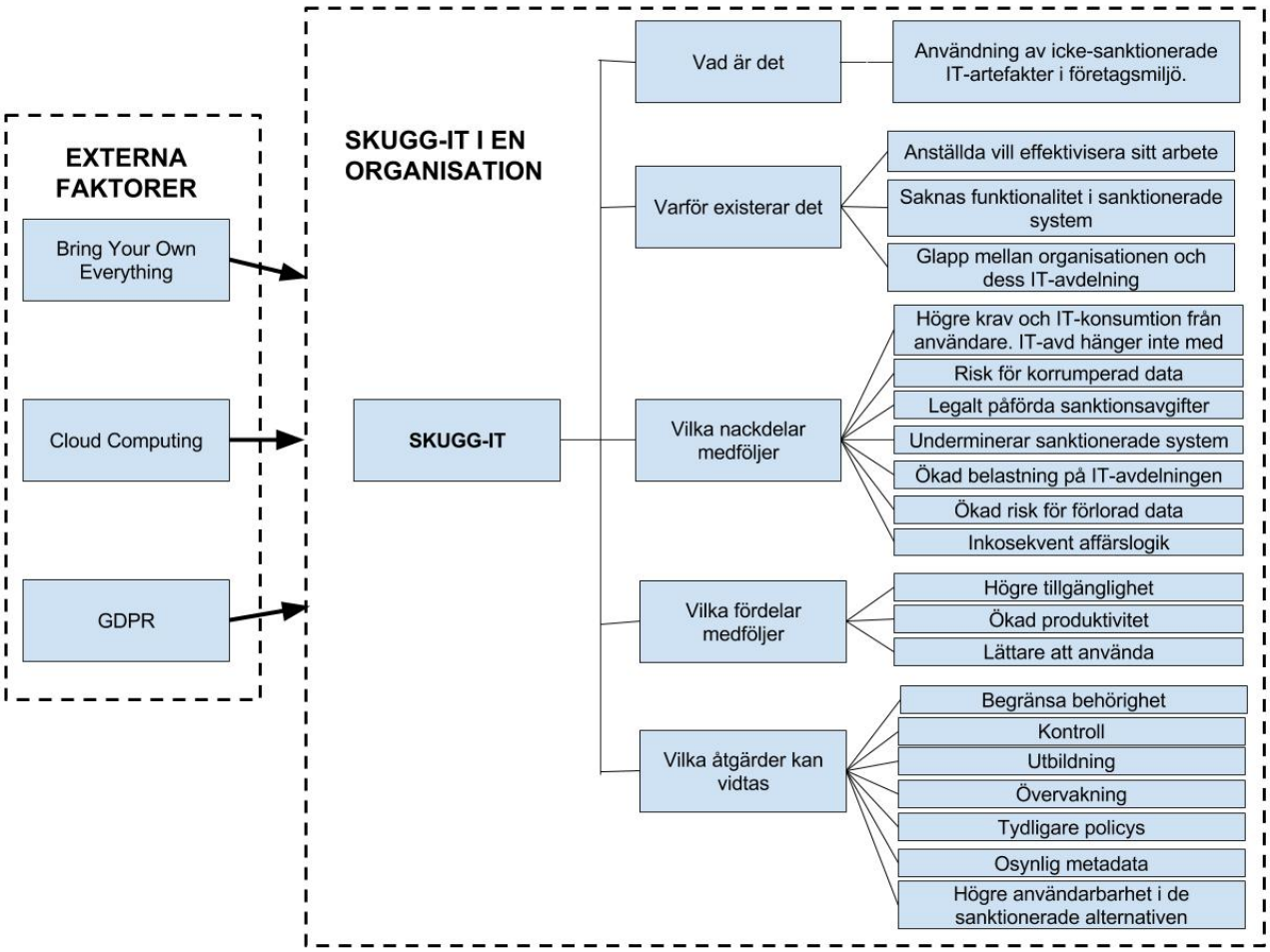
Nedan presenteras de mest centrala begreppen ur litteraturstudien. I kolumnen längst till vänster har de olika fenomenen delats in i teman.

Tabell 1: Sammanfattning av litteraturstudien.

Tema	Litteraturgenomgången gällande Skugg-IT	Referens
Vad är skugg-IT?	- Samtliga IT-artefakter som används i en organisation där användandet inte är kontrollerat och godkänt av en IT-avdelning eller liknande.	Silic & Back 2014
	-Användning av obehöriga applikationer i företagsmiljö och bearbetning samt lagring av företagsinformation på icke-godkända enheter.	Walters 2013
	-Representeras av hårdvara, mjukvara eller någon annan teknisk lösning som används av anställda inom organisationens ekosystem som inte blivit formellt godkänt av IT-avdelningen och inte är grundad i organisationens policys.	Silic, et al. 2017
Varför existerar skugg-IT?	-Skugg-IT existerar för att det finns ett glapp mellan organisationens och IT:ns inriktning.	Silic & Back 2014
	-Skugg-IT förekommer i organisationer när "gapet" mellan vad ett system utlovar och vad användarna av systemet faktiskt behöver är för stort.	Behrens 2004, Silic, et al. 2017
	-Detta grundar sig i att de anställda vill använda verktyg som hjälper dem att utföra sitt arbete på ett bättre och snabbare sätt. Dock ignoreras ofta de negativa konsekvenser som användandet av Skugg-IT kan få.	Walters 2013, Silic & Back 2014
	-Mängden högkvalitativa molntjänster som finns lätt tillgängliga som alternativ för anställda utan IT-avdelningens godkännande.	Roos 2015
Vilka nackdelar medföljer skugg-IT?	Användandet av skugg-IT ökar bland annat risken för inkonsekvent affärslogik, problem med minskad medgörlighet mellan system och ökad risk för att förlora data då datan lagras utspritt.	Silic & Back 2014
	Användningen av skugg-IT har lett till förhöjda krav och förhöjd IT-konsumtion hos anställda. Detta har lett till att många IT-avdelningar har problem med att hålla jämn takt rent utvecklingsmässigt vilket kan resultera i att användningen av skugg-IT fortsätter att öka	Williams 2011
	Skugg-IT lägger extra belastning på IT-avdelningen. Utöver deras vanliga arbetssysslor så kommer problemen som skugg-IT orsakar naturligt förväntas att tas hand om av dem då de är experterna inom området.	Walters 2013
	I vissa fall kan användningen av skugg-IT vara så hårt förankrat hos anställda att de medvetet utsätter organisationen för risker vilket kan leda till väldigt allvarliga påföljder för både organisationen och den ansvarige anställde.	Walters 2013
	Underminerar organisationens vanliga system, drar mycket resurser och kan skada organisationens data och processer.	Behrens 2009

	Sanktionsavgift på fyra procent av organisationens omsättning eller 20 miljoner Euro om inte personuppgifter hanteras på rätt sätt.	Allmän dataskyddsförordning 2016/679 av den 27 april 2016
	Data fragmenteras ytterligare och sprids ut på okända platser både inn anför och utanför organisationens brandvägg.	Micallef 2015
Vilka fördelar medföljer skugg-IT?	De nämner allt från att det är lättare att använda till en högre grad av tillgänglighet och framförallt att fördelarna var lätta att observera vilket gjorde att andra anställda kunde snabbt förstå hur systemet direkt kunde underlätta deras dagliga arbetsrutin.	Behrens 2009
	Öka de anställdas produktivitet.	Silic & Back 2014
Vilka åtgärder kan vidtas mot skugg-IT?	Övervaka organisationens trafik, begränsa åtkomst till vissa webbsidor, justera behörighet så att bara administratörer kan installera program, tydligare policys och mer fokus på utbildning.	Silic & Back 2014
	Erkänn att dem finns, lär från dem och dra nytta av de som fungerar bra. Försök inte kontrollera dem.	Behrens 2009
	Verifiera användare, kontroll och övervakning för att kunna dra nytta av fördelarna med molnapplikationer.	Walters 2013
	Flertalet undersökningar med IT-chefer och ledningspersonal har kommit fram till att det absolut största säkerhetshotet är nuvarande och före detta anställda i organisationen. Hanteras till viss grad av hot om sanktioner.	Silic, et al. 2017
	Osynlig metadata, full kontroll över krypteringsservicen och hög användbarhet i de sanktionerade alternativen.	Micallef 2015
Vilka externa faktorer påverkar skugg-IT?	Molntjänster har blivit betydligt mer populära. Både sanktionerade och icke-sanktionerade.	Netskope 2016, Netskope 2017
	Teknologin har blivit mer komplex och flera dimensioner har introducerats, BYOE har blivit allt mer populärt.	Silic & Back 2014, Walters 2013
	Kraven på hantering av personuppgifter har ökat i och med införandet av den nya dataskyddsförordningen.	Datainspektionen

2.6.1 Ramverk



Figur 4: Modell över det teoretiska ramverket.

3 Metod

Inledningsvis i detta kapitlet beskrivs och motiveras hur undersökningen genomförts och vilka metoder som har använts. Därefter presenteras informanterna som bidragit med empiri till uppsatsen samt vad de har för relevant kompetens. Slutligen redovisar vi vad vi har gjort för att öka kvalitén på uppsatsen genom att diskutera validitet, reliabilitet, etik och urvalet vi har gjort. Målet med detta kapitlet är att ge läsaren en inblick i hela processen för att öka undersökningen trovärdighet och ge andra en möjlighet att replikera den.

Inledningsvis genomförs en litteraturstudie där tidigare forskning på området undersökts för att kartlägga de redan existerande förutsättningar som finns på området och hur de nya förutsättningarna som introduceras med dataskyddsförordningen kan komma att påverka skugg-IT. Som komplement till den akademiska litteraturen undersöks också de rekommendationer och tolkningar av dataskyddsförordningen som Datainspektionen har gjort. En deduktiv ansats har valts då syftet med studien är att studera hur skugg-IT påverkas av en förändring i miljön den existerar i. För att göra detta måste vi först etablera någon form av utgångspunkt för att påvisa hur de nya omständigheterna påverkar fenomenet. Litteraturen som behandlats i litteraturstudien är skriven innan dataskyddsförordningen blivit en faktor och representerar hur skugg-IT tidigare uppfattats (Jacobsen 2002). De tolkningar Datainspektionen hitintills har gjort, tillsammans med resultatet av intervjuerna representerar det nya förutsättningarna. Med en induktiv ansats hade vi haft svårt att avgöra vad som varit relevant för vår studie och riskerat att samla in stora mängder data som vi inte har någon nytta av (Jacobsen 2002).

Litteraturstudien mynnar ut i ett teoretiskt ramverk som innehåller de viktigaste faktorerna kopplat till vårt problemområde. Från ramverket har sedan en intervjuguide utformats, de tidigare efterforskningarna som gjorts i litteraturen ställs mot hur informanterna anser att den nya förordningen kommer att påverka skugg-IT.

Efter litteraturstudien har gjorts utformas ett underlag för att genomföra en pilotintervju. Eftersom det råder många oklarheter och fenomenet skugg-IT är ett relativt svårt ämne att få grepp om, har vi valt en kvalitativ ansats för att få en djupare förståelse för fenomenen vi undersöker. Att försöka göra en kvantitativ undersökning hade till hög grad begränsat oss till att samla in data utifrån den information vi redan har, eftersom relativt lite forskning har gjorts på området skulle det bli svårt att belysa tillräckligt många perspektiv (Jacobsen 2002). En kvalitativ ansats ger oss istället möjlighet att undersöka de olika begreppen på djupet och samtidigt vara öppna för nya perspektiv. Utifrån underlaget från litteraturstudien och de lärdomarna som dragits från pilotintervjun utformas sedan det slutgiltiga intervjuunderlaget.

Vi har inte tolkat dataskyddsförordningen på egen hand, utan använder oss, vid minsta tvivel, istället av Datainspektionens tolkningar på området som sekundärkällor, Anledningen till detta är helt enkelt att vi saknar den kunskapen som krävs för att tolka det på ett adekvat sätt.

Eftersom litteraturstudien genomförts före datainsamlingen finns det risk för att vi har förutfattade meningar om vad som är rätt och fel. Dessutom finns det relativt lite forskning gjort på området, vilket ökar risken för att de källorna som finns ses som någon form av absolut fakta. Att ha semistrukturerade intervjuer och använt andra källor för att undersöka begrepp relaterade

till skugg-IT har bidragit till att vi är öppna för ytterligare perspektiv (Jacobsen 2002). Studien ämnar till att undersöka hur personer som har erfarenhet av skugg-IT och dataskyddsförordningen anser att det kommer påverkas i relation till informationssäkerhet samt problematiken som kommer uppstå med dataskyddsförordningens införande.

3.1 Intervjuer

Frågorna är formulerade på ett sådant sätt så att det är informantens personliga åsikter, baserat på deras tidigare erfarenhet, som undersöks. Alternativet hade varit att formulera dem på ett sätt som undersöker vad organisationen ståndpunkt i de olika frågorna är (Jacobsen 2002). Detta medför dock en risk för att informantens svar färgas av bakomliggande faktorer istället för att förmedla sin egen professionella åsikt. Intervjuerna genomfördes över telefon för att göra det möjligt för så många som möjligt att delta. Dessutom är de personer som besitter den kompetens vi är ute efter ganska få och utspridda rent geografiskt. Inom ramen för vår studie har vi inte haft möjlighet att genomföra intervjuer på plats, både ur ett ekonomiskt och ett tidsmässigt perspektiv.

Jacobsen (2002) påpekar att det är lättare för informanten att ljuga när personen som genomför intervjun inte sitter i samma rum. Det går dessutom inte att avläsa eventuella ansiktsuttryck eller kroppsspråk på informanten när frågorna ställs. Hade vårt ämne varit av en mer personlig karaktär hade en viktig dimension gått förlorad (Jacobsen 2002). Dock är vi enbart ute efter informantens professionella åsikter, detta i kombination med att inte informantens namn eller organisatoriska tillhörighet nämns i resultatet och telefonintervjuns mindre personliga karaktär minskar incitament för att tala osanning (Jacobson 2002).

Vi har valt att genomföra semistrukturerade intervjuer då ämnet vi undersöker är tämligen outforskat och det inte finns något absolut svar på hur den stundande implementeringen av dataskyddsförordningen har, och kommer, påverka skugg-IT. Graden av struktur på en intervju är inte fast utan snarare en glidande skala från helt sluten till helt öppen (Jacobson 2002). Vi har strävat efter att ha så öppna intervjuer som möjligt utan att helt försvinna från själva ämnet.

Intervjun struktureras med hjälp av intervjuguiden i bilaga 2. Enligt Jacobsen (2002) menar somliga att någon form av strukturering strider mot den grundläggande tanken med en kvalitativ forskningsmetod. Vi har som sagt strävat efter att ha så öppna intervjuer som möjligt, men på grund av både tidsbrist och risken för att spendera tid på att samla in alldeles för mycket irrelevant information (Jacobsen 2002) har vi valt att förhålla oss till de sex teman som återfinns i det teoretiska ramverket. Till dessa finns även ett antal underfrågor, som använts som stöd ifall informanten av någon anledning inte kunnat komma på något att säga om ett specifikt tema. Att övergripande teman används har även bidragit till att den data vi samlar in inte bli för inkonsekvent. Fokus har dock legat på att vara så flexibel som möjligt och ge informanten möjlighet att tolka frågorna utifrån sina egna erfarenheter (Bryman 2011). Det har dock varit en avvägning för att hinna genomföra intervjuerna inom den aktuella tidsramen.

3.1.1 Bearbetning av data

Efter intervjuerna transkriberades inspelningarna i sin helhet för att i så stor utsträckning som möjligt behålla den ursprungliga innebörden och kompletterades med relevanta kommentarer.

Transkribering kan vara en tidsödande process (Bryman 2011) men med tanke på vår undersökning ringa omfattning kommer detta inte var något problem. Enligt Bryman (2011) finns det två intressanta dimensioner i en intervju både *vad* intervjupersonen säger och *hur* det sägs. Vår transkribering behandlar endast vad som sägs under intervjun, en bidragande faktor till detta är att intervjuerna genomförts över telefon vilket gör det svårare att observera reaktioner (Bryman 2011). Istället har informantens reaktioner följts upp under intervjun med följdfrågor eller att upprepa eller be dem förklara ett påstående. Under transkriberingen har delar som är relevanta för vårt resultat markerats för att underlätta vidare bearbetning.

3.1.2 Analys av data

För att göra resultatet av intervjuerna överskådligt har vi sammanfattat de viktigaste observationerna i tabeller (tabell 3–9) som bygger på intervjuguidens olika teman. Kategorier som grundar sig i den insamlade datan har tagits fram (Jacobsen 2002). Den insamlade datan analyseras återigen igenom och svar från informanten som berör en kategori abstraheras och förs in under den mest relevanta kategorin (Jacobsen 2002). Därefter identifieras likheter och olikheter mellan de olika informanternas svar i samma kategori. Resultatet från detta ligger till sist till grund för den följande diskussionen.

3.1.3 Informanter

Tabell 2: Informanter.

Informant 1 Pilotintervju **Intervju genomförd** 2017- 04 - 21 **Längd** 34:35	**Roll** Konsult - IT management. **Organisation** - O1 Mindre konsultbolag med <20 anställda och omsättning på <10 000 000 kronor. **Relevant erfarenhet** Informationssäkerhetspecialist med inriktning på den offentliga sektorn. Arbetat med medgörlighet till dataskyddsförordningen inom kommuner.
Informant 2 **Intervju genomförd** 2017- 04 - 26 **Längd** 47:02	**Roll** Senior konsult. **Organisation** - O2 Internationellt konsultbolag med >1500 anställda och omsättning på >2 000 000 000 kronor. **Relevant erfarenhet** Internt certifierad att arbeta med GDPR av O2. Många år som ansvarig för flertalet system inom banksektorn.
Informant 3 **Intervju genomförd** 2017-05-02 **Längd** 34:32	**Roll** Senior IT-revisor. **Organisation** - O2 Internationellt konsultbolag med >1500 anställda och omsättning på >2 000 000 000 kronor. **Relevant erfarenhet** Stött på Skugg-IT i rollen som IT-revisor vid revisioner eller på stora företag i USA. Även vid arbete som linjechef för en större statlig myndighet i Sverige
Informant 4 **Intervju genomförd** 2017-05-08 **Längd** 20:08	**Roll** Informationssäkerhetsansvarig **Organisation** - O3 Privat företag inom välfärdssektorn, omsätter >10 000 000 000 och har >10 000 anställda. **Relevant erfarenhet** Funktionellt ansvarig i organisationers arbete mot GDPR-efterlevnad.

3.2 Undersökningens kvalitet

Vi har hela tiden strävat efter att förutsättningarna inför varje intervju skall vara så lika som möjligt. Detta för att från vårt håll påverka informanten så lite som möjligt (Jacobsen 2002). Samma person har genomfört alla intervjuer. Båda har dock varit närvarande vid samtliga intervjuer. Underlaget har skickats ut i förväg till alla och metoden överlag har varit likadan vid varje intervju. Intervjuerna spelades in för att underlätta bearbetningen av datan Det enda som skiljer sig är innehållet i de olika intervjuerna då dess semi-strukturerade karaktär och vårt flexibla förhållningssätt gör att informanten till viss del kan påverka resultatet av intervjun. För att försäkra oss om intervjufrågornas validitet baseras dem på vårt teoretiska ramverk som är framtaget från litteraturstudien.

3.2.1 Urval

De personer vi har valt att intervjua arbetar på något sätt med informationssäkerhet eller problematiken kopplat till införandet av den nya dataskyddsförordningen. Urvalet har skett målstyrt där vi själva aktivt valt informanter som har erfarenhet av de fenomen vi diskuterar i uppsatsen (Bryman 2011). Vi har dessutom valt att intervjua personer med en mer övergripande blick, till exempel konsulter och personer som kommer i kontakt med fenomenet från olika perspektiv. Detta för att bilda oss en mer generell uppfattning om fenomenet. Skulle endast anställda med ett snävare perspektiv intervjuats finns det risk för att deras åsikter är alltför nyanserade av organisationen de arbetar i och hur fenomenen påverkar just deras verksamhet. Dessutom är ofta ämnen relaterade till informationssäkerhet känsliga. Det kan därför vara svårt att få informanterna att diskutera specifika fall.

3.1.1 Undersökningens validitet och reliabilitet

Enligt Jacobsen (2002) behöver alla former av empiriska undersökningar uppfylla två krav, att den är giltig och relevant (valid) och att den är tillförlitlig och trovärdig (reliabel). Validiteten delas sedan i två kategorier. Intern validitet, som fokuserar på att undersökning skall mäta det vi tror att vi mäter, och extern validitet som innebär att resultatet av undersökningen skall vara generellt gångbart (Jacobsen 2002). I vårt fall representeras detta av att resultatet går att applicera på flera organisationer än de som undersöks då våra informanter har erfarenhet från skilda branscher. Att undersökningen är reliabel innebär att undersökningen går att lita på. Den skall med andra ord vara genomför utan uppenbara mätfel och på ett trovärdigt sätt (Jacobsen 2002). Att vår inställning till dataskyddsförordningen är mer allmän och att den snarare hanteras som en generell ökning av kraven på integritet gör att våra slutsatser i större utsträckning kommer att kunna appliceras på liknande situationer. Hade vi istället fokuserat på specifika delar av förordningen skulle vi riskera att våra slutsatser endast hade gått att tillämpa på detta unika fallet.

I vår undersökning säkerställs den interna validiteten genom att undersökningen är väl förankrad i litteraturstudien. Detta har gjorts genom att intervjuguiden är framtagen utifrån det teoretiska ramverket. Intervjuerna har genomförts individuellt då vi är intresserade av den vad den enskilda informanten, baserat på deras erfarenhet, har för åsikter av ämnet. Vi har dessutom strävat efter att genomföra intervjuerna under så lika förhållanden som möjligt för att minska den externa påverkan, eller den så kallade intervjuareffekten, på informanten (Jacobsen 2002). Eftersom intervjuerna har genomförts via telefon så har påverkan från denna effekt minskat

ytterligare. Dock har vi inte kunnat kontrollera miljön informanten har vistats i. Den externa validiteten säkerställs genom dels genom att ha ett generellt förhållningssätt till dataskyddsförordningen, vi fokuserar inte på specifika detaljer (Jacobsen 2002). Och dels genom att vårt urval där informanterna har en övergripande roll och generell uppfattning om fenomenet. Hade de istället arbetat på en lägre nivå hade risken funnits att de endast fokuserat på sin egen direkta omgivning och resultatet hade inte i lika stor utsträckning vara generellt applicerbart. Två av informanterna arbetar i samma organisation, dock har de i sin roll som konsulter haft olika kunder och arbetar inom olika verksamhetsområden vilket gör att de kan bidra med två olika perspektiv till undersökningen.

Att vi bygger en del av vår studie på en förordning som inte i sin helhet är implementerad än kan påverkar validiteten på vår undersökning. Vissa förutsättningar kan fortfarande ändras fram till datumet då förordningen börjar gälla. För att i så stor utsträckning som möjligt undvika att vår studie påverkas har vi istället för att fokusera på enskilda detaljer så långt som möjligt inriktat oss på vad förordningen kommer att innebära rent generellt så som ökade krav på informationssäkerhet, justerade ansvarsförhållande och möjligheten till att behöva betala omfattande sanktionsavgifter om förordningen bryts.

3.3 Etiska principer

Under undersökningen har fyra grundläggande etiska principer tagits i beaktning. Dessa är informationskravet, samtyckeskrav, konfidentialitetskravet och nyttjandekravet (Bryman 2011).

Informationskravet innebär att informanterna har rätt att vet syftet med undersökningen och att deltagande är frivilligt (Bryman 2011). I vår undersökning har vi från början vara tydliga med undersökningens syfte och har informerat all deltagarna i förväg vad intervjun kommer att handla om genom att ge dem tillgång till en beskrivning av vårt problemområde samt intervjuguiden.

Samtyckeskravet betyder att deltagarna i undersökningen samtycker frivilligt att delta i undersökningen (Bryman 2011). I vår undersökning har varje enskild individ tackat ja till att delta, inga externa påtryckningar från chefer eller liknande har enligt vår uppfattning förekommit. Syftet med undersökningen har dessutom redovisats och ingen dold observation eller alternativa agendor finns.

Konfidentialitetskravet, att uppgifter om informanter hanteras på för att garantera att de uppfyller den högsta möjliga graden av konfidentialitet (Bryman 2011). Alla informanter som deltar i vår studie hanteras med fingerade namn, både själva individen och organisationen de tillhör. Även information som framkommer under intervjuerna som kan användas för att identifiera en enskild person eller organisation tas bort. De inspelningar som finns kommer bara att lyssnas på av författarna av uppsatsen.

Nyttjandekravet uppfylls genom att materialet som samlas in endast används inom ramen för vår uppsats (Bryman 2011).

4 Resultat

Nedan presenteras resultatet från vår empiriska studie. Resultaten av intervjuerna sammanfattas i en tabell för att ge läsaren en bättre överblick över innehållet samt förevisa återkommande resultat i undersökningen. Varje enskilt tema från intervjuguiden har en egen tabell. I tabellen refererar vi till den transkriberade intervjuerna i bilaga 3 genom att först ange vilken intervju vi refererar till och därefter vilket eller vilka stycken (t.ex. I2, 6) Till vänster i tabellen presenteras kategorierna som hanteras. Saknas ett svar för en viss informant och kategori markeras detta med ett X.

Tabell 3: Vad är det?

Kategorier	**Informant 1**	**Informant 2**	**Informant 3**	**Informant 4**
Hur kan skugg-IT förekomma i organisationer?	Stött på det i ganska liten utsträckning i min professionella karriär (I1, 1). Jag tror inte att det är många som har tänkt på att det kan finnas egensnickrade lagringsplatser. Det är ju en jättegrej naturligtvis (I1, 1).	Skuggregister där enskilda anställda som replikerar ut t.ex. personuppgifter (I2, 10). Enskilda använder en egen server, använder molntjänster ingen har koll på. Tillslut skapas en parallell IT-miljö (I2, 10).	Verksamhetsnära utrustning som historiskt sett har varit mer mekanisk och inte räknats som IT är numera nätverksansluten som t.ex. industriutrustning, medicinteknisk utrustning och övervakningsutrustning (I3, 4).	Det finns ju de här Dropbox och de andra lagrings-plattformarna som anställda väldigt enkelt kan skapa ett eget konto och bjuda in kollegor och börja använda det som någon slags kommunikationsplattform. (I4, 8) Medicinteknisk utrustning innehåller i många fall personuppgifter och gör det fram tills att det tas bort. (I4, 6).

Tabell 4: Varför existerar skugg-IT?

Kategorier	**Informant 1**	**Informant 2**	**Informant 3**	**Informant 4**
Enligt informanternas uppfattning, varför uppstår skugg-IT?	Man vill skapa sin lilla egna lagringsplats. Man vill behålla sin kompetens i sin egen sfär som man absolut kan tänka sig att delge sig av men man vill se till att den inte försvinner. Saknas tydliga strukturer och forum för medarbetare att lagra information (I1, 6).	Delar av organisationen inte längre förlitar sig på den centrala IT-organisationen utan börjar göra saker på egen hand (I2, 10). Dåligt förtroende för den centrala IT-avdelningen. Man är trött på beställningstiden, det går snabbare att göra saker själv (I2,12)	Olika avdelningars tillkortakommanden leder till att folk löser problemen på egen hand. Det (skugg-IT) är i regel relaterat till organisationens bristande förmåga att kunna tillhandahålla de verktygen som krävs eller specifik utrustning (I1, 2).	Det uppstår för att det är så enkelt. Säg att man som anställd har ett behov och man vet att det tar tid i de vanliga kanalerna att få en IT-lösning på plats som fyller det behovet så är det väldigt enkelt att använda sig av molntjänster till exempel som fyller samma behov som användaren har. (I4, 8).

Tabell 5: Vilka åtgärder bör vidtas?

Kategorier	Informant 1	Informant 2	Informant 3	Informant 4
Hur bör problematiken med skugg-IT hanteras?	Det övergripande arbetet med informationssäkerhet måste fungera och skapa en kultur av att man tar det på allvar. Arbetet måste förankras i ledningen (I1, 16).	Informera hela företaget vad regelverket (GDPR) innebär, vad syftet är och hur de skall förhålla sig till det och skapa en medvetenhet i organisationen (I2, 16). Kontrollera åtkomst (I2,14).	Finns ett strukturerat informationssäkerhetsarbete som ligger ovanför IT-avdelningen så kommer man även att fånga upp skugg-IT. IT-avdelningen kan inte själva ha hela ansvaret. (I3, 8).	Finns tydligt uppsatta styrande dokument, policys och riktlinjer för vad anställda får och inte får göra. (I4, 4)
Bör skugg-IT hanteras tekniskt eller organisatoriskt?	Man behöver ha ett fungerande informationssäkerhetsarbete (I1, 15). Det är mer än att bygga brandväggar och virusskydd. Det handlar om kultur och att förankra det i ledningen (I1, 16). Den tekniska säkerheten ligger redan på en högre nivå (I1,35).	Illegala personuppgiftsflöden kommer inte att gå att skanna av då företagen har för mycket legacy (I2, 16). Göra god hantering av personuppgifter till en del av företagets kultur (I2, 16).	Organisatoriskt, det är dock inte endast IT-avdelningens ansvar. Det måste ligga högre upp i organisationen (I3, 8).	Vi hanterar det främst organisatoriskt. I vissa delar av verksamheten har vi gjort tekniska uppföljningar för att undersöka vad de anställda använder (I4, 10).

Tabell 6: Vilka fördelar medföljer?

Kategorier	Informant 1	Informant 2	Informant 3	Informant 4
Finns det några positiva aspekter med skugg-IT?	X	Kan användas som ett medel för att komma snabbt fram i affärsutvecklingen (I1, 14). Definiera vilka områden skugg-IT bör vara tillåtet inom (I1, 16).	Tycker inte det finns några som helst fördelar med skugg-IT. Utan skugg-IT är ett symptom på andra brister (I3, 16).	Den positiva effekten är som sagt att det går snabbt och det är en del i innovationen att hitta IT-sätt som gör det lättare och effektivare att arbeta (I4, 12).

Tabell 7: Vilka nackdelar medföljer?

Kategorier	Informant 1	Informant 2	Informant 3	Informant 4
Finns det några negativa aspekter med skugg-IT?	X	Omfattande utmaning att fånga in förekomsten av personuppgiftshantering som inte sker centralt (I2, 10). Personer som inte är IT-kunniga kan lätt skapa problem genom att exempelvis duplicera ett register (I2, 10). Skugg-IT förvränger bilden av organisationens kostnader och effektivitet kopplat till IT. (I2, 26).	Varför ska jag vända mig till min IT-avdelning, om vi säger att det tar ett och ett halvt år att ta fram ett nytt IT-system där jag kan hitta en viss information i min telefon, när den appen redan finns klar och tillgänglig att hämta. Då tror man att ens IT-avdelning är dålig och att den inte kan leverera (I3, 16).	Det finns ju risk kopplat till molntjänster som inte bara är kopplat till säkerhet utan även att man inte har rätt avtal på plats som beskriver hur personuppgifter får hanteras och så vidare (I4, 10).

Tabell 8: Externa faktorer (GDPR, Cloud computing, BYOE).

Kategorier	Informant 1	Informant 2	Informant 3	Informant 4
Hur har GDPR påverkat skugg-IT som fenomen?	Fört fram problematiken i rampljuset, märks på efterfrågan av konsulttjänster inom området. I med att medvetenheten ökar tvingas organisationer se över var de lagrar sin information, skugg-IT involveras i detta arbetet (I1, 4).	Att man som organisation bör vara hårdare mot vissa typer av skugg-IT. Ok med viss data men inte annan, exempelvis personuppgifter (I2, 16).	Hjälpa till med kostnadsanalysen, tidigare har det inte funnits en konkret summa som behöver betalas om information försvinner. Tidigare kunde man strunta i detta utan några större konsekvenser. Du kan fortfarande strunta i det, dock riskerar du en hög sanktionsavgift (I3, 10).	Inte till så stor grad. Har redan en hög mognadsgrad och lång vana av hantering av personuppgifter i deras organisation. Möjligtvis så kommer antalet interna medarbetarutredningar öka (I4, 16).

Hur kommer sanktionsavgifterna påverka organisationer?	Böter kommer inte börja delas ut med en gång, det kommer dock leda till ett tuffare klimat (I1, 4).	Datainspektionen har inte kapacitet att kontrollera alla. Böter kommer således inte börjas delas ut med en gång (I2, 12). Sanktionsavgiften i sig är inte relevant. Rykte och att eventuellt tappa kunder kommer ha större påverkan (I2, 16).	Osäker på hur, vet dock säker att det har gjort det. "Jag har aldrig haft något uppdrag rörande PUL exempelvis men nu får jag jobba hela dagarna överallt med GDPR". Har en positiv påverkan på företagens vilja att göra något (I3, 12). Tror inte att någon i juni 2018 kommer få 20 miljoner euro i böter (I3, 14).	Sanktionsavgiften är väl den stora nyheten sett till dataskyddsförordningen. För i övrigt så är det väldigt likt nuvarande regelverk, finns vissa ytterligare tillägg om rapportering av incidenter och så vidare (I4, 20). Sanktionsavgifterna är inget som driver compliance-arbetet. Det värsta som kan hända är att tappa kunder på grund av att de tappar förtroendet I4, 20).
Hur har BYOE påverkats?	Problematiken kommer att komma upp till ytan när organisationer tvingas kartlägga var de lagrar sin information med införande av GDPR (I1, 18).	Finns det tillräckligt bra alternativ i organisationen finns det ingen anledning att ta med egen IT (I2, 18).	Stort problem. Är så pass kostnadseffektivt så det kommer förmodligen fortsätta att förekomma (I3, 10).	I koncernövergripande policys och regelverk så säger vi att vi inte tillåter egna devices. Specifika affärsområden kan dock besluta om undantag, där de i sådana fall måste upprätta en policy för hur BYOD får användas (I4, 22).
Hur har molntjänster påverkats?	Molnanvändningen kommer nog inte gå tillbaka. I många fall har nog t.ex. Microsoft bättre koll på informationen än organisationen som äger den (I1, 51).	Tillräckligt bra molnlösningar inom organisationer förebygger skugg-IT. Det bästa är interna molnlösningar, då vet man var informationen finns (I2, 20).	Många saknar kontroll över var och hur informationen lagras. Samma företag har ofta traditionellt saknat kontroll över sin information även i sina interna miljöer (I3, 18).	Kommer fortsätta som de alltid gjort. Har journalsystem för mindre verksamheter i molnet. Ser inte molntjänsterna som större risk än vanliga IT-system (I4, 26).
Hur kommer molnleverantörerna påverkas?	Mer gemensamt fördelat ansvar. Dialogen mellan de olika parterna kommer bli bättre (I1, 47).	De stora leverantörerna kommer inte ha några problem att anpassa sig. Om de inte gör det kommer de inte ha en chans (I2, 20).	Det kommer dyka upp fler och bättre molntjänster. Det är en konkurrensfördel att vara så GDPR-complaint som möjligt (I3, 22).	Har framställt en checklista över krav på molntjänstleverantörer då de förutspår att molntjänster kommer fortsätta att bli populärare. Denna listan utgör arbetet som utförs innan avtal med leverantörer ingås (I4, 26, 28).
Hur kommer organisationer behöva förhålla sig till personuppgifter?	Det är individens perspektiv man måste ha på det här då lagen är till för oss vanliga medborgare (I1, 22).	"Man ska inte ha GDPR-utbildningar utan utbildningar som handlar om värdering med fokus på personuppgifter" (I3, 34).	Måste inse att det inte är företagets information, Många företag har inte förstått att de hur länge som helst har suttit med andras information (I3, 14).	X

5 Diskussion & Analys

I detta kapitlet jämför vi det empiriska resultatet med våra teoretiska efterforskningar och presenterar likheter, skillnader och intressanta fynd. Vi har valt att behålla liknande rubricering som i litteraturgenomgången för att stärka samt göra det enkelt att följa den röda tråden.

5.1 Metodkritik

Relativt få enheter har undersökts, dels beroende på svårigheter att hitta informanter med relevant kompetens kopplat till både skugg-IT och dataskyddsförordningen, och dels för att tidsåtgången kring administrationen kring intervjuerna och analysarbetet riskerade att gå ut över kvalitén på den övriga uppsatsen. Dessutom upplevde vi redan vid den fjärde intervjun att andelen nya poänger och perspektiv på fenomenen hade minskat. Vilket enligt Jacobsen (2002) är vanligt förekommande vid öppna intervjuer. Informanterna var överens i många frågor och skulle ytterligare en eller två intervjuer genomförts hade de antingen ytterligare bekräftat resultatet eller motsatt sig det. Om det motsatt sig resultatet från de andra intervjuerna hade det dock inte räckt för att avfärda något fyra andra informanter påpekat eller påverkat slutsatsen. Det hade däremot kunnat bidra med ytterligare nyanseringar av begreppen vi har behandlat.

5.2 Skugg-IT

Att Skugg-IT är ett stort problem för organisationer är samtliga av våra informanter överens om. Problemet har under lång tid varit i skymundan men kommer bli mer uppmärksammat i samband med introduktionen av dataskyddsreformen. En av våra informanter uttryckte sig såhär:

> *"Jag tror att skugg-IT kommer hamna mer under luppen ifall du förstår vad jag menar, det kommer hamna mer i rampljuset. Det kommer komma upp till ytan den här sortens problematik.*
>
> - Informant 1 (I1, 4)

Den ursprungliga problematiken som kännetecknar skugg-IT är svårigheterna att kartlägga och bevaka vart information faktiskt lagras. I och med införandet av dataskyddsreformen kommer detta få ökad betydelse då organisationen skall säkerställa att tillräckliga åtgärder vidtas för att skydda personuppgifterna.

I litteraturgenomgången presenteras framförallt skugg-IT som applikationer och enheter som innefattas av begreppet BYOE (Silic & Back 2014), molntjänster (Walters 2013) och större skuggsystem (Behrens 2009). Under en av intervjuerna påpekar informant 3 att personuppgifter även återfinns i verksamhetsnära utrustning inom industrin och vården. Exempel på detta kan vara övervakningskameror, dialysmaskiner och styr- och reglerteknik. Även informant 4 bekräftar att det kan finnas risker med denna typ av utrustning. Enligt informant 3 har denna

typen av utrustning traditionellt sett inte räknats som IT, men i med den tekniska utvecklingen styrs dem numera av datorer och är nätverksanslutna. Utrustningen riskerar att hamna i ett gränsland mellan att vara sanktionerad och icke-sanktionerad om inte organisationen har kunskap om hur den fungerar och vilken information den lagrar. Den kan vara sanktionerad av organisationen i sitt ursprungliga förfarande och för sin huvudsakliga uppgift men inte som ett lagringsmedium av information och personuppgifter. Om vi återgår till den ursprungliga definitionen av skugg-IT enligt Silic & Back (2014); skugg-IT innefattar samtliga IT-artefakter som används i en organisation där användandet inte är kontrollerat och godkänt av en IT-avdelning eller liknande ser vi att definitionen inte stämmer in på detta fenomenet. Dels är det inte säkert att utrustningen räknas som en IT-artefakt och dels finns det risk att den faktiskt är sanktionerad av organisationen. Inte heller Walters (2013) definition; Skugg-IT är användning av obehöriga applikationer i företagsmiljö och bearbetning samt lagring av företagsinformation på icke-godkända enheter, stämmer in på det nya fenomenet.

5.3 Uppkomsten av skugg-IT

Hur skugg-IT uppkommer är både informanterna och litteraturen som behandlats i uppsatsen till stor del överens om. När gapet mellan vad ett system kan leverera och vad användarna vill ha kommer dem att börja använda icke-sanktionerade verktyg för att fylla luckan (Behrens 2004). Silic & Back (2014) presenterar också en liknande förklaring; skugg-IT uppstår då den IT-lösningen som erbjuds inte är tillräcklig för att på ett bra sätt uppfylla verksamhetens mål. Phil Hagen, som citeras i Yeadons (2016) artikel, anser att skugg-IT kommer från IT-avdelningars ovilja att acceptera nya enheter och applikationer. Eftersom det anses för omständligt att gå via dem börjar helt enkelt de anställda att använda egna IT-artefakter på eget initiativ. Utifrån ett informationssäkerhetsperspektiv är det med andra ord intressant för organisationer att motivera sina anställda att använda deras sanktionerade verktyg, lyckas inte detta ökar risken att skugg-IT introduceras i organisationen.

Att viss funktionalitet inte existerar är inte det enda problemet som finns. Vet inte användarna *att* eller *hur* en viss funktion skall användas uppstår samma problematik. Informant 4 säger att skugg-IT förekommit i deras organisation på grund av att de anställda efterfrågat en viss funktionalitet som de inte trodde fanns i det sanktionerade systemen. Det visade sig dock att det gjorde det. Luckan mellan vad de anställda efterfrågade och de sanktionerade lösningarna uppkom på grund av de anställdas uppfattning att funktionaliteten de efterfrågade inte fanns. Något som återkommer både i intervjun med informant 2 och 4 är de anställdas vilja att göra utföra uppgifter snabbare. Den enda avvikande åsikten framkom under intervju med informant 1 som påpekade att det finns möjlighet att anställda vill hålla information för sig själva. Detta, har dock inte framkommit i någon av de andra intervjuerna eller i teorin.

Som tidigare påpekats kan utrustning som traditionellt sett inte räknats som IT i efterhand få kapacitet att lagra personuppgifter. Skugg-IT kan således också skapas genom att traditionell utrustning utvecklas och ändrar karaktär. Informant 4 är väl medveten om problematiken och åtgärder vidtas i deras organisation för att ta bort personuppgifter i denna typ av utrustning inom en rimlig tidsperiod. Eftersom organisationen i fråga är ett vårdföretag är mycket av deras verksamhet beroende av behandling av personuppgifter. Detta har bidragit till en ökad medvetenhet om problematiken kring personuppgiftshantering och deras medicinska utrustning har involverats i det ordinarie informationssäkerhetsarbete. Har organisationen ingen liknande tradition av omfattande personuppgiftsbehandling finns det risk att detta överses.

5.3.1 För- och nackdelar med Skugg-IT

Ett utbrett användande av skugg-IT kan enligt den teoretiska studien innebära många nackdelar för en organisation. Den mest centrala delen inom ramen för vår uppsats är risken att personuppgifter förloras då den lagras utspritt på platser som inte organisationen har någon kontroll över (Silic & Back 2014). Att fånga in och få kontroll på personuppgiftslagring som inte sker centralt är en stor utmaning enligt informant 2. Informant 2 påpekar också att det är väldigt lätt för en enskild individ med låg eller ingen IT-kompetens att kopiera personuppgifter och lagra dem vart de behagar. Detta påvisar en av det största problemet med att kontrollera skugg-IT kopplat till personuppgiftshantering. Enskilda individer kan med några få musklick kopiera och placera personuppgifter i stort sett var som helst i världen.

Den snabba tekniska utvecklingen har gjort att många har vant sig vid att alltid använda de senaste enheterna och applikationerna. Detta gör att många även vill använda dem i sitt arbete, både beroende på att de upplever att de arbetar effektivare och de är vana vid den senaste teknologin (Williams 2011). De IT-avdelningar som ansvarar för att ta fram nya verktyg har ofta svårt att följa med i utvecklingen och gör dem inte det ökar risken för att de anställda helt enkelt går förbi dem och börjar använda sina egna enheter och applikationer i organisationen (Williams 2011). Kan inte IT-avdelningen leverera den funktionalitet som efterfrågas sjunker förtroendet för den ytterligare och risken finns att anställda i större utsträckningar förlitar sig på skugg-IT. Informant 3 uttrycker sig enligt följande:

> *"Varför ska jag vända mig till min IT-avdelning, om vi säger att det tar ett och ett halvt år att ta fram ett nytt IT-system där jag kan hitta en viss information i min telefon, när den appen redan finns klar och tillgänglig att hämta. Då tror man att ens IT-avdelning är dålig och att den inte kan leverera och det ligger ju något i det."*
>
> - Informant 3 (I3, 16)

Att säkerheten i de icke-sanktionerade tjänsterna uppfyller organisationens krav kan inte garanteras. Ignoreras de officiella kanalerna för framtagande av IT-lösningar förbises enligt informant 4 dessutom de avtal som existerar kopplat till personuppgifter.

De fördelar som skugg-IT bidrar med är framförallt kopplat till den enskilde individens effektivitet. Detta är både informant 2 och 4 överens om. Även Behrens (2009) anser att skugg-IT kan vara till hjälp för att underlätta det dagliga arbetet. Informant 2 är den enda av våra informanter som till större grad är positivt inställd till skugg-IT och anser att skugg-IT i kontrollerade miljöer kan vara ett medel för att snabbare komma fram i affärsutvecklingen. Genom att strikt definiera vad som är tillåtet att göra går det att dra nytta av skugg-IT:s informella karaktär för att snabbt utveckla ytterligare funktionalitet eller anpassa sig efter en kunds önskemål.

5.3.2 Hantering av skugg-IT

I vår uppsats har vi delat in undersökningen i två olika övergripande metoder för att hantera skugg-IT, tekniska och organisatoriska. Den enda förekomsten av någon teknisk åtgärd framgick under intervjun med informant 4. Där de i delar av organisationen använt tekniska åtgärder för att skanna nätverk och identifiera vilka molntjänster som används. Efter detta utreds syftet med användandet, om det är för privata eller för företagsändamål. Om den anställde använt en icke-sanktionerad molntjänst klargörs varför detta har hänt och den anställda informeras om organisationens sanktionerade alternativ, som enligt informant 4 erbjuder samma funktionalitet som motsvarar externa molntjänster. Det huvudsakliga syftet med dessa tekniska åtgärder är alltså att identifiera förekomsten av skugg-IT och utreda varför det förkommer, inte att på något sätt förhindra förekomsten. De tekniska åtgärderna kan alltså ses som reaktiva och de organisatoriska som proaktiva. Organisationer utan ett etablerat informationssäkerhetsarbete kan tvingas till att ta reaktiva åtgärder, ur ett längre perspektiv är dock den enda lösningen att etablera ett fungerande övergripande informationssäkerhetsarbete.

Samtliga informanter är överens om att skugg-IT bör bäst hanteras genom ett strukturerat, övergripande, informationssäkerhetsarbete i organisationen. De är även överens om att arbetet skall vara förankrat i ledningen för att ha möjlighet att driva igenom det och syftet skall vara att skapa en medvetenhet och kultur i organisationen där personuppgiftshantering värderas högt. Att med hjälp av tekniska åtgärder försöka kontrollera skugg-IT är ytterst komplicerat. Förekomst av skugg-IT är ofta i stor utsträckning okänd för organisationen och existerar i varierande former. Dessutom kan enskilda anställda, medvetet eller omedvetet, introducera skugg-IT i organisationen. Med detta i åtanke blir det svårt att med hjälp av tekniska åtgärder kontrollera skugg-IT.

Tekniska åtgärder kan användas som ett komplement eller för att identifiera förekomst men inte som någon universallösning. Informant 2 beskriver detta enligt följande:

> *"Det finns säkert firmor som kommer såhär och säger 'Hej vi har köpt en produkt som du kopplar in i nätverket och den kommer scanna alla paket och så kommer vi kunna se om de innehåller personnummer.' Att man på det sättet skulle kunna identifiera illegala personuppgiftsflöden då så att säga. Den typen av produkter kommer inte funka då de flesta företag har så mycket legacy och är så spretiga att om du startade ditt företag i fredags med unix-plattform och allting utvecklat i JAVA, då kanske du kan fånga upp sådant men inte på ett stort företag, inte en chans."*
>
> - Informant 2 (I2, 16)

Även Silic & Back (2014) poängterar att behörighetskontroll, övervakning och att begränsa användarna till att använda vissa webbsidor kan användas som verktyg för att hantera skugg-IT. Dessa åtgärder har dock visat sig vara ineffektiva och det egentliga problemet är att användare inte förstår vad användande av skugg-IT kan få för några konsekvenser. Fokus bör enligt Silic & Back (2014) ligga på att tydliggöra policys och utbildning för att öka användarnas medvetenhet.

Problematiken ökat ytterligare då dataskyddsreformen tas med i beräkningen. Enligt informant 2 måste den enskilde individen ha en grundläggande förståelse för vad syftet med den nya lagstiftningen är och själv kunna agera korrekt. Syftet är i slutändan att skydda enskilda personers integritet. Detta måste kommuniceras ut och förståelsen för att det är andras information som hanteras måste öka enligt informant 3. Även informant 1 och 2 är inne på samma spår, fokus bör ligga på värderingar kopplat till personuppgiftshantering, inte på lagen i sig. När samtliga har insett hur både skugg-IT kan få för några konsekvenser och hur viktigt behandling av personuppgifter, är kommer organisationen ha en bra utgångspunkt för att hantera skugg-IT.

5.3.3 Dataskyddsförordningen och skugg-IT

Vare sig personuppgifter lagras inom ramen för vad det som räknas till de klassiska definitionerna av skugg-IT eller inte. Så är det huvudsakliga problemet kopplat till informationen som lagras, inte vad det är för enhet som informationen lagras på. Walters (2013) är också av uppfattningen att det är informationen som är de mest intressanta i sammanhanget.

Detta har tidigare inte varit ett lika omfattande problem. Det har funnits regler för hur personuppgifter skall behandlas, ändå har dessa inte följts till någon större utsträckning enligt informant 1 och informant 3. Eftersom det inte har funnits någon vilja att följa reglerna har det heller inte funnit något behov av att ha kontroll på var informationen lagras. Straffen i PUL (Högsta Domstolen 2013) är inte alls lika omfattande för organisationer som de i dataskyddsförordningen. Informant 1 säger under intervju att efterfrågan på konsulttjänster har ökat, även informant 3 har märkt av detta och uttrycker sig tydligt:

> *"Men det jag kan säga med stor säkerhet är att det har påverkat marknaden i Sverige avsevärt. Därför jag har aldrig haft något uppdrag rörande PUL exempelvis, men nu får jag jobba hela dagarna överallt med GDPR."*
>
> - Informant 3 (I3, 12)

Med andra ord har många organisationer insett att det faktiskt behöver göra något åt deras lagring av personuppgifter. Om detta endast är kopplat till eventuella sanktionsavgifter råder det delade meningar om. Alla är dock överens om att det inte kommer att börjas dela ut böter den närmsta tiden efter förordningen införs. Detta baseras på informant 3 som pekat på hur liknande lagar har behandlats (HIPAA, som är ett regelverk för att skydda patienters personliga hälsoinformation i USA.) och informant 2 som påpekar att Datainspektionen knappast har resurser att följa upp hur personuppgifter hanteras i Sverige. Däremot är det fortfarande hotet om sanktionsavgifter som verkar vara den faktorn som realiserar och konkretiserar förordningen. Informant 3 anser att sanktionsavgiften kommer att hjälpa till med kostnadsanalysen, till skillnad från innan finns det en konkret summa som ledningen måste förhålla sig till. Antingen struntar ledningen att vidta några åtgärder och riskerar en hög sanktionsavgift, eller så ser de till att deras behandling av personuppgifter följer kraven. Det finns ytterligare en motivationsfaktor som organisationer behöver ha i åtanke.

Få vill anlita organisationer som inte har ett hållbart miljöarbete eller ett etiskt förhållningssätt till sin omgivning. Informant 2 berättar sitt perspektiv:

> *"Det är lika självklart för oss som att vi ska välja porslinsmuggar istället för pappersmuggar och så vidare. Vi har inga ambitioner att dyka upp i Dagens Industri eller Expressen där det står att vi har registrerat fel typ av information."*
>
> - Informant 2 (12, 16)

Enligt informant 3 skulle en god behandling av personuppgifter på samma sätt kunna bidra med konkurrensfördelar till organisationer som värderar den enskilde individens integritet högt. Även informant 2 anser att det inte är sanktionsavgiften som är det organisationer bör fokusera på utan det är deras rykte och att eventuellt tappa kunder som kommer vara det största problemet. Sanktionsavgifterna är inte heller något som driver organisationen informant 4 arbetar för i deras arbete med dataskyddsförordningen och poängterar att det värsta som kan hända är att de förlorar kunder och patienter för att de inte litar på att de hanterar deras personuppgifter på rätt sätt.

Samtliga informanter är överens om att det inte är någon idé att stirra sig blind på sanktionsavgiften i sig. Lagens syfte är inte att bötfälla organisationer för att de gör fel utan att skydda den enskilde individens integritet. Enligt informant 3 har många organisationer inte förstått att personuppgifter faktiskt är andras information, utan behandlat den som om det var deras egen. Informant 2 påpekar också att det inte är utbildning i lagen i sig organisationer behöver, utan utbildningar med fokus på värderingar kopplat till personuppgiftsbehandling. Arbetet med detta, som ur individens perspektiv innebär personlig integritet kommer från organisationens håll hanteras som informationssäkerhet.

5.4 Informationssäkerhet

Våra informanter är överens om att hanteringen av skugg-IT bör involveras i det övergripande informationssäkerhetsarbetet och att det bör hanteras främst organisatoriskt. Informant 2 påpekar vikten av att skapa en medvetenhet i organisationen kring hela kedjan som bearbetas i informationssäkerhetsarbetet. Informant 3 påpekar dock att om anställda inte erbjuds ett bättre eller åtminstone lika bra alternativ så kommer de fortsätta välja skugg-alternativen. Folk vill vara effektiva och de vill göra rätt. Men tvingas dem att välja så kommer de välja effektivitet. Det som kan balansera detta är kunskapsförståelse och organisationen måste göra det lätt för anställda att välja rätt.

Vad empirin och teorin kommer fram till pekar stort sett på samma sak. Informationssäkerhetsarbetet bör starta från grunden och genomsyra hela organisationen och det räcker inte att förlita sig på enbart tekniska lösningar (Bulgurcu et al. 2010). Informanterna instämmer med detta och två av dem säger följande:

> *"Det är mycket mer än att bara bygga upp brandväggar och virusskydd, det vill jag säga. Det handlar om att skapa en kultur av att man tar det på allvar och att det är förankrat i ledningen"*.
>
> - Informant 1 (I1, 16)

> *"Illegala personuppgiftsflöden kommer inte att gå att skanna av då företagen har för mycket legacy"*.
>
> - Informant 2 (I2, 16)

Efterlevnad av informationssäkerhetspolicys är en av de viktigaste resurserna i informationssäkerhetsarbetet (Bulgurcu et al. 2010). Det intressanta är vem som ska se till att efterlevnad sker. Det kan vara IT-avdelningen, närmsta chefen eller så genomsyrar ansvaret hela organisationen. Informant 3 påpekar:

> *"Finns ett strukturerat informationssäkerhetsarbete som ligger ovanför IT-avdelningen så kommer man även att fånga upp skugg-IT. IT-avdelningen kan inte själva ha hela ansvaret."*
>
> - Informant 3 (I3, 8)

Skugg-IT kan uppstå var som helst i en organisation, en enskild anställd kan använda sin egen enhet i arbetet eller en avdelning kan börja använda ett mer omfattande icke-sanktionerat system. För att hantera skugg-IT behöver hela organisationen vara medvetna om problematiken. Arbetet bör givetvis utgå från och initieras av ledningen. Ett strukturerat informationssäkerhetsarbete som är förankrat i ledningen med solidariskt ansvar för efterlevnad i hela organisationen är ett starkt tillvägagångssätt för att efterfölja dataskyddsförordningen och dess krav.

Ur den enskilda individens perspektiv så är deras integritet den viktigaste punkten medans ur organisationsperspektivet så är det snarare en del av det övergripande informationssäkerhetsarbetet. Informant 3 hade en intressant synpunkt som visar på skillnaden som kan påvisas när individperspektivet, det vill säga integritet, kan glömmas bort i det omfattande informationssäkerhetsarbetet.

> *"En sak med GDPR som jag tycker många missförstår när jag är ute hos dem och det jag tycker är intressant med GDPR ur ett informationssäkerhetsperspektiv är att det skär rakt igenom allt i organisationen därför det är inte min information, man glömmer bort när man börjar fundera på hur man ska göra att det är någon annans information."*
>
> - Informant 3 (I3, 14)

Eftersom dataskyddsreformen delar individperspektivet, det vill säga att den personliga integriteten ligger i fokus. Så är det som informant 3 påpekar intressant. Slutsatsen vi drar av detta är att företag bör överväga att skifta fokus till ett mer individperspektiv och respektera faktumet att de bara medlar och behandlar och inte äger personuppgifterna.
Detta ligger mer i linje efter vad dataskyddsreformen vill åstadkomma och kan effektivisera arbetet för att åstadkomma eftergivenhet. Avslutningsvis så bekräftar informant 1 delvis detta när vi diskuterade om hur organisationer kommer behöva förhålla sig till personuppgifter i framtiden:

> "*Jag tror det är lätt att en organisation går in i det här arbetet och ser 'okej hur kan det här gynna oss'. Den sortens tänk är ju helt fel, det är individens perspektiv man måste ha på det här då lagen är till för vi vanliga medborgare."*
>
> - Informant 1 (I1, 22)

Om den aktuella organisationen har någon tradition av en starkt etablerad informationssäkerhet bidrar det i stor utsträckning till dess förmåga att hantera skugg-IT kopplat till de nya kraven på integritet. Enligt informant 3 har få företag som de kommer ut till någon kontroll över sin information, inte heller i sina egna interna miljöer och har aldrig haft det. Informant 3 påpekar att det finns de som har bra kontroll på sin information, men de behöver sällan deras konsulttjänster. Informant 4 beskriver sin organisation, som är ett stort företag inom vården, där det finns en lång tradition av personuppgiftsbehandling. Deras verksamhet kräver en omfattande behandling av personuppgifter och patienternas integritet är en viktig del av verksamheten. Enligt informant 4 hanterar redan deras riktlinjer och policys den problematik som kan uppstå när skugg-IT möter dataskyddsförordningen.

5.5 Bring Your Own Everything

Våra informanter är till stor del överens om att BYOE försvårar arbetet mot efterlevnad till dataskyddsförordningen. Walters (2013) styrker detta och säger att den moderna utvecklingen har försvårat problematiken. Specifikt gällande användarnas egna enheter så uttryckte informant 3 extra oro för att detta fenomen skulle överleva trots striktare policys och hot om sanktioner.

> *"Ja det här är ett jätteproblem. Det stora problemet är att det är så pass kostnadseffektivt så vi kommer att fortsätta med det. Jag kan köpa en telefon till en anställd för fyratusen kronor och så har jag tiotusen anställda. Eller så säger den anställde 'Nej men jag har en egen som är mycket modernare och coolare som jag tycker är roligare att jobba med'. Då kostar det mig ingenting. Pengarna styr ganska mycket och man har ganska dålig koll på riskhanteringen. "*
>
> - Informant 3 (I3, 10)

Användandet av egna enheter i tjänsten kan vara sanktionerat i vissa fall och då existerar inte samma problematik. Informant 4 beskriver deras organisation där de helt förbjudit anställda att

använda egna enheter i tjänsten. Specifika affärsområden kan dock besluta om undantag. För att göra detta krävs de specifika policys och kontroller av enheternas mjukvara, operativsystem och antivirus-skydd. Dock så är det svårt att ha kontroll över allt som de anställda gör och information som överförs från sanktionerade system på deras enhet skulle exempelvis automatiskt kunna laddas upp på deras privata lagringsinstanser (Miller et al. 2012).

Vad gäller mjukvara som används på eget bevåg så argumenterar Walters (2013) för att anställda som arbetar med information som är skyddad av diverse regelverk måste vara informerade om att detta är strängt förbjudet. Detta är såklart inget som garanterar att anställda kommer avstå från att använda icke sanktionerade tillvägagångssätt som förenklar deras arbete. Informant 2 upplyser om hur det är möjligt att få sina anställda att välja rätt och att det handlar om att hålla en modern arbetsmiljö. Kan organisationen erbjuda tillräckligt bra verktyg kommer inte de anställda ha någon anledning till att använda egna enheter och applikationer.

> *"Det beror lite på hur modernt företag man har. Men om man går mot att workplacemiljön och den personliga lagringen är molnbaserad och du kör Office 365 eller du kör Sharepoint eller sådär, då är problemet ganska litet. Finns ingen anledning för mig att lagra det på min Ipad när jag ändå är connectad till ett cloud. "*
>
> - Informant 2 (I2, 18)

Detta bekräfta Behrens (2004) teorier om hur skugg-IT uppstår. En stor motivationsfaktor till att en organisation håller koll på vilka enheter och mjukvaror de anställda använder är sanktionsavgifterna i dataskyddsreformen som kan medfölja vid eventuell felhantering av personuppgifter.

5.6 Molntjänster

Walters (2013) är tydlig med hur molntjänster och dess komplexitet bidrar till svårigheterna med informationshantering. Eftersom molnet är så pass abstrakt och av en distribuerat karaktär så kan data befinna sig på flera olika geografiska platser och även flyttas runt mellan olika fysiska lagringsplatser. Om det dessutom är molntjänster som är icke-sanktionerade så har organisationen nästintill ingen kontroll över var informationen lagras. Enligt Netskope (2017) så visar molntjänster inga tecken på att bli mindre populära utan fortsätter att öka i användning. Informant 3 bekräftar de svårigheter med molntjänster som teorin tar upp, men tar även upp ett intressant perspektiv att det kan föreligga en företagskultur med undermålig informationshantering:

> *"Många saknar kontroll över var och hur informationen lagras. Samma företag har ofta traditionellt saknat kontroll över sin information även i sina interna miljöer."*
>
> - Informant 3 (I3, 18).

Våra informanter är dock positivt inställda till molntjänsternas framtid i samspel med dataskyddsreformen och tror på att det kommer dyka upp bättre och säkrare molntjänster som hjälper till att förebygga skugg-IT.

> *"Det kommer dyka upp fler och bättre molntjänster. Det är en konkurrensfördel att vara så GDPR-complaint som möjligt."*
>
> - Informant 3 (I3, 22)

Informant 1 samt informant 2 anser också att ofta så har de stora och mest populära molntjänstleverantörerna betydligt bättre koll på säkerheten än vad den egna organisationen har internt. Microsoft kommer exempelvis inte ha några problem att anpassa sig till det nya förhållanden på marknaden.

> *"Molnanvändningen kommer nog inte gå tillbaka. I många fall har nog t.ex. Microsoft bättre koll på informationen än organisationen som äger den."*
>
> - Informant 1 (I1, 51)

> *"De stora leverantörerna kommer inte ha några problem att anpassa sig. Om de inte gör det kommer de inte ha en chans."*
>
> - Informant 2 (I2, 20)

Problemet kommer dock inte lösa sig av sig självt och skugg-IT i molnet måste hanteras innan dataskyddsförordningen träder i kraft. Micallef (2015) stärker hur enkelt och billigt det är för anställda att välja andra alternativ. Anställda lagrar företagsinformation både innanför och utanför företagets brandvägg och trenden fortsätter. Med tanke på molnets användbarhet och hur smidigt det är så kan det bli svårt för organisationer att bemöta problematiken utan att erbjuda ett sanktionerat substitut. Informant 2 påpekar:

> *"Tillräckligt bra molnlösningar inom organisationer förebygger skugg-IT. Det bästa är interna molnlösningar, då vet man var informationen finns."*
>
> - Informant 2 (I2, 20).

Ett exempel på detta skulle kunna vara organisationen som informant 4 arbetar i. De har haft en lång erfarenhet av att behandla personuppgifter och övergången till IT-system i molnet skedde naturligt för dem. Informant 4 uttrycker ingen oro för dataskyddsreformen och ser inte molntjänster som ett allvarligare hot än något annat.

> *"Vi kommer fortsätta som vi har gjort,* vi har exempelvis journalsystem för mindre verksamheter i molnet. *Jag ser inte molntjänster som en större risk än interna IT-system. Det handlar snarare om att se till att det är rätt säkerhet i tjänsterna."*
>
> - Informant 4 (I4, 26)

6 Slutsats

Nedan sammanfattas våra fynd och vad uppsatsen har resulterat i baserat på resultatet från empirin och den tidigare genomförda forskningen på området. Kapitlet ämnar uppfylla syftet samt besvara vår forskningsfråga. I slutsatsen presenterar vi hur organisationer ska förhålla sig till skugg-IT och hur fenomenet kommer påverkas av ökade krav på integritet från omvärlden.

Hur påverkar ökade krav på personlig integritet skugg-IT i organisationer?

Införandet av dataskyddsförordningen kommer att tvinga organisationer att se över var de egentligen lagrar de personuppgifter som de hanterar. Detta kommer göra att problematiken kring skugg-IT, som tidigare ha kunnat existera i skymundan, kommer att belysas i större utsträckning. Fenomenets natur gör det svårt att kontrollera användandet av skugg-IT genom tekniska åtgärder. Har däremot organisationen ett väl fungerande informationssäkerhetsarbete kommer problematiken kopplat till skugg-IT hanteras inom ramen för detta.

Huvudanledningen till att skugg-IT uppstår är enligt vår undersökning för att anställda vill kunna göra sitt jobb effektivare och organisationen antingen ignorerar eller misslyckas med att möta deras önskemål. Organisationer som har ett väl fungerande informationssäkerhetsarbete och arbetar för att tillgodose sina anställdas behov kommer inte påverkas av skugg-IT i någon större utsträckning. För att hantera de ökade kraven på integritet måste medvetenheten kopplat till personuppgiftsbehandling öka. Samtliga måste inse vad skugg-IT innebär för personuppgiftsbehandlingen och hur det kan drabba organisationen och den enskilde individen.

Organisationer som inte har ett etablerat informationssäkerhetsarbete som hanterar skugg-IT kommer att ha ett omfattande arbete framför sig. Samma gäller organisationens mognadsgrad gällande behandling av personuppgifter. Det finns inga snabba lösningar för att hantera skugg-IT när dataskyddsförordningen införs. Arbetet behöver i längden vara proaktivt för att förebygga uppkomsten av skugg-IT. Detta kombinerat med ett omfattande arbete för att utöka medvetenheten kring skugg-IT och personuppgiftsbehandling kommer att vara avgörande för få kontroll på den skugg-IT som existerar. I en organisation som saknar ett gediget informationssäkerhetsarbete kommer det inledningsvis krävas reaktiva åtgärder för att utreda i vilken utsträckning och i vilka former skugg-IT förekommer i organisationer.

Det kan vara av intresse för organisationer att låta anställda använda sina egna enheter i arbetet med på grund av hur kostnadseffektivt det är och dess informella karaktär kan öka effektiviteten. Detta är dock inte aktuellt i organisationer utan ett etablerat och välfungerande informationssäkerhetsarbete med tydliga riktlinjer kring vilken information som får hanteras. I dessa organisationer bör snarare förekomsten av skugg-IT begränsas så mycket som möjligt på grund dess komplexa karaktär och hur svårt det är att kontrollera.

Eftersom skugg-IT kan uppträda på så många sätt: lokal lagring på enheter, molntjänster, skuggsystem och verksamhetsnära utrustning, så bör fokus ligga på behandling av informationen i sig istället för att förbjuda enheter eller blockera vissa tjänster. Detta förutsätter att varje enskild individ har en så hög grad av medvetenhet kopplat till personuppgiftsbehandling att de kan ta relevanta beslut själva.

7 Förslag på vidare forskning

Eftersom denna uppsats bygger på ett regelverk som inte ännu har införts så är det av intresse att genomföra en liknande studie efter att dataskyddsreformen har varit den gällande lagstiftningen i något år så det finns eventuell rättspraxis att undersöka. Detta för att undersöka om dataskyddsreformen hade någon inverkan på skugg-IT och hur stora problem organisationer hade med att genomföra arbetet mot efterlevnad och ifall det fick några konsekvenser.

Vi tycker också att det vore av intresse att genomföra en undersökning där efterlevnaden jämförs mellan organisationer med olika mognadsgrad kopplat till informationssäkerhet. En del av vår slutsats är exempelvis att organisationer med lång vana av personuppgiftsbehandling kommer ha en mer smärtfritt efterlevnadsarbete än organisationer som inte har samma företagskultur gällande informationssäkerheten. Det hade varit intressant att se ifall denna slutsats stämmer och hur de organisationerna med lägre mognadsgrad valde att tackla arbetet mot efterlevnad av regelverket.

8 Referenser

Behrens, S, Sedera W (2004). Why Do Shadow Systems Exist after an ERP Implementation? Lessons from a Case Study" (2004). PACIS 2004 Proceedings. 136.

Behrens, S (2009). SACM - Inspiring Women in Computing, Volume 52 Issue 2, Pages 124-129,ACM, New York, USA.

Bulgurcu, B, Cavusoglu, H & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523-548.

Datainspektionen (2017a). Allmänna frågor om EU:s dataskyddsreform. http://www.datainspektionen.se/fragor-och-svar/eus-dataskyddsreform/allmanna-fragor/#A2 [2017-04-24]

Datainspektionen (2017b). Dina rättigheter enligt personuppgiftslagen. http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/dina-rattigheter/ [2017-04-24]

Datainspektionen (2017c). Förberedelser för personuppgiftsbiträden. http://www.datainspektionen.se/dataskyddsreformen/forberedelser/forberedelser-for-personuppgiftsbitraden/ [2017-04-24]

Datainspektionen (2017d). Om dataskyddsreformen. http://www.datainspektionen.se/dataskyddsreformen/ [2017-02-26]

Datainspektionen (2017e). Introduktion till dataskyddsförordningen. http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/dataskyddsdagen/ [2017-04-26]

Datainspektionen (2017f). Frågor och svar om personuppgiftsansvar och personuppgiftsbiträden. http://www.datainspektionen.se/fragor-och-svar/eus-dataskyddsreform/personuppgiftsansvar-och-personuppgiftsbitraden/# [2017-04-26]

Datainspektionen (2017g). Personuppgiftsansvarig. http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/personuppgiftsansvarig/ [2017-04-26]

Datainspektionen (2011). Tillsyn enligt personuppgiftslagen (1998:204) – Enköpings kommunstyrelsens användning av molntjänsten Dropbox. http://www.datainspektionen.se/Documents/beslut/2011-09-30-enkopings-kommun.pdf [2017-04-03]

Donnelly, Caroline. 'Gartner predicts 25% of enterprises will use enterprise app stores by 2017'. IT Pro,12 Feb 2013.
http://www.itpro.co.uk/645640/gartner-25-of-enterprises-will-use-corporate-app-stores-by-2017
[2017-05-04]

EU-upplysningen (2016). Olika typer av EU-lagar.
http://www.eu-upplysningen.se/Om-EU/Om-EUs-lagar-och-beslutsfattande/Olika-typer-av-EU-lagar/
[2017-04-26]

Europaparlamentets och rådets direktiv 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119/1,4.5.2016).
http://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679&rid=1
[2017-04-03]

Frost & Sulivan (2013). The Hidden Truth Behind Shadow IT.
https://www.mcafee.com/cn/resources/reports/rp-six-trends-security.pdf
[2017-04-24]

Ghosh, A et al. (2013). Journal of Global Research in Computer Science, 4 (4), April 2013, pp. 62-70.

Gordon, L & Loeb, M (2002). The economics of information security investment. *ACM Trans. Inf. Syst. Secur.* 5, 4 (November 2002), 438-457.

Informationssakerhet.se (2015). Om informationssäkerhet
https://www.informationssakerhet.se/Om-informationssakerhet-kon/vad_ar_informationssakerhet/
[2017-04-25]

Högsta Domstolen (2013). *Skadestånd enligt personuppgiftslagen.* Dom mål nr: T 2807-12 meddelad i Stockholm den 6 december 2013.
http://www.hogstadomstolen.se/Domstolar/hogstadomstolen/Avgoranden/2013/2013-12-06%20T%202807-12%20dom.pdf
[2017-05-10]

Jacobsen, D, Sadin, G, & Hellström, C. *Vad, Hur Och Varför?: Om Metodval I Företagsekonomi Och Andra Samhällsvetenskapaliga Ämnen*.
Lund: Studentlitteratur, 2002.

Leeuwen, D (2014). Bring your own software. Network Security Volume 2014, Issue 3, March 2014, pp. 13-14.

Marston, S, et al. (2011) Cloud computing — The business perspective, Decision Support Systems, Volume 51, Issue 1, April 2011, Pages 176-189, ISSN 0167-9236

Mell, P & Grance, T (2011). The NIST Definition of Cloud Computing. Nist Special Publication 800-145, National Institute of Standards and Technology, Gaithersburg, MD.

Micallef, M (2015). NetworkWorld Asia. Nov/Dec2015, Vol. 12 Issue 2, p48-48. 1p.

Miller, K et al. (2012). BYOD: Security and Privacy Considerations. IT Professional Volume: 14, Issue: 5, Sept.-Oct. 2012, pp. 53-55.

Netskope (2016). Netskope Report Reveals 75 Percent of Cloud Apps Not Ready for EU General Data Protection Regulation.
https://www.netskope.com/press-releases/netskope-report-reveals-75-percent-cloud-apps-not-ready-eu-general-data-protection-regulation/
[2017-04-24]

Netskope (2017). January 2017 - Worldwide Cloud Report.
https://resources.netskope.com/h/i/319349682-january-2017-worldwide-cloud-report/
[2017-04-24]

Rienecker, L., Jörgensen Peter Stray & Hedelund, L (2014). Att skriva en bra uppsats. Lund: Liber.

SFS 1998:204 Personuppgiftslag. Stockholm: Justitiedepartementet L6.

Silic, M and Back, A (2014). Shadow IT – A view from behind the curtain, Computers & Security, 45, pp. 274-283, ScienceDirect, EBSCOhost.

Silic, M, Barlow, J, and Back, A (2017). A new perspective on neutralization and deterrence: Predicting shadow IT usage. Information & Management, 2017.

Strong, D.M. and Volkoff, O (2004). A roadmap for enterprise system implementation. Computer 37, 6, pp. 22-29.

Walters, R (2013). Bringing IT out of the shadows, Network Security, 2013, pp. 5-11, ScienceDirect, EBSCOhost.

Williams, J (2011). Experts warn of growth of 'shadow IT' use outside IT department control.
http://www.computerweekly.com/news/2240104901/Experts-warn-of-growth-of-shadow-IT-use-outside-IT-department-control
[2017-04-25]

Yeadon, J (2016) Smartfile - Businesses: You Can’t Keep Ignoring Shadow-IT
https://www.smartfile.com/blog/shadow-it-risks/
[2017-04-27]

9 Bilagor

9.1 Beskrivning av problemområde skickat till informanterna

Icke sanktionerad IT i en omvärld med ökande krav på säkerhet.

Fenomenet Skugg-IT (eller icke sanktionerad IT) har funnits i så länge IT har används i organisationer. Skugg-IT innefattar samtliga IT-artefakter som används i en organisation där användandet inte är kontrollerat och godkänt av en IT-avdelning eller liknande (Silic & Back 2014). Samma fenomen kan även definieras som att det är användning av obehöriga applikationer i företagsmiljö och bearbetning samt lagring av företagsinformation på icke-godkända enheter (Walters 2013). Den senaste tiden har skugg-IT fått allt mer fotfäste i organisationer och företeelsen får allt mer betydelse då ny teknik har introducerats (Silic & Back 2014), både på grund av det ökade användandet av diverse molntjänster och att personliga enheter börjat användas i professionella sammanhang (Frost & Sullivan 2013).

Enligt en undersökning gjord av Frost & Sullivan (2013) så erkände 80% av deras tillfrågade objekt att de använder icke sanktionerade molnapplikationer i sitt dagliga arbete. Kombinationen av att användandet av molntjänster ökat och det nya datalagringsdirektivet som introduceras i maj år 2018 så problematiseras användningen av icke-sanktionerad IT ytterligare. Hårdare krav ställs på både molnleverantörer och den enskilda organisationen när de hanterar personuppgifter. I värsta fall kommer organisationen som ansvarar för ett eventuellt intrång där data förloras bli skyldiga att betala ett vite på upp till fyra procent av organisationens globala omsättning (Allmän dataskyddsförordning 2016/679 av den 27 april 2016). Frågan är dock vilka ansvarsförhållanden som råder och hur införandet av den nya förordningen kommer att påverka skugg-IT

I den nuvarande gällande lagstiftningen (personuppgiftslagen) så är företag, vid ett dataintrång, enbart skyldiga att betala ut eventuellt skadestånd till de utsatta personerna som blivit kränkta som resultat av dataintrånget (Datainspektionen 1). Det nya datalagringsdirektivet tvingar företagen att ta mer hänsyn till behandlingen av personuppgifter då dataintrång nu direkt påverkar organisationen.

Ytterligare en problematisering som medföljer införandet av det nya datalagringsdirektivet är ansvarsförhållandena. I dagsläget är, enligt Datainspektionen, de organisationer som behandlar personuppgifter i tjänsten personuppgiftsansvariga och de företag som tillhandahåller molntjänster som används för lagringen av dessa uppgifter är personuppgiftsbiträden (Datainspektionen 2 2011). Skulle ett dataintrång ske så är det i dagsläget enbart den personuppgiftsansvarige som gör sig skyldig till brott mot personuppgiftslagen, inte personuppgiftsbiträdet. Det är dessutom den enskilda individen som behöver bevisa att den personuppgiftsansvarige faktiskt har brutit mot lagen för att få någon ersättning. (Datainspektionen 3).

Den nya dataskyddsförordningen kommer inte påverka dessa definitioner men däremot förändras rollernas ansvarsförhållande. Personuppgiftsbiträdet kommer få nya skyldigheter och dess eget ansvar i relation till personuppgifterna kommer öka kraftigt. I flertalet situationer kommer personuppgiftsbiträdet omfattas av samma skyldigheter som personuppgiftsansvarige (Datainspektionen 4). Detta leder till att problemområdet utökas till

att även involvera ansvarsförhållandet då organisationer omöjligt kan veta hur de ska förhålla sig till detta när inga prejudikat existerar ännu då lagen inte ännu trätt i kraft.

Syftet med vår uppsats är att undersöka hur dessa nya omständigheter kommer att påverka fenomenet skugg-IT i organisationer. Nedan följer ett par intervjufrågor vi har tänkt använda som underlag för intervjun.

9.2 Intervjuguide

Inledning

- Vad har du för tidigare erfarenhet av Skugg-IT?
- Hur länge har du arbetat med ditt nuvarande arbete?

Vad är det?

- Känner du till fenomenet skugg-IT?
    - Har du haft någon erfarenhet av skugg-IT? Både hos kunder samt i egna organisationen.

Varför existerar skugg-IT?

- Varför tror de skugg-IT har blivit så vanligt förekommande fenomen i organisationer?

Vilka åtgärder bör vidtas?

- Hur skulle du hantera problemen kopplade till skugg-IT?
    - Hanteras på ett tekniskt eller organisatoriskt sätt?
        - För/nackdelar
    - Hur kommer användandet av BYOD, BYOS och BYOA se ut i organisationer i framtiden?
    - Kommer det behövas några styrmedel för att kontrollera dessa?
        - Vilka?

Vilka fördelar medföljer?

- Kan organisationer på något sätt utnyttja skugg-IT?
    - Finns det något fall där de positiva aspekterna överväger de negativa?

Vilka nackdelar medföljer?

- Några förekommande nackdelar med skugg-IT är:
    - Korrumperad data
    - Legalt påförda sanktionsavgifter till följd av GDPR
    - Underminerar sanktionerade system
    - Ökar belastningen på IT-avdelningen
    - Ökad risk för förlorad data.
    - Inkonsekvent affärslogik
- Anser du att någon av dessa har större chans att inträffa än de andra?
- Anser du att någon av dessa är värre än de andra?

Externa faktorer (GDPR, Cloud computing, BYOE)

- Hur stor del av en organisations totala problematik kopplat till skugg-IT utgörs av icke-sanktionerade molntjänster?

    - Har detta förändrats i med det kommande införandet av GDPR?
- Hur kommer införandet av GDPR påverka användandet av skugg-IT?
    - Hur stor är arbetsbelastningen för att hantera användandet av skugg-IT?
    - Kommer detta att påverka organisationens struktur eller policys på något sätt?
- Kommer de ökade kraven på molnleverantörer påverka dem?
- Kommer de ökade kraven påverka användandet av molntjänster i organisation?
- Hur skall man som personuppgiftsansvarig gå tillväga för att validera en molnleverantör?
    - Finns det några extra kritiska punkter?
- Hur förändras rollen som databiträde?
    - Kan en molnleverantör ofrivilligt bli databiträde?
- Har du något övrigt att tillägga gällande detta ämne?

9.3 Intervjuer

9.3.1 Intervju 1 – Informant 1 – Organisation 1

Intervjuare - Erik Bråtendal (EB)
Sekreterare - Per Jansson
Informant 1 - IT management konsult, specialisering informationssäkerhet i offentliga sektorn.

START

1 EB: I vilken utsträckning har du personligen kommit i kontakt med fenomenet Skugg-IT?

2 Informant 1: Faktiskt inte så vansinnigt mycket i min professionella karriär så att säga. Vi har ju belyst GDPR utifrån tänkbara områden som kommuner behöver förhålla sig till. Egentligen så handlar det om alla typer av organisationer, det skiljer sig inte så mycket mellan kommuner och företag vad vi vet då. Alla kommer behöva förhålla sig till den lagstiftningen. Men alltså Skugg-IT har jag inte sett ur den synvinkeln. Man kan säga såhär, man kan ju börja med att hålla koll på alla personuppgifter i dem IT-system man har liksom, eller i alla informationstillgångar man har, det behöver inte bara vara IT-system. Jag tror inte att det är många som har tänkt på att det kan finnas egensnickrade lagringsplatser. Det är ju en jättegrej naturligtvis. Utifrån mitt perspektiv så har inte det här behandlats alls. Jag har ändå gjort en del informationsklassningar av olika system där man tittar på vilken typ av information som lagras och vilka tänkbara risker som finns. Jag har inte stött på fall än så länge i alla fall där jag stött på det begreppet. Så ja, i ganska liten utsträckning har jag stött på det begreppet.

3 EB: Tror du det här skulle kunna få några konsekvenser nu när lagstiftningen så smått börjar användas i organisationer?

4 Informant 1: Absolut, alltså säg såhär. Det är ju få som jag har talat med som tror att det kommer börja delas ut böter hej vilt. Men däremot så kommer det bli ett mycket tuffare klimat i Sverige tror jag, i och med den här lagstiftningen. Det ser man inte minst på efterfrågan av konsulttjänster när det gäller detta. Så ja klimatet när det gäller hantering av personuppgifter kommer bli mycket tuffare. Det är ju det man vill åt med den här lagstiftningen, man vill stärka individens rättigheter kan man säga. I och med att det här uppmärksammas mer och mer och man får höra om det ifrån alla håll och kanter så tror jag att man börjar tänka i verksamheten “Okej var lagrar vi våra kunduppgifter, vi måste tydligen ha koll på det”. Eftersom man får in det här perspektivet så tror jag också att man börjar titta på alla olika möjliga sätt som kunduppgifter lagras på. Sen finns det ju många som använder sig av molnlagring fast på ett professionellt sätt. I och med så kommer man ju behöva se över “Okej finns det några risker med det här?” Till exempel att privatpersoner själva sätter upp cloudlösningar. Så jag tror att skugg-IT kommer hamna mer under luppen ifall du förstår vad

jag menar, det kommer hamna mer i rampljuset. Det kommer komma upp till ytan den här sortens problematik, absolut.

5 EB: Varför tror du att anställda tar egna initiativ till att gå runt organisationers vanliga system?

6 Informant 1: Jag tror det är för man vill skapa sin egen lilla lagringsplats med information. Jag tror det har att göra med att man vill behålla sin kompetens inne i sin lilla sfär som man absolut kan tänka sig att delge sig men man vill förvissa sig om att den inte försvinner. Sen ibland tror jag det kan saknas tydliga strukturer och forum för medarbetare att lagra information helt enkelt.

7 EB: Det är ett intressant perspektiv du tar upp där för information är ju makt på många sätt och vis och det kanske man inte vill dela med sig av i det första taget.

8 Informant 1: Exakt, information kan ju vara, eller är ju väldigt värdefullt och kan ses som en tillgång du besitter som anställd. Då kanske du har samlat på dig unik kompetens och därmed inte sagt att man inte vill dela med sig av den men däremot att du ska ha förmågan att komma ihåg den eller kunna ha kvar den i sin lilla sfär, eller på sitt konto så att säga, då kan man ju ta till sådana metoder som ligger nära till hands, som ett personligt molnlagringskonto exempelvis, det är ju trendigt att ha en dropbox liksom. Det sätter såklart prägel på den anställde. Sen tror jag det påverkar hur företag väljer att bemöta detta. Man kan ju ha en policy som säger att information ska lagras här och där men jag tror ändå att man personligen ruckar lite på de policies och ser dem mer som riktlinjer.

9 EB: Nej men det tror vi stämmer. Vi har sett i litteraturen att det finns inte tydliga policies på hur det här skall hanteras ordentligt liksom.

10 Informant 1: Nej men precis det tror jag stämmer, vad är titeln på er uppsats ifall ni har bestämt er för en sådan än? Eller vad går den under för arbetstitel liksom?

11 EB: Icke-sanktionerad IT i en omvärld med ökade krav på informationssäkerhet heter den. Så vi har ju valt att aktivt ta lite avstånd ifrån GDPR och mer hantera det som någonting som påverkar den här miljön som fenomenet skugg-IT verkar inom.

12 Informant 1: Det tror jag är helt rätt och det låter som ett väldigt intressant perspektiv. Där tycker jag att ni ligger rätt på det.

13 EB: Som du sa förut att när den här miljön kring personuppgiftslagring hårdnar så kommer organisationer behöva belysa det här fenomenet skugg-IT i sina egna organisationer. Vad bör man vidta för några åtgärder?

14 Informant 1: Man behöver ha ett fungerande informationssäkerhetsarbete och det behöver ju då definieras först och främst. Man behöver ju ha, eller det här är ju rekommendationer eller egentligen riktlinjer men det var ganska nyligen som Anders Ygeman gick ut och sa att "Informationssäkerhetsarbetet måste fungera i våra offentliga organ i Sverige". Det börjar väl där skulle jag säga. Informationssäkerhet är ju mer än bara hantering av personuppgifter givetvis. Men det är en så pass central del att man måste börja med att få igång ett fungerande informationssäkerhetsarbete för det är långt ifrån vad alla har skulle jag säga. Det kan man då göra genom att titta på vilka system man har men man måste komma ihåg att det också har att göra med tjänster. För det är inte bara ett affärssystem liksom utan, amen ni vet det är ju det vi talar om det är molntjänster och det är sharepoint och så vidare. Alla typer av filytor måste man ha koll på. Om man får till ett informationssäkerhetarbete där man klassificerar informationen som finns i varje tillgång och att man på något sätt tar upp de risker som man kan tänkas förekomma. Då måste man blanda in hela verksamheten och alla typer av enheter i ett företag. Om man säger så här man kan inte göra det med en workshop liksom, det finns så mycket information som florerar inom en organisation. Det var ett långt svar insåg jag nu men det korta svaret är att ja, man får till ett fungerande informationssäkerhetsarbete helt enkelt.

15 EB: Så man måste lägga en grund i organisationen liksom och då pratar vi inte om tekniska biten utan hela organisationen.

16 Informant 1: Det är mycket mer än att bara bygga upp brandväggar och virusskydd, det vill jag säga. Det handlar om att skapa en kultur av att man tar det på allvar och att det är förankrat i ledningen. Man kan ju sitta här och säga till exempel "Ja de måste få till ett informationssäkerhetsarbete" men det är kritiskt att arbetet förankras i ledningen. Så det är också en nyckelfaktor skulle jag säga. Oavsett vilken information det gäller så måste ledningen förstå att informationssäkerhet är viktigt.

17 EB: Vi diskuterar även i vår uppsats begrepp så som "Bring Your Own Device", "Bring Your Own Service" och "Bring Your Own Application". Det här är någonting som vi också tror kommer påverkas av GDPR. Man tar in massvis med okända enheter i företagets miljö. Just nu har vi märkt att det är väldigt populärt i organisationer. Tror du detta är något som kommer behöva regleras på samma sätt? Kommer man behöva sätta ner foten och säga såhär "Nej, ni får bara lov att använda enheterna som företaget förser er med" eller kommer den här trenden fortsätta?

18 Informant 1: Jag tror det kommer behöva regleras och detta är något man måste få med i informationssäkerhets-biten. Att sådana risker kommer komma upp till ytan när man väljer att ta ett helhetsgrepp kring informationssäkerhetsarbetet.

19 EB: Vart man lagrar sin information och så vidare.

20 Informant 1: Ja precis. Jag tror kanske inte man kontrollerar vilka devices folk har med sig men om riskerna kommer upp till ytan på ett samlat sätt så kan man förhålla sig till det och

om det finns en funktion i informationssäkerheten som är väl utarbetat så kommer den snappa upp sådana här saker. Det är så vi angriper den typen av problematik. När jag varit ute hos kund och tittat på det här så kommer det upp sådana här saker till slut. Det där kan vara lite olika beroende på om det är en offentlig sektor, myndighet eller privat företag. Det kan hända att det är mycket vanligare i ett företag med Bring Your Own Device än vad det är på andra ställen. Så där tror jag det kommer komma upp olika fort beroende på mognadsgraden i organisationen.

21 EB: Du nämnde tidigare att du inte tror att datainspektionen kommer börja dela ut böter till höger och vänster när GDPR är infört, det tror inte vi heller. Hur tror du hotet om sanktionsavgifterna kommer påverka organisationer, kommer det vara dem som är någon form av wake up call som får dem att inse "Oj, nu måste vi göra någonting åt det här" och inte att det är risken för att förlora data till konkurrenter exempelvis.

21 Informant 1: Jag tror det är lätt att en organisation går in i det här arbetet och ser "okej hur kan det här gynna oss". Den sortens tänk är ju helt fel, det är individens perspektiv man måste ha på det här då lagen är till för vi vanliga medborgare. Vad var frågan nu igen?

22 EB: Nej men så du tror inte att företag kommer kolla på den här eventuella sanktionsavgiften och säga "nu måste vi göra något för att undvika det här".

23 Informant 1: Jo det tror jag väl ändå. Det är det alla kommer komma ihåg och det är det jag tror som kommer få ledningar att agera och såhär. Själva sanktionsavgiften är ändå det som trycker på. Alltså händer inte någonting konkret så jag vet inte hur många det är som arbetar aktivt med sitt personuppgiftsarbete, hur många följer PUL idag liksom?

24 EB: Ja inte jättemånga.

25 Informant 1: Nej, hur ofta görs det stickprovskontroller idag liksom. Om du skulle följa PUL till punkt och pricka idag så skulle man inte ha särskilt lång väg till när GDPR införs. Det är väldigt mycket som är samma sak. Men det är inte många som kan visa på att de faktiskt följer PUL idag. Företag kommer förhålla sig till sanktionsavgifterna absolut. Det är ju 20 miljoner euro liksom. Sen kanske man inte förstår helt vad det innebär då det inte är ordentligt utrett. Jag menar 20 miljoner euro är ju helt olika i Sverige jämfört med Rumänien liksom. Men det står klart i alla fall att det blir väldigt kännbart om man inte tar detta på allvar. Det är väl det man vill få till och man vill få till ett tryggare samhälle för individen. Så jag tror sanktionsavgifterna är väldigt centrala för att man ska ta det här på allvar.

26 EB: Det är väl så vi har valt att förhålla oss till just de här sanktionsavgifterna också att det spelar ingen roll exakt hur stor just summan är egentligen utan det är snarare görs ingenting så kommer något väldigt dåligt att hända.

27 Informant 1: Ja egentligen. Man kanske sätter upp sådana här bötesbelopp bara för att statuera exempel på vad som kan hända då får alla något att förhålla sig till. Ännu värre kan man ju få fyra procent av organisationens omsättning. Så de har ju en funktion helt klart. Men det är inte så svart på vitt att det kommer börja delas ut böter svart på vitt den 25:e maj 2018 liksom. Sen kan man kanske tänka sig att det krävs att någon åker på smällen för att det ska gå att förhålla sig till.

28 EB: För att sätta någon praxis liksom

29 Informant 1: Ja exakt, någon kanske åker på en rejäl böter. Men man ska ju komma ihåg att om man inte jobbat mycket med PUL eller på något sätt tagit något grepp om alla de saker GDPR innebär redan i ett tidigare skede så har man en väldigt lång resa att gå, det händer ju inte över en natt liksom. Att börja inventera alla lagringssystem och se över alla kommunikationskanaler, det tar väldigt lång tid och man skulle börjat med detta för länge sen.

30 EB: Syftet med vår uppsats är egentligen att vi har identifierat skugg-IT som det var innan GDPR och nu vill vi veta hur det kommer hanteras efter GDPR. Du tror att det här problemet kommer belysas och komma upp till ytan och tas med i informationssäkerhetsarbetet. Man börjar utvärdera var man faktiskt har data i organisationen, har jag förstått dig rätt då?

31 Informant 1: Ja precis helt klart. Det kommer få mycket mer uppmärksamhet. Om man har en skala på uppmärksamhet så har det innan haft noll och nu kommer det ha uppmärksamhet.

32 EB: Nej det har ju tidigare inte kunnat uppstå några riktiga konsekvenser. Möjligtvis att man förlorar data eller liknanade på grund av en säkerhetsbrist eller att man tappar bort datan helt enkelt. Hur omfattande tror du arbetet med skugg-IT är kopplat till övriga problem i organisationen kommer bli?

33 Informant 1: Vad skulle ett annat problem vara då exempelvis bara så man kan sätta det i relation till något?

34 EB: Tänk exempelvis serversäkerhet och brandväggar och så vidare som vi pratade om tidigare.

35 Informant 1: Aa just det. Nej jag tror man kommer behöva lägga ner mycket mer tid på det här. Man har kommit så pass långt idag med teknologin, servrar, nätverk och kopplingar mellan system och sånt. Jag tror redan att företag har ganska bra koll på det där då den sortens problematik kom mycket tidigare än exempelvis hanteringen av personuppgifter eller för all del molntjänster kan man säga. Så jag tror att organisationer kommer behöva lägga mycket mer tid på den typen av problematik.

36 EB: Dessutom kanske man kan tänka sig eftersom företag använder mycket sanktionerade molntjänster där det finns policys och färdiggjorda avtal med leverantörer osv. Skulle man då istället använda en icke sanktionerad tjänst så går man förbi hela organisationens i förväg gjorda säkerhetsstruktur.

37 Informant 1: Det har du helt rätt i. Det är jätteintressant för det har att göra med personuppgiftsbiträdesavtal. Även kallat PUB-avtal. Helt rätt. Jag tror att organisationer kommer bli varse om att de måste jobba med sina personuppgiftsbiträdesavtal. Det är jag helt säker på. Det är många som använder sig av de stora leverantörerna exempelvis google och microsoft. De kan ju säkert vara behjälpliga också liksom men i takt med ett företag eller en kommun jobbar med sina PUB-avtal så kommer det finnas en högre medvetenhet i organisationen och om det då upptäcks att det finns andra icke sanktionerade vägar för att hantera informationen då kommer det blåsas i visselpipan.

38 EB: Nu kommer vi in lite mer på ansvarsförhållanden mellan databiträde och dataansvarig. Skulle det kunna bli så att en molntjänstleverantör ofrivilligt blir databiträde? Och hur regleras det? Om jag exempelvis jobbar på ett valfritt företag och väljer att lagra en kundlista med mina kunder i min dropbox. Hur ser ansvarsförhållandena ut då mellan databiträde och dataansvarig och jag som anställd?

39 Informant 1: Det är alltid den personuppgiftsansvarige som är ansvarig för hanteringen av personuppgifterna.

40 EB: Även om den anställda på eget initiativ lagrar informationen på ett ställe som det inte är tänkt?

41 Informant 1: Ja för det finns ett kontrakt där den anställda är anställd på ett företag. Företaget är i detta fallet personuppgiftsansvarig, så det är ju de som kommer åka dit. Jag skulle ha svårt att se att dropbox i detta fallet är inblandade i ansvarsförhållandet om det inte finns ett PUB-avtal, alltså om det inte finns något som reglerar avtalet där det står uttryckligen att leverantören, typ dropbox, de hanterar för vår räkning, det här, det här och det här gäller. Om det saknas ett sådant då är det alltid personuppgiftsansvariges som slutligen bär ansvaret. Jag kan inte svära på det då det är lite av en djungel det där. Men de är rätt noga med att det måste regleras i personuppgiftsbiträdesavtalen. Det måste stå klart och tydligt vem som ansvarar för vad. Även om det är biträdet som står för molnleveransen så ska det framgå vilket ansvar de har i situationen.

42 EB: Den anställda är helt enkelt alltid en representant för den personuppgiftsansvarige i detta fallet då?

43 Informant 1: Ja det är är min tolkning i alla fall.

44 EB: Hur kommer de ökade kraven påverka förhållandet mellan molnleverantörer som databiträde då och personuppgiftsansvarige, tidigare har personuppgiftsansvarige ensamt varit ansvarige enligt personuppgiftslagen då. Vi har pratat lite med datainspektionen och det dem har sagt är att personuppgiftsbiträdenas ansvar kommer öka.

45 Informant 1: Ja de kommer också vara ämne för sanktioner faktiskt. De har också lite mer, vad ska man säga….

46 EB: Ett mer solidariskt ansvar verkar vara målsättningen för lagstiftningen.

47 Informant 1: Ja men exakt. Det blir mer gemensamt fördelat. Skulle det vara dropbox i privat syfte så har vi helt andra förutsättningar än om du lagrar på one drive för företag liksom. Jag tror det kommer bli en bättre dialog mellan biträde och ansvarige.

48 EB: Ja tidigare har det varit två läger liksom, men nu känns det som alla har ett gemensamt intresse.

49 Informant 1: Ja exakt. Jag tror förhållandet kommer bli bättre och mer öppet mellan ansvarige och biträde. Även om man måste krita ner exakt vad som gäller i avtalen. Det brukar inte vara svårt att komma fram till dessa avtalen bara man är tydlig. Nu är jag ingen expert men det är väl samma som med alla avtal liksom.

50 EB: Tror du detta kommer bidra till att användningen av molntjänsterna ökar inom organisationer eller kommer de blir negativt inställda och tänka att det är världens djungel och vi ska kanske gå tillbaka till att lagra vår egen data.

51 Informant 1: Ja det är ju en jätteintressant diskussion. I vissa fall kan det vara att man tror att det är säkrare att lagra allting i sin egen burk, alltså fysiskt inom organisationen men det finns ingenting som säger att det är så. I många fall har nog exempelvis microsoft bättre koll på säkerheten i sina serverhallar än vad du har på hemmaplan så att säga. Så jag tror väl inte att molnanvändningen kommer gå tillbaka. Det är klart att det kommer upp nya frågeställningar och nya risker med molnet.

52 EB: Med andra ord ju mer etablerad den här metodiken blir så kommer användandet förbli stabilt så att säga.

53 Informant 1: Ja precis.

54 EB: Nu har jag faktiskt inga mer frågor, såvida du inte har något övrigt du vill tillägga kring ämnet?

55 Informant 1: Nej jag har nog inget mer vad jag kan komma på.

56 EB: Dåså, då får vi tacka för din medverkan.

9.3.2 Intervju 2 – Informant 2 – Organisation 2

Intervjuare - Erik Bråtendal (EB)
Sekreterare - Per Jansson
Informant 2 - Senior konsult, internet certifierad att arbeta med kunders arbete mot GDPR-compliance. Lång tids erfarenhet av skugg-IT inom banksektorn.

START

1 EB: Vi kan ju börja med att du berättar lite om vad du jobbar med? Vad har du för befattning på ditt företag?

2 Informant 2: Ja jag jobbar ju på *Organisation 2* då. Jag jobbar på den avdelningen inom *Organisation 2* som heter consulting och har då titeln senior management consultant. Det innebär då att jag är ute på uppdrag, tyvärr kan jag inte berätta var jag är då det är hemligt. Men det vi gör bland annat är att vi hjälper organisationer med deras IT-styrning och just i det här fallet just nu är jag inne och stöttar en CIO på ett företag kring diverse frågor. Det som kanske är mer intressant för er eller varför jag tyckte det här lät så intressant är att jag har en ganska lång bakgrund inom finansvärlden och jag har jobbat inom IT i banksektorn, specifikt på *Organisation X*. Där jobbade jag väldigt länge och hade ett antal olika chefspositioner och jobbade i det berömda gränslandet mellan IT och affär. Haft både leveransansvar som avdelningschef och även varit systemansvarig för cirka 50 system finansiellt och strategi-mässigt. Mycket handlar då i stora företag om centralisering och gemensam arkitektur. Så när ni kontaktade och berättade att ni skrev om utmaningarna relaterat till shadow-IT så lät det jätteintressant. Där har jag mycket erfarenhet kring just det. Jag har även arbetat väldigt mycket med regelverk under många många år, framförallt finansiella regelverk. Detta är då regler man ska följa för att vara compliant och de kan vara satta på EU-nivå eller kanske sätts av amerikanska myndigheter om man har kunder i USA. De är väldigt likt det som kommer nu med GDPR då. I GDPR är jag också riktigt insatt i och är certifierad inom *Organisation 2* att jobba med GDPR-frågor som våra kunder har. Jag känner till det regelverket väldigt bra och framförallt börjar jag få ganska stor förståelse för vad det innebär för företag och organisationer. Så det är väl bakgrunden kan man säga.

3 EB: Ja men det låter ju som vi verkligen hittat rätt.

4 Informant 2: Ja och jag måste säga att jag tycker det är väldigt kul eftersom jag varit med ett tag att stöta på studenter som har identifierat det här som ett spännande område. Det är ju lite såhär, GDPR kan ju vara lite väl detaljerat och byråkratiskt vissa lägen. Man ska kunna paragrafer och så vidare. Men just den här kombinationen som ni har identifierat den är ju superintressant, hur har ni kommit fram till just det här? Berätta lite mer.

5 EB: Det började väl egentligen för ungefär ett halvår sedan där vi var på en gästföreläsning om just GDPR. Då insåg vi väl med en gång att det här kan gå lite hur som helst och vi har

ingen aning om hur detta kommer att påverka organisationerna i Sverige. Vi insåg snabbt att organisationer inte är beredda på en så pass omfattande lagstiftning. Sen var det väl av en slump som vi snubblade över fenomenet skugg-IT som också var någon form av väckarklocka. Vi kunde relatera till det själva direkt och tänka "oj, det här är ju något som jag har gjort i mitt arbete" utan att reflektera över det över huvud taget. Sen började vi gräva i det här och såg en form av koppling mellan de här två fenomenen. Nu har vi då suttit och plöjt igenom den forskning som går att hitta på ämnet och forskningen är ju inte up-to-date kopplat till GDPR. Så det är väl där som vi försöker göra ett kunskapsbidrag.

6 Informant 2: Nej men det är inte så konstigt eftersom det inte finns något företag som gjort en fullständig GDPR-implementation än så länge, vad jag vet. Alla håller på och är i olika faser. Så det är klart att det inte finns så mycket forskning.

7 EB: Nej precis, då skulle vi kunna dra igång själva intervjun här om det är okej?

8 Informant 2: Ja absolut.

9 EB: Första frågan är väl egentligen hur har du kommit i kontakt med fenomenet skugg-IT i de organisationer du har arbetat i?

10 Informant 2: Mm. Till att börja med så tänker jag att det finns två nivåer på det där. Det ena är skugg-IT, det vill säga när delar av organisationen inte längre förlitar sig på den centrala IT-organisationen utan börjar göra saker på egen hand. Man kanske ställer en server under bordet, man kanske beställer lite molntjänster och vips som har man 12 stycken burkar som ligger på amazon som kör i molnet som man inte har koll på. Resultatet blir en parallell IT-miljö. Det är ett bekymmer i sig. Det kan samtidigt vara en jäkligt stor enabler för att göra saker mycket snabbare. Jag är inte enbart negativt inställd till skugg-IT. Kontrollerad skugg-IT ger en dynamisk utvecklingstakt. Det är verkligen både och. Men om du tittar på GDPR-perspektivet så har vi till exempel skugg-personregister. Det vill säga att någon på HR jobbar i HR-systemet där man har full koll på personuppgifter eller kunduppgifter eller vad det kan vara. Men sen för eget bruk så laddar man ner en kopia av databasen i ett excel-ark på sin burk eller att man har excel-ark med ODBC eller SQL-anrop i sig och så vips så har du replikerat ut personuppgifter hos personer som inte nödvändigtvis är IT-kunniga. Och det är GDPR-perspektivet, där har ni en jätteutmaning. Hur fasiken fångar man in det om man har ett bolag med 10,000 anställda, hur fångar man in förekomsten av personuppgiftshantering som inte sker centralt? Då pratar jag inte om den organiserade pirat-IT som kan finnas inom organisationer utan enskilda personer.

11 EB: Ja vi tror ju att det här är mycket mer vanligt förekommande än vad folk tror.

12 Informant 2: Ja och jag ska säga så här. Jag tror inte det finns förmågor hos datainspektionen att börja syna alla företag i Sverige. Det finns ju inte en chans. Utan det som kommer vara problem eller det som triggar igång böter eller skriverier, det är om man har

konkreta leakage där uppgifter kommer ut av någon anledning. Man får vara lite sansad i ett företag om hur mycket man ska lägga tid på att reda upp allting. Men att vara medveten om de här förekomsterna i en organisation, om man har en data-protection officer eller någon informationssäkerhetsansvarig, det är en bra start. Sen vet jag inte konkret hur man ska lösa dessa problemen. Ni kanske har läst GDPR, det är ingen höjdarläsning direkt. Men om man läser igenom den och förstår den så inser man att det här ställer jättehöga krav på leverantörer och organisationer. Det jag har stött på tidigare i yrkeslivet är dels att man har lite för dåligt förtroende för den centrala ITn. Man är trött på beställningstiden, det kan ta tre månader att få upp en server. Då börjar man sätta upp grejer på egen hand, det går snabbt, det är fiffigt. Speciellt i finansvärlden där om du tar en kvantitativ analytiker, de är ju lika mycket finans och matte-mästare som de är utvecklare. Jag tycker man ska hitta ett sätt att promota det för det skapar en tillväxt och en affärsutveckling som är viktig. Det som har drabbat mig då när jag varit ansvarig för ett antal system, i bästa fall så kommer intern audit och säger till mig "nu vill vi syna dina system så du uppfyller de interna regelverken", det är det bästa fallet. Det sämsta fallet är om kundens revisorer kommer och utför en audit. Då får du ett helsike om du inte har stenkoll på grejerna. Orsakerna till att det inte är så omskrivet är att man hittar ju inte det här. Så när en extern audit kommer in så hittar de inte de här förekomsterna utan det måste till ett riktigt forensic-arbete för att hitta shadow-IT.

13 EB: Ja tack vare fenomenets natur så är det väldigt svårt att både studera och reglera. Hur tror du man skulle kunna hantera det här fenomenet, du sade att du anser att man bör promota det till viss del, hur tacklar man det här?

14 Informant 2: Ja man sätter upp ramarna för vad man får lov att behandla inom shadow-IT. Till exempel om du snabbt vill få igång en ny produkt till kunden eller ett erbjudande eller någon fiffig funktion på onlinetjänsten man har eller vad det kan vara. Då kanske det är bra om man låter en liten grupp utvecklare jobba jättenära med affärsutvecklarna och ta en kopia på systemet så kan de sitta och fiffla där på egen hand. Man skapar en sorts "sandbox" och säger att ni får lov att jobba med det här och det här och ni får absolut inte använda er av live-data eller kund-data utan det måste vara tvättad information som inte innehåller riktiga person- eller kunduppgifter. Men ta den delen sen och koda på. På det sättet kan man då auktorisera vissa typer av shadow-IT internt. Med support från security och compliance till och med. Jag vill inte promota begreppet shadow-IT men jag tror att det kan vara ett medel för att komma snabbt fram i affärsutvecklingen. Det andra man kan göra är att börja titta på sina access- och behörighetsregelverken. Är det verkligen rimligt att man ska kunna etablera shadow-IT genom att koppla upp sig med ett API till CRM-systemet utan att någon märker någonting. Nej det ska givetvis inte vara rimligt. Utan då får du lägga en request där du säger "Hej, vi håller på här borta lite, vi skulle ha access till det här API:et". Då kan man styra mer över behörigheterna. Det handlar litegrann om att förbättra behörighetsmodellerna. Nu har jag mest erfarenhet ifrån bankvärlden och där är det inte ett jätteproblem, det finns jättehöga krav på säkerheten. Men det gör det såklart inte på alla företag.

15 EB: Om man kopplar detta till införandet av GDPR på ett mer generellt plan. Hur ska en organisation hantera sin skugg-IT för att bli compliant med GDPR?

16 Informant 2: Första steget är väldigt enkelt. Du måste informera i princip hela företaget och säga "Det här är det som gäller, det här regelverket är stort och det här är det man vill värna om". Asså GDPR är ett jäkla bra regelverk egentligen utifrån individens integritet. För oss EU-medborgare är det ju hur bra som helst. Men det ställer såklart till massa bekymmer för företag. Men om man förklarar vad det är och vad det är till för, vad de vill värna om och vad man eventuellt kommer åka dit på. Jag börjar bli trött på alla konsultfirmor och även oss själva ibland som hotar med viten och böter och det är 20 miljoner euro och så vidare, strunt i det, det är inte det som är grejen. Rykte och att eventuellt tappa kunder det är där som verkligen kommer svida. Av 10 konkurrenter så kommer de som är bäst på att hantera och kommunicera hur de hanterar personuppgifter som kommer få störst förtroende. Men informera organisationen och meddela att ni som eventuellt håller på med någonting, tänk på vad ni gör på dagarna. Har ni någonting som innehåller personuppgifter eller liknande och då kanske någon kommer på "ja men herregud jag har ju den här databasen som jag fick av en utvecklare för tre veckor sen". Kan man trigga det på det viset så är det bra, jag tror blir väldigt svårt om man tror att man centralt kan skanna av varenda disk i hela företaget för att hitta personuppgifter eller vad det nu kan vara. Man måste börja med medvetandegrejen och förklara att det kommer vara avgörande för vårt företag att vi har koll. På samma sätt som att vi inte vill köpa produkter från diktaturer eller produkter framställda av barnarbete. Mekanismen för att försöka genomföra detta centralt är så pass stor så det kommer knappt att gå. Då hade man fått lägga ner all affärsutveckling de kommande åren bara för att syna all shadow-IT. Sen får man bestämma sig för, och jag tillhör då de som är lite mer liberal gällande shadow-IT, att man bestämmer sig för att vi vet att det förekommer parallella databehandlingssätt och det är okej till viss del, det är ok i detta området men absolut inte i detta området, så är man tydlig med att klargöra vad som gäller. Det finns säkert firmor som kommer såhär och säger "Hej vi har köpt en produkt som du kopplar in i nätverket och den kommer scanna alla paket och så kommer vi kunna se om de innehåller personnummer." Att man på det sättet skulle kunna identifiera illegala personuppgiftsflöden då så att säga. Den typen av produkter kommer inte funka då de flesta företag har så mycket legacy och är så spretiga att om du startade ditt företag i fredags med unix-plattform och allting utvecklat i JAVA, då kanske du kan fånga upp sådant men inte på ett stort företag, inte en chans. Det är medvetenheten som styr. Man ska inte koppla detta då till att man kan få böter utan koppla det till företagskulturen. Vi tycker att det är superviktigt på vårat företag att vi hanterar våra kunders data på ett rätt och riktigt sätt. Det är lika självklart för oss som att vi ska välja porslinsmuggar istället för pappersmuggar och så vidare. Vi har inga ambitioner att dyka upp i dagens industri eller expressen där det står att vi har registrerat fel typ av information. Till exempel på HR-avdelningen, där tror jag det finns rekryteringsansvariga eller HR-chefer som skrivit ner hur duktig de tycker Pelle Olsson är på sitt jobb. Då får man säga "låt bli med det, eller så får vi hitta ett sätt att kunna redovisa det där". Jag tror inte att folk tänker på det som en personuppgift. Inte bara var man är född och bor och så men även dessa omdömena som skrivs. Framförallt när det blir så att de snuddar på den personliga integriteten. Det är ju inte

så kul att det finns registrerat att Pelle är en surpuppa liksom. Det blir så klassiskt men det är det som gäller, det är mindset och information av vad som gäller. Jag tror inte man lyckas genom hot med viten. Jag har jobbat jättemycket med olika regelverk och speciellt inom finansvärlden så är det jätteviktigt att man säkerställer att banken till exempel alltid agerar i kundens bästa. Om kunden vill köpa 10 volvoaktier då är banken skyldig att säkerställa att kunden alltid får det bästa priset. Då måste banken gå ut på börserna och fråga vad alla tar för volvoaktierna och se om det finns någon matchning någonstans. Värnar man inte om det så är man ju rökt. Den delen kan man visserligen sköta med viss mekanik men det är ändå viktigt att förstå att man ska värna om kunden.

17 EB: Under de senaste åren så har fenomenen “Bring your own device”, “Bring your own service” och “Bring your own app” blivit otroligt populärt i organisationer. Hur ska man hantera detta nu när GDPR skall införas? Hur tror de här fenomenen kommer påverkas utav de ökade kraven på informationssäkerhet?

18 Informant 2: Det beror lite på hur modernt företag man har. Men om man går mot att workplacemiljön och den personliga lagringen är molnbaserat och du kör office365 eller du kör sharepoint eller sådär, då är problemet ganska litet. Finns ingen anledning för mig att lagra det på min ipad när jag ändå är connectad till ett cloud.

19 EB: En sanktionerad cloud-lösning då menar du.

20 Informant 2: Absolut. Att ligga kvar då med gamla fil-servrar och fil-kataloger där du egentligen måste ta med dig grejer på en sticka eller så för att kunna jobba hemifrån, där har du ett stort problem. Då måste man låsa ner de möjligheterna. Man kan ha mjukvarucertifikat på devices eller hur man vill men i det här fallet så är ju molntjänster att föredra. Det bästa är ju egentligen att man har interna moln, för då behöver man inte bry sig om var datan lagras. Vilket kan bli ett bekymmer om du lagar på ett internationellt cloud, du vet ju inte exempelvis om kundens data kommer ligga i Mexiko eller i Hong-Kong. Jag ser inte att problemet med BYOD är så jättestort. Pappersportföljen är ett minst lika stort problem liksom. I en ipad har kan du i alla fall ha en pin-kod för att komma in i, det har inte alla portföljer. Man skulle nästan kunna vrida det till ifall man har en modern workplace och en hårdvaru-agnostisk syn på hur man accesar den personliga datan och kör allt i molnet så är det nästan en fördel. Sen som ni var inne på i intervjuunderlaget där att då blir amazon eller microsoft personuppgiftsbiträden, det kommer de inte har några problem med att hantera, jag är inte bekymrad alls över de stora molntjänstleverantörerna. Bara man skriver in i avtalet klart och tydligt vem som är ansvarig och att de accepterar det. Men det är mer en juridisk del än någonting annat. Jag har ganska stort förtroende för molntjänsterna som vi snackat om hur många år som helst och de är ju här nu, de är hur säkra som helst. Men du behöver kanske inte lägga allt i Berras molnfirma i källaren. Kör de på de stora och de kommer inte ha en chans om de inte anpassar sig. Detta gäller ju inte bara företag inom EU utan även företag som hanterar kunder som är EU-medborgare. Vilket gör att det blir ett internationellt regelverk.

21 EB: Nej många förstår inte hur pass omfattande regelverket är och det kommer ju påverka de flesta organisationer i hela världen.

22 Informant 2: Ja och jag då som arbetat med regelverk i många år. Singapore brukar vara tidiga och MAS, dvs kinesiska regelverk. Sen tar det bara något år och sen uppträder samma regelverk någon annanstans. Att GDPR just bara finns i EU är bara en tidsfråga, det kommer snart dyka upp i resten av världen. Vi skojar internt om att detta är Y2K nivå på det här med GDPR och då var det någon nittiotalist som undrade vad Y2K var och då fick jag förklara det. Det var en jättestor hype då om att säkerställa driften, man visste inte vad som skulle ske. Med GDPR så vet vi vad som kommer ske, den kommer träda i kraft 25 maj nu om 13 månader idag, eller igår kanske. Nej så det här är mycket större än folk tror. Så där har ni gjort helt rätt spaning. Däremot så kommer många företag att ha is i magen och chansa. Det kommer inte börja delas ut böter till en firma på 100 pers som hanterar 1000 kunder. Jag tror inte det kommer att ske.

23 EB: Nej men det är väl lite det vi har identifierat också. I vår uppsats behandlar vi mer GDPR som en extern faktor som ökar kraven på organisationerna, vi fokuserar inte så mycket lagtext eller siffror.

24 Informant 2: Nej jag körde samma retorik i mina tidigare år. Jag jobbade mycket med att övertyga både stakeholders och IT-personal att de får ha koll på sina grejor då det kommer ett nytt regelverk. Då slutade jag alltid med att fråga ifall de tror att det kommer komma fler eller färre regelverk framöver. Då skrattade alla och sa ja men det kommer komma fler. Ja det kan ni ge er på att det gör. Det är så det kommer att se ut och då är det lika bra att hålla koll på grejerna. Man kanske kan dansa undan GDPR om man har tur men sen vips så kommer det något annat så det är lika bra att ha koll på grejerna liksom.

25 EB: Då går vi in på slutspurten här i frågeguiden. Det är vilka nackdelar skugg-IT för med sig. Vi har ju pratat mycket om fördelar.

26 Informant 2: Det som jag har stött på mest i alla fall i mitt yrkesliv är ju mer nackdelar än fördelar. De flesta företag idag fortfarande, och det är märkligt, delar upp IT-kostnader och andra kostnader. Så mäter man det på IT-kostnader och sen har man ett mål som säger att man ska få ner IT-kostnaden, då blir sådana som jag väldigt upprörd för IT-kostnaderna ska ju gå upp. Då frågar de vad man menar, jo men vi ska ju automatisera och robotisera och vi ska digitalisera, det säger sig självt att IT-kostnaderna ska gå upp. Det säger sig självt att IT-kostnaderna ska gå upp. Det finns ju inga företag som inte är beroende av IT. Då gör man ofta så att man benchmarkar och följer upp och mäter effektivitet i kopplat till IT-kostnader. Så försöker man hitta ett mått på företagets effektivitet eller liknande och då fångar man inte in shadow-IT. Ur det perspektivet så får du en felaktig uppföljning. Du får inte till det incitament som krävs för att följa upp vissa kostnader. Du får inte in shadow-IT kostnader och du får inte in tillräckligt med mängd för att styra åt ett visst håll. Du kanske har 10 servrar centralt och 20 servrar utsmetade i shadow-IT. Då har du helt plötsligt 30 servrar och det är dem du ska gå in

med i dialogen med leverantören om du ska sänka priserna. Ur väldigt många perspektiv måste du få in det. Enligt min erfarenhet finns det en väldigt begränsad ambition men även förmåga i shadow-IT förekomsterna att titta på IT-säkerheten, att jobba med internal controls och se till att kvaliten är hög, till att man tänker långsiktigt. Det ser jag inte så mycket av utan det är ju oftast frifräseri liksom. Det blir inget bra på totalen. Dessutom blir det ju svårt att styra IT, det blir svårt att följa upp och återigen tillbaka till compliance, oavsett om det är ett regelverk eller ett företags egna policy som gäller så är det väldigt svårt att följa upp och veta om man är en god organisation eller inte. Det andra som kan bli ett bekymmer är ju kompetensfrågan. Det har jag sett hands-on exempel på. Duktiga utvecklare som borde kunna sitta och utveckla system för tiotusentals personer, de blir internt headhuntade till att jobba på någon affärsenhet eller någon business support enhet men i själva verket sitter dem och kör shadow-IT. Då suger du ut en väldigt bra kompetens till ett smalt område men den kompetensen skulle kunna användas mycket bättre. Speciellt om du tar data-science eller data-mining som jobbar mycket med algoritmer och skriva strategier. Den kompetensen går inte att hitta på stan så att säga. Då utarmar du den centrala IT förmågan genom att de har försvinner ut i linjen på väldigt smala användingsområden.

27 EB: Det du säger egentligen då är att hanteringen av skugg-IT måste integreras i det vanliga informationssäkerhetsarbetet i organisationen?

28 Informant 2: Ja precis, om vi då tar GDPR perspektivet. Om man lyckas övertyga och informera om och sälja in behovet av en hög nivå av GDPR-compliance i organisationen, då kommer allting lösa sig självt. Då kommer man inte behöva några kontrollanter som går runt och kollar att folk gör rätt. Då ligger det i grunden hur man jobbar. Men så är det ju inte utan då måste man ha någon form av kontrollmekanism för att kompensera för det där.

29 EB: Okej, jätteintressant!

30 Informant 2: Ja det här är jätteintressant. Ni har valt helt rätt ämne. Egentligen så skulle jag gett er något mer namn. Ni skulle fått tag på en som jag känner som byggt upp en egen shadow-IT organisation parallellt på sitt företag han jobbar på och höra efter varför.

31 EB: Det skulle varit otroligt intressant. Jag tror inte de skyltar med det heller å andra sidan. Om man tänker kostnader och om du tänker ordning och reda. Jag tror inte att man kan få en organisation att ha rätt mindset. Vi är inte så som personer, vi klarar inte av att följa alla regelverk samtidigt. Jag är väldigt mycket för att man behöver ha en centraliserad styrning och centraliserad uppföljning. Jag tror dessutom att det blir billigare att köra IT om man centraliserar så mycket det går. Inget snack om det liksom. När det gäller framför allt affärsutveckling och “time-to-market” så måste man acceptera en viss form av shadow-IT. Om du tar utvecklingsperspektivet så tycker jag man kan ha det. När man sen kommer fram till att man vill provsätta ny kod eller nya funktioner. Då kan man kanske placera det centralt med central förvaltning. Det är förmodligen lättare då att vara förvaltare och agil utvecklare är sällan samma persontyp. Men utvecklingen måste ske kontrollerat. Att göra det med maskad

eller anonymiserad eller pseudoanonymiserad data är ett sätt rent konkret att göra det på. Shadow-utveckla allt ni vill här borta men se för fan inte till att ha live data för vi får inte enligt lag. I de flesta branscher är det inte god utvecklingssed och i de flesta är det inte tillåtet.

33 EB: Nej precis. Det bekräftar mycket av det vi har läst i teorin också att det finns fördelar att hämta från shadow-IT och att man bör uppmuntra viss användning då det kan leda till en stark affärsutveckling.

34 Informant 2: Nej precis, nu kommer jag från bankvärlden som är väldigt traditionell men till och med där så ser dem det som ett starkt konkurrensfördel att jobba på det här viset. Men som sagt i GDPR-perspektivet så är jag mer bekymrad över shadow-IT i relation till personuppgiftsbehandlingen. Man ska inte ha GDPR-utbildningar utan utbildningar som handlar om värdering med fokus på personuppgifter, och by the way det finns ett regelverk också.

35 EB: Kanon! Då har vi inget mer och får tacka för din medverkan.

9.3.3 Intervju 3 – Informant 3 – Organisation 2

Intervjuare - Erik Bråtendal (EB)
Sekreterare - Per Jansson
Informant 3 - Intervjuobjekt - Senior konsult, internet certifierad att arbeta med kunders arbete mot GDPR-compliance. Lång tids erfarenhet av skugg-IT inom banksektorn.

START

1 EB: Sådär, du skulle kunna börja med att berätta vad du har för erfarenhet av skugg-IT och hur du känner till fenomenet?

2 Informant 3: Ja, jag har nog egentligen stött på det i två perspektiv, först när jag jobbat som IT-revisor och utfört revisioner eller audits på stora företag i USA. Jag har även stött på

det när jag arbetat som linjechef för en större statlig myndighet i Sverige. Där jag då konstaterade att olika avdelningars tillkortakommanden leder till att folk löser problemen på egen hand. Min erfaranhet är att det är i regel relaterat till organisationens bristande förmåga att kunna tillhandahålla de verktygen som krävs eller specifik utrustning eller specifika delar av en verksamhet som inte täcks in i den så kallade 80/20 leveransen som så många IT-avdelningar levererar efter.

3 EB: Då menar du att det finns sanktionerade IT-artefakter som ändå inte täcks in av deras vanliga säkerhetsarbete.

4 Informant 3: Ja, det är sånt vi hittar när vi gör revisioner. Oftast handlar det om extremt verksamhetsnära IT-utrustning. Ofta handlar det om sådan IT-utrustning som inte vanligtvis är nätverksansluten. Om man tittar 50 år tillbaka i tiden så på ett sjukhus till exempel så finns det medicinteknik-avdelningar som ligger utanför IT-avdelningen. De har ju traditionellt sett haft hand om att exempelvis byta papper i EKG-skrivaren och så vidare. Den IT-utrustning som historiskt sett har varit mer mekanisk är numera nätverksansluten och ställer egentligen större krav på säkerhet men är oftast styvmodigt behandlade när det gäller säkerheten eftersom de teknikerna inte har kunskapen själva. De kraven de eventuellt kan ställa är krav som IT-avdelningen inte är vana att tillgodose. Annat exempel är i industrin med svarvar och borrar och så vidare, kärnkraftsutrustning till exempel. Den utrustningen är ju i regel rätt väl skyddad. Samma med övervakningskameror och kringutrustning, styr- och regler-teknik för industrikomponenter där man egentligen inte ser IT som IT utan man köper utrusting som man tycker ska hålla i 20 år och den ska styras av en dator och den ska övervakas helst utan att behöva sitta i det där bullriga rummet. Dessa skyddas inte som de ska.

5 EB: Det är intressant för det blir ju en helt ny dimension till vår frågeställning, det här har vi inte snubblat över tidigare.

6 Informant 3: Jag tycker den är viktig därför att det här är en stor massa och en stort problem. Dessutom när vi börjar prata om den här utrustningen så de som har utvecklat utrustningen och de som har utvecklat styr- och regler-teknik för industri. De kan tänka på massvis med saker, hållbarhet, tåla dåliga miljöer och fokuserar mycket på tillgängligheten kring jsut timmälmningen, men de fokuserar ofta inte på informationssäkerheten så det är väldigt oskyddat. Är ni lite intresserade av säkerhet har ni säkert läst att övervakningskameror regelbundet hackas för att användas i DDOS-attacker.

7 EB: Vad skall man i organisationer vidta för åtgärder för att förhindra den här uppkomsten av skugg-IT?

8 Informant 3: Först och främst så är det viktigaste vad vi kallar sjukdomsinsikten. Man måste förstå sina IT-miljöer och inte skilja ut saker, man får helt enkelt inte delegera till IT-avdelningen att säkerställa att utrustning och information är skyddad. Ansvaret och uppställningen måste ligga mycket högre upp i organisationen. Om du har ett strukturerat

informationssäkerhetsarbete som ligger ovanför IT-avdelningen så kommer man även att fånga upp sådana här saker. Om det ligger i linje eller parallellt med business operations. Då får man en bättre bredd och då frågar man inte bara IT innanför ramen av deras ansvar utan då frågar man alla innanför ramen just dem har. Det är väl det mest grundläggande sen behöver man även förstå sin arkitektur och sin IT-miljö. Vart det finns information, vilken typ av information det finns, vart det finns utrustning och vilken typ av utrustning det är. När man vet det och när man har god kontroll över var man har vilken information och vilken utrustning och vad den kan användas till, då har man kommit en bra bit på vägen. Man behöver befinna sig på en så pass hög nivå och man måste samtidigt ha tillgång till kunskap. Säkerhetsavdelningar kallas idag för informationssäkerhetsavdelningar men de har också ansvar för fysisk säkerhet i en stor organisation och traditionellt sett så är de bättre på det. Eller jag kan inte säga att det alltid är så men av det jag har stött på så är det så. De är liksom lite traditionella och gammaldags. Det är en organisatorisk utmaning som många står inför.

9 EB: Vi pratade tidigare om det här att det är viktigt att hålla koll på var någonstans informationen är. De senaste åren har vi ju sett trenderna som BYOD, BYOS och BYOA fått mer utrymme. Folk tar in osanktionerade prylar och mjukvaror i organisationerna och hur tror du detta kommer påverkas av införandet GDPR?

10 Informant 3: Ja det här är ett jätteproblem. Det stora problemet är att det är så pass kostnadseffektivt så vi kommer att fortsätta med det. Jag kan köpa en telefon till en anställd för fyratusen kronor och så har jag tiotusen anställda. Eller så säger den anställda “Nej men jag har en egen som är mycket modernare och coolare som jag tycker är roligare att jobba med”. Då kostar det mig ingenting. Pengarna styr ganska mycket och man har ganska dålig koll på riskhanteringen. Återigen lite det där med sjukdomsinsikten, man har inte satt en peng på risken att information försvinner och där har man ett ganska bra case med GDPR för det är precis det som GDPR gör. De hjälper till med kostnadsanalysen, du kan strunta i allt det här men då kommer det kosta dig såhär och såhär mycket och så vidare. När vi hade PUL så kunde du strunta i allt det här, det kan du fortfarande göra men eftersom ni gjorde det gällande PUL så petar vi in lite sanktionsavgifter här så ni förstår att om de tycker det är dyrt med att köpa in telefoner och etablera ett fungerande säkerhetsarbete så får de vara beredda att ta risken med att få betala upp till 4% av omsättningen i sanktionsavgifter.

11 EB: Hur stor påverkan tror du sanktionsavgifterna kommer ha? Är det något företagen faktiskt kommer förhålla sig till eller kommer de tänka att det aldrig kommer hända oss?

12 Informant 3: Det där är lite olika. Men det jag kan säga med stor säkerhet är att det har påverkat marknaden i Sverige avsevärt. Därför jag har aldrig haft något uppdrag rörande PUL exempelvis men nu får jag jobba hela dagarna överallt med GDPR. Det har absolut en positiv påverkan på företagens vilja att göra någonting.

13 EB: Ja det blir ju väldigt tydligt när du säger på det sättet.

14 Informant 3: Ja det är nästan fånigt. Det jag ägnar en stor del utav min tid åt är att förklara att om ni hade brytt er om PUL och om ni hade brytt er om informationssäkerhet så hade det här varit en lätt övergång men nu har dem inte gjort det. Nu tycker dem det är viktigt helt plötsligt. Ska dem börja från grunden eller vill de ta en genväg? GDPR är också informationssäkerhet, personuppgifter är en informationstyp. En sak med GDPR som jag tycker många missförstår när jag är ute hos dem och det jag tycker är intressant med GDPR ur ett informationssäkerhetsperspektiv är att det skär rakt igenom allt i organisationen därför det är inte min information, man glömmer bort när man börjar fundera på hur man ska göra att det är någon annans information. Det har företag inte riktigt fattat trots att suttit med andras information hur länge som helst. Det är spännande, men ja sanktionsavgifterna gör nytta idag och det blir spännande att se vad dem leder till. Man kan dra paralleller till HIPAA, den amerikanska motsvarigheten med fokus på hälsoinformation. Där har de med fängelsestraff i skalan som är lika inarbetat som sanktionsavgifterna i GDPR. Där får man en enkel biljett till Riker Island om det går åt skogen. Ingen har åkt i fängelse hittills. De tidigare domarna ligger på cirka tiotusen dollar, nu för tiden är de uppe i 4,5 miljoner dollar. Det där handlar om att man hotar om att man kan döma ut det. Jag tror inte att någon i juni 2018 kommer få 20 miljoner euro i böter, vilket jag tycker är bra. Samtidigt som det en balansgång, man måste, och här är åtminstone Sverige i regel, jag skulle inte säga sämre men vi har det svårare att anpassa situationen, upplever jag rent juridiskt. Det är väldigt mycket antingen eller. För om man gör fel och saker och ting har hänt och du kommer undan, då kommer man tappa respekten för det här. Det är ganska små marginaler.

15 EB: Vi pratade lite tidigare om vilka fördelar som kunde komma med skugg-IT.

16 Informant 3: Jag tycker egentligen inte det finns några som helst fördelar med skugg-IT. Utan skugg-IT är ett symptom på andra brister. Det skulle inte hetat skugg-IT om det fanns något bra med det, då skulle det hetat effektiv-IT eller något åt det hållet. Det finns ingenting som är positivt med det i sak, men jag tror det kommer ta väldigt lång tid att hitta effektiva lösningar på det. Det handlar om att IT-avdelningar, säg att du har en IT-avdelning på mellan 30 och uppåt anställda. Det är ändå en rätt stor avdelning och du har jobbat med att utveckla en etablerad IT-avdelning under ett antal år, du har rekryterat folk med viss kompetens för att göra en viss sak och så vidare. Det man har gjort de senaste 20 åren är att försöka rektrytera och leverera till 80/20. Vi ska vara effektiva till allt som vi förstår och känner till. Men verksamheterna har idag så mycket mer behov som de inte kommunicerar samtidigt som tekniken fullkomligt exploderar. Varför ska jag vända mig till min IT-avdelning, om vi säger att det tar ett och ett halv år att ta fram ett nytt IT-system där jag kan hitta en viss information i min telefon, när den appen redan finns klar och tillgänglig att hämta. Då tror man att ens IT-avdelning är dålig och att den inte kan leverera och det ligger ju något i det. IT blir ju aldrig bättre än de kraven man ställer på den liksom. När jag är ute hos kund så förutsätter jag att de behöver vidta åtgärder för att hantera skugg-IT även om de inte säger rakt ut att de ska ha det. För annars kommer de skapa sig falsk trygghet när de säger “nej men vi har sagt att man inte får ta med sig egna enheter, så därför händer det inte”. Så är det ju inte. Det finns inga motsättningar egentligen till att folk tar med sig egna enheter, det blir en diskussionsfråga som

inte är löst bara. Man borde föra diskussionen som så att “Ja men om du vill använda din enhet i tjänsten så får du göra det förutsatt att…..” och så vidare. Man kan inte promota att stoppa Bring your own device utan att erbjuda ett alternativ. Om du inte erbjuder ett alternativ så får du då vara beredd på att den anställda säger “jag vill inte att du managerar min telefon, så vet du vad, jag tänker inte använda telefonen i mitt arbete”. Då får du acceptera att individen inte kommer vara tillgänglig på telefon exempelvis. Det där kommer nog skilja sig från arbetsplats till arbetsplats och jag tror att facken kommer nog ha lite åsikter om det där också.

17 EB: Vi har kollat lite på GDPR kopplat till molntjänster. Det är väldigt intressant för molntjänster är lite samma sak som BYOD bara det att man skickar upp informationen i något moln som man inte har någon aning om vad informationen lagras. Hur stor problematik tror du det finns här hos organisationer? Har de koll på var de har all sin information på nätet?

18 Informant 3: Nej, dem har inte det idag och när du säger dem, jag är ju då från IT-avdelningen så då är det väl 80/20 igen då. Det finns folk som har förhållandevis eller väldigt god kontroll över sin information. Men dem ringer ju inte oss å andra sidan. De flesta som vi kommer ut till har inte det, men de har heller ingen tradition av att ha det. De har inte koll på sin egen information i sina egna miljöer och har aldrig haft det heller.

19 EB: Så de har inte ens identifierat det som ett problem?

20 Informant 3: Nej, dem vet inte vad de faktiskt har för information och de vet inte vad det kan få för påverkan på organisationen om den hamnar i orätta händer. Det gäller inte bara personuppgifter utan jag har stött på kunder som har en IT-avdelning som levererar efter 80/20 om vi kallar det så, så har de en avdelning som visserligen har väldigt få användare men de genererar en anseende mängd av firmans revenue, det vill säga det firman lever på. Det kan vara R&D avdelningar, det kan vara folk som sitter på patent pending, det kan vara massvis med sådana saker som är en liten del organisatoriskt men en tung del rent informationssäkerhetsmässigt och dem får inte sina behov tillgodosedda. Men dem förstår i regel dem här behoven så dem kommer skaffa sig lösningar i molnet, eller på andra sätt som är mycket, mycket bättre än det organisationen levererar. Men den sista lilla touchen är att det blir jättesvårt för alla obehöriga att komma åt den här informationen för den här molnlösningen är jättebra men leverantören kan komma åt all information. Så de väljer att lita på en entitet. Men man får inte glömma att det är ingen skillnad på molntjänster och det vi har sysslat med de senaste 20 åren; outsourcing. Det är samma sak, skillnaden är väl då att definitionen av en molntjänst är att den bygger på tillgänglighet och att informationen kan vara utspridd och var som helst kan informationen befinna sig vid ett givet tillfälle. Det upplever man ju som ett stort problem med GDPR, att man börjar funderar över vart informationen finns och i vilket tredje land och så vidare. Problemet har man redan haft när man började outsourca saker. Du kan ju välja att strategiskt säga att vi ska bara outsourca till ett svenskt företag, men du kan ju inte styra marknaden och det svenska företaget du outsourcade till idag kan vara kinesiskt imorgon.

21 EB: Tror du outsourcing kommer påverkas av GDPR? För det är ju också information som skickas ut.

22 Informant 3: Ja jag tror det kommer påverkas på exakt samma sätt som molntjänster och det jag tror som kommer hända är att det kanske är tydligare med molntjänster så de blir först. Eftersom sourcing partners är i regel så att säga en "gammal" IT-avdelning. Men jag tror att det kommer dyka upp fler och bättre molntjänster. För det är ändå en konkurrensfördel att vara så nära compliant man kan vara. Så att folk säger "ska vi välja molntjänster så ska vi välja dem där". Jag tror att det kommer hända mycket gällande det här och GDPR för den ligger och spänner överallt. Men det borde ha hänt tidigare men det har det inte gjort.

23 EB: Precis som med BYOD så finns det icke-sanktionerade molntjänster, det vill säga anställda lagrar information i sin privata dropbox eller liknande. Är det någonting du har stött på och hur ska man hantera det här? Är det återigen uppifrån eller är det via IT-avdelningen?

24 Informant 3: Det finns egentligen inte så vansinnigt många sätt. Du bör och kan etablera policies och riktlinjer och så vidare. Sen kan du följa upp dem och så kan du börja hota folk med avsked och annat ont. Det kommer inte lösa problemet men det är nog viktigt att ha med det. Sen måste du utbilda folk, inte till att använda de befintliga systemen utan att förstå vilken information de har och vad den har för påverkan och vad det leder till. Det är nog den kanske den enskilt bästa hanteringen för en individ som förstår vad det är den behandlar kommer åtminstone ställa sig själv frågan i första hand "kan jag göra såhär men den här informationen?" i bästa fall frågar samma person någon mer, en säkerhetsansvarig eller IT-ansvarig och så vidare. Problemet är återigen då att folk vill vara effektiva, de vill vara duktiga och de vill få jobbet gjort. Klarar man inte av att tillhandahålla det som IT-avdelning då vette sjuttsingen. Men jag tror det kommer dyka upp fler och fler bra lösningar. Jag tror det kommer komma fler tillämpade lösningar, om du vill göra det här så gör det här och så vidare. Teoretiskt sätt kan både en molnleverantör och en outsourceleverantör leverera det, även en intern IT-avdelning. Men gör man inte det så kan det gå illa. Folk vill vara effektiva och de vill göra rätt men om de får välja mellan de två så kommer de välja att vara effektiva. Det enda som kan balansera det är kunskapsförståelse. Men du måste göra det lätt att göra rätt.

25 EB: Exakt, då har jag faktiskt inga fler frågor till dig så vi får lov att tacka för din medverkan.

9.3.4 Intervju 4 – Informant 4 – Organisation 3

Intervjuare - Erik Bråtendal (EB)
Sekreterare - Per Jansson
Informant 4 - Intervjuobjekt – Informationssäkerhetsansvarig på ett privat företag inom välfärdssektorn.

1 EB: Vad har du för någon relevant erfarenhet av fenomenen skugg-IT och GDPR?

2 Informant 4: Ja, när det kommer till dataskyddsförordningen så arbetar jag väldigt mycket med den just nu i min roll som funktionsansvarig för informationssäkerhet här på *Organisation 3*. Jag hjälper till i arbetet när vi försöker försäkra oss om att vi kommer efterleva förordningen till 100% när den träder i kraft i maj 2018. Så jag är bra uppsjungen i dataskyddsförordningen. Vad gäller skugg-IT så känner jag till begreppet.

3 EB: Har du någon erfarenhet från skugg-IT i din egen organisation? Är det någonting ni har i åtanke nu med implementeringen av GDPR?

4 Informant 4: Ja det är väldigt tydligt i våra styrande dokument att man som anställd inte får installera mjukvara som inte är godkänd eller använda sig av molntjänster som inte är godkända. Men vi vet ju trots allt att det förekommer och då måste vi säkerställa att de används på ett sätt som är förenligt det vill säga att patientdata inte lagras i molnet i tjänster som inte är godkända och så vidare.

5 EB: I en annan intervju så pratade vi med en konsult som har erfarenhet inom vårdföretag bl.a. Han berättade att ett stort problem är verksamhetsnära utrustning som tidigare inte var uppkopplad numera är det. Till exempel EKG-skrivare eller dialysmaskiner och att de numera också kan lagra personuppgifter. Är det någonting ni också reflekterat över?

6 Informant 4: Medicinteknisk utrustning innehåller i många fall personuppgifter och gör det fram tills att det tas bort. Det kan tas bort genom att integreras med journalsystemet men det kan också vara så att de ansvariga anställda måste aktivt ta bort informationen från utrustningen. Så det är vi väl medvetna om, att det finns risker kopplat till den medicinska utrustning. Man måste säkerställa att personuppgifter tas bort inom en rimlig tidsperiod från till exempel ultraljudsapparater och så vidare.

7 EB: Varför tror du skugg-IT uppstår i organisationer?

8 Informant 4: Det uppstår för att det är så enkelt. Säg att man som anställd har ett behov och man vet att det tar tid i de vanliga kanalerna att få en IT-lösning på plats som fyller det behovet så är det väldigt enkelt att använda sig av molntjänster till exempel som fyller samma behov som användaren har. Det finns ju de här dropbox och de andra lagrings-plattformarna som anställda väldigt enkelt kan skapa ett eget konto och bjuda in kollegor och börja använda

det som någon slags kommunikationsplattform. Så det är väl det som är anledningen egentligen, att det är så enkelt och det går snabbt att fylla det behovet man har.

9 EB: Du nämnde innan att ni hanterar detta med hjälp av policys och regelverk. Är det hela lösningen på hur man bör hantera detta?

10 Informant 4: Vi hanterar detta med policys och riktlinjer och sedan så har vi delar av organisationen där vi gjort vissa tekniska uppföljningar för att identifiera molntjänster som används. I vår franska verksamhet så har vi skannat av nätverket för att undersöka vad som används och då är nästa del sen att kontakta de individer som använder sig av dem och undersöka hur de används. Används det för privat bruk eller används det för företagsändamål och i så fall, vad är det för behov som behöver fyllas upp och vad är anledningen till att man använder det. Om vi tar dropbox som exempel så har vi interna molnlösningar som är minst lika bra och minst lika användarvänliga men framförallt säkerställda. Det finns ju risk kopplat till molntjänster som inte bara är kopplat till säkerhet utan även att man inte har rätt avtal på plats som beskriver hur personuppgifter får hanteras och så vidare. Sen har vi sett i de analyser vi gjort i bland annat Frankrike där vi identifierat molntjänster som användes så kunde vi säkerställa att det inte var patientdata som användes. Vi har haft lite dialog internt då och tagit upp om vi ska blocka till exempel dropbox eller vissa molntjänster. Men det handlar nog mer om att utföra analyserna, följa upp och föra en dialog så att man säkerställer att de används på rätt sätt och att man styr de anställda mot att använda de godkända tjänsterna.

11 EB: Tror du det finns några positiva aspekter med att anställda använder sig av egna skugg-IT lösningar?

12 Informant 4: Den positiva effekten är som sagt att det går snabbt och det är en del i innovationen att hitta IT-sätt som gör det lättare och effektivare att arbeta. Men som jag säger så oavsett detta så är det big no här för oss för vi har lösningar som motsvarar de externa molntjänsterna och det kan mycket väl vara så att man kommer fram till att en viss molntjänst skall användas men då vill vi säkerställa att den används på rätt sätt och är tillräckligt säker.

13 EB: Kan det bero på att era anställda inte vet att ni har motsvarande funktionalitet i era egna sanktionerade system?

14 Informant 4: Ja så kan det nog absolut vara i vissa fall.

15 EB: I och med implementeringen av GDPR, hur tror du skugg-IT kommer påverkas av detta? Det har inte varit jättemycket i fokus.

16 Informant 4: Utifrån vårt perspektiv med vårt regelverk och vår strategi för hur personuppgifter skall hanteras så på inget sätt egentligen. Vi har idag ställningstagandet att bara godkänna molntjänster där detta kan appliceras. Sen så har vi precis fått igenom ny policy kopplat just till dataskyddsförordningen och personuppgiftshantering och kopplat till

den kommer det nu göras större utredningsinsatser för medarbetare. Det kan ju vara så att man som en del i de utrednings-insatserna själv identifierar något och blir mer medveten själv och på så sätt kan identifiera de enstaka fall där man hanterar personuppgifter på fel sätt och på det sättet kan det komma till rätta och se till så man hanterar det på rätt sätt. Men i grund och botten så tror jag väl inte att dataskyddsförordningen har så jättestor inverkan på oss. Jag skulle bli väldigt förvånad om vi till exempel hade patientuppgifter i molnet som inte är godkända.

17 EB: Så det du säger är att ni hanterar redan detta inom ramen för de existerande policys och regelverk ni satt upp för att verka mot GDPR-compliance?

18 Informant 4: Ja och sen får vi se om vi överväger att göra motsvarande tekniska analys här som vi gjorde i Frankrike för att följa upp om molntjänster som inte är godkända används och i så fall identifiera ifall det finns personuppgifter i något av dem.

19 EB: I och med att GDPR införs så introduceras också sanktionsavgifterna. Hur kommer ni förhålla er till den? Är det någonting ni tänker på över huvud taget? Sjukvården har ju en lång tradition av att behandla personuppgifter. Anser ni ens att sanktionsavgifterna är en del av problemet?

20 Informant 4: Sanktionsavgiften är väl den stora nyheten sett till dataskyddsförordningen. För i övrigt så är det väldigt likt nuvarande regelverk, finns vissa ytterligare tillägg om rapportering av incidenter och så vidare. Men i övrigt så ser vi dataskyddsförordningen som något positivt, att vi på koncernen har samma regelverk i samtliga länder som vi har verksamhet i. På så vis får vi en bättre förståelse för regelverket. För den franska personuppgiftslagen exempelvis så är det väldigt svårt för oss att få en helhetsbild. Men eftersom vi kommer leva under samma regelverk så kommer det underlätta en del. När det gäller sanktionsavgifterna så tror jag att det absolut värsta som kan hända är att vi förlorar kunder och patienter för att de inte litar på hur vi hanterar deras personuppgifter på rätt sätt. Sanktionsavgifterna är något därutöver, det är inget som driver vårt compliance-arbete.

21 EB: Bring your own device känner du säkert till, sen finns även bring your own application och bring your own service. Är det något ni har i er organisation?

22 Informant 4: I koncernövergripande policies och regelverk så säger vi att vi inte tillåter egna devices. Specifika affärsområden kan dock besluta om undantag, där de i sådana fall måste upprätta en policy för hur BYOD får användas. Det är under uppstart och det handlar om rådgivning via nätet, där är det väldigt styrt kring hur den egna utrustningen skall underhållas och skyddas. Så då hanterar vi det genom att sätta upp tydliga regler för firmwareuppdateringar, antivirusskydd och säkerhetspatchar och så vidare.

23 EB: Vad var motiveringen till att ni valde att stänga ned användandet av medtagna egna devices?

24 Informant 4: Det är någonting som har varit med långt innan jag började här men det har med att göra att vi inte kan säkerställa säkerheten för alla olika devices som kan existera i företagsmiljön. Vi kan inte säkerställa alla olika operativsystem och vi kan inte säkerställa att man har ett up to date anti-virusskydd och så vidare.

25 EB: Du nämnde tidigare att ni använder er av molntjänster i ert dagliga arbete. Kommer de påverkas någonting av GDPR över huvud taget eller kommer ni fortsätta som ni alltid har gjort?

26 Informant 4: Vi kommer fortsätta som vi har gjort. Vi har exempelvis journalsystem för mindre verksamheter i molnet. Jag ser inte molntjänster som en större risk än interna it-system. Det handlar snarare om att se till att det är rätt säkerhet i tjänsterna. Vad vi har tagit fram för ett tag sedan eftersom vi ser att det går mot mer och mer molntjänster är en checklista för att analysera molntjänstleverantörer innan vi då går in och skriver några avtal. Vi har en gedigen utvärdering av molntjänster för att se till att säkerheten är tillräckligt god. Till exempel två-faktors autentisering och att lagringen är krypterad exempelvis och så vidare.

27 EB: Så ni har alltid fört en dialog med molntjänstleverantörerna?

28 Informant 4: Det har vi väl alltid haft men checklistan är ganska nyligen framtagen, i slutet av förra året. Den är som sagt för att vara stöd till verksamheten för att säkerställa att vi får rätt säkerhet i molntjänsterna. Checklistan skickas över som du säger till leverantörerna så vi tillsammans kan gå igenom den och säkerställa tillsammans om adekvat säkerhet innan vi går in i avtal med dem.

29 EB: Intressant. Då har jag inga mer frågor faktiskt och får tacka så mycket för din medverkan!