LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Privat molnlagring i tjänsten

Orsaker och potentiella risker

Kandidatuppsats 15 hp, kurs SYSK02
Framlagd juni 2015

Författare: Andreas Lindberg
Katja Marat
David Månsson

Handledare: Björn Johansson

Examinatorer: Bo Andersson
Anders Svensson

Sammanfattning

Titel:	Privat molnlagring i tjänsten – orsaker och potentiella risker
Nivå:	Kandidatuppsats i informatik, 15 hp
Författare:	Andreas Lindberg, Katja Marat och David Månsson
Utgivare:	Institutionen för informatik, Lunds Universitet
Examinatorer:	Bo Andersson, Anders Svensson
Nyckelord:	Molnlagring, BYOD, BYOC, Säkerhetsrisker, Implementering, Efterlevnad.
Forskningsfrågor:	Vilka potentiella risker kan associeras med lagring i externa molntjänster? Varför väljer anställda att lagra yrkesrelaterad data i privata molntjänster före verksamhetens egen lagringstjänst?
Syfte:	Fenomenet analyseras i denna uppsats i syfte att belysa varför anställda väljer att lagra yrkesrelaterad data i privata molnbaserade lagringstjänster före verksamhetens egen lagringstjänst. Vidare ämnar även forskningsbidraget belysa potentiella risker detta kan utsätta företag för. Bidraget önskar skapa bättre insikt och följaktligen stödja beslutsfattande kring verksamheters framtida förhållningssätt till fenomenet.
Metod:	Intervjuer har genomförts hos två företag där fenomenet identifierats. Fenomenets orsaker och potentiella risker har sedan analyserats med hjälp av en analysmetod där våra fynd i praktiken ställts mot motsvarande problematik i teorin.
Slutsats:	Fenomenet orsakas dels av att företag saknar implementerade säkerhetspolicys och dels för att dessa inte efterlevs. Vidare orsakas även fenomenet av att anställda upplever att de interna lagringsmöjligheterna som ges inte erbjuder tillräcklig lättillgänglighet och smidighet. De potentiella riskerna som associeras med fenomenet är att den yrkesrelaterade datan riskerar att hamna i fel händer.

Innehållsförteckning

Disposition

Kapitel 1: Introduktion – I detta inledande kapitel ges en bakgrund till studiens fenomen, en beskrivning av problemområdet samt en presentation av undersökningsfrågorna.

Kapitel 2: Teoretisk referensram – Detta kapitel syftar till att redogöra för de centrala delarna i ämnet och utgör således grunden för denna studie. Kapitlet inleds med ett avsnitt där teorivalen som gjorts motiveras. Vidare presenteras aspekter om molntjänster och BYOD som arbetssätt för att kunna analysera varför anställda lagrar yrkesrelaterad data i privata molntjänster före verksamhetens lagringstjänst.

Kapitel 3: Metod – Följande metodkapitel inleds med en presentation av valet av metodiskt angreppssätt vi applicerat för att besvara forskningsfrågorna. Kapitlet redogör även för hur den teoretiska referensramen framarbetats och hur vi gått tillväga för att samla in den empiriska datan. Vidare redogörs för valet av företag och respondenter i undersökningen. Detta följs av ett avsnitt om analysmetod där vi redogör för hur teorin och empirin ställs i relation till varandra för att besvara forskningsfrågorna. Avslutningsvis återfinns ett avsnitt om kvalitet och metodkritik.

Kapitel 4: Empirisk analys – I detta avsnitt presenteras och analyseras den data som samlats in. Att teori och empiri redovisas och analyseras i samma avsnitt beror på en önskan om att skapa ett bättre flöde i texten men också för att undvika upprepningar. Avsnittet är strukturerat utifrån de delmoment som presenterats i analysmetoden och avslutas med en sammanfattande analys av fenomenets orsaker.

Kapitel 5: Slutsats – I detta avslutande kapitel besvaras undersökningens forskningsfrågor. Avslutningsvis innehåller kapitlet ett avsnitt med våra egna reflektioner kring fenomenet och rekommendationer för framtida forskning.

1 Introduktion

I detta inledande kapitel ges en bakgrund till studiens fenomen, en beskrivning av problemområdet samt en presentation av undersökningsfrågorna.

1.1 Inledning

I en artikel i Computer Sweden presenteras ett fall där gymnasieområdet i Malmö implementerat Googles molnbaserade tjänst Google app for education. Gymnasieområdeschefen i Malmö förklarar i artikeln att majoriteten av de digitala verktyg som används i skolan idag är molnbaserade, och att de i princip aldrig installerar program på elevernas datorer. Trenden att flytta all ”Skol-IT” till molnet är något som gett Datainspektionen en utmaning eftersom skolvärlden hanterar mängder av persondata och när kommunikationen sker via nätet ställs det på sin spets. Avtalet mellan gymnasieskolorna och Google blev därför underkänt av Datainspektionen två gånger, men att man trots detta inte gett upp hoppet. Den framgår även i artikeln att det snart kommer en ny EU-förordning som reglerar detta förhållande, och att de molnleverantörer som siktar på skolmarknaden får se till att kavla upp ärmarna och ta fram avtal som håller måttet (Lindström, 2015).

Efter att ha tagit del av innehållet i denna artikel väcktes en del frågetecken då Datainspektionen exponerat bristfälligheter utifrån ett perspektiv som behandlar individers personliga integritet. Finns det möjligtvis fler bristfälligheter med betydande effekt för verksamheten att beakta utifrån andra perspektiv gällande dessa molnbaserade tjänster?

Inledningsvis väcktes alltså intresset om vilka bristfälligheter i användandet av molntjänster som kan ha betydande effekt för en verksamhet. Detta kom snabbt att identiferas efter en intervju med Mjukvaruutvecklaren hos Företag V. I intervjun framgår det nämligen att flertalet anställda hos Företag V aktivt väljer att lagra företagskänslig data i sina privata molnbaserade lagringstjänster före verksamhetens egen lagringstjänst.

Denna studie avser besvara frågan om varför detta arbetssätt, vidare benämnt *fenomenet*, uppstår och vad detta arbetssätt medför för potentiella säkerhetsrisker för verksamheten. Sedermera förankras frågeställningen djupare i underliggande orsaker med avseende att kartlägga potentiella förbättringsområden för verksamheten att angripa. Frågan om varför detta arbetssätt uppstår studeras mer ingående utifrån litteraturens och verksamhetens syn på säkerhet, implementering/strategi och slutligen hur strategin efterlevs.

Fenomenet beskrivs i teorin som Bring Your Own Cloud (BYOC) och sägs vara den nya tidens Bring Your Own Device och beskrivs som en privat molntjänst som den anställda använder i tjänsten (Merrill, 2014; Patrizio, 2014). Frågan om varför detta arbetssätt uppstår med djupare förankring till säkerhet, implementering och efterlevnad utgör ett tämligen

outforskat område då forskningen om BYOC är relativt sparsam. Denna studie söker därför svar i litteraturen gällande molntjänster och i fenomenet med BYOD där litteraturen (Morrow, 2012) ser övertygande likheter med studiens identifierade arbetssätt. Konceptuellt går det inte att likställa studiens forskningsfenomen med BYOD på samma sätt som att ett äpple inte är ett päron. Båda är dock frukter. BYOD används därför i denna uppsats i syfte att se relevanta likheter mellan hur företag enligt tidigare forskning kan arbeta med BYOD som ett arbetssätt.

1.2 Forskningsfrågor

Forskningsfrågorna, och därmed denna uppsats, ämnar identifiera potentiella risker som kan associeras med lagring i externa molntjänster. Vidare ämnar forskningen identifiera orsakerna till varför anställda väljer att lagra yrkesrelaterad data i privata molntjänster likt Dropbox och Google Drive före verksamhetens egen lagringstjänst. Vårt bidrag till forskningen kan således delas in i två kategorier där den första, 1) analyserar vilka risker fenomenet potentiellt utsätter företag för och 2) vad som orsakar att fenomenet sker. Den första frågan om säkerhetsrisker i association med lagring i molnet besvaras genom att studera litteratur som sedan jämförs med empiri. Den andra frågan om vad som orsakar fenomenet besvaras genom att granska teori och empiri om hur verksamheter i näringslivet implementerar policy och sedan säkerställer att detta efterlevs för att hantera fenomenet. De slutgiltiga forskningsfrågorna utkristalliseras därför i:

Vilka potentiella risker kan associeras med lagring i externa molntjänster?

Varför väljer anställda att lagra yrkesrelaterad data i privata molntjänster före verksamhetens egen lagringstjänst?

1.3 Syfte

Fenomenet analyseras i denna uppsats i syfte att belysa varför anställda väljer att aktivt lagra yrkesrelaterad data i privata molnbaserade lagringstjänster före verksamhetens egen lagringstjänst. Vidare ämnar även forskningsbidraget belysa potentiella risker detta kan utsätta företag för. Bidraget önskar skapa bättre insikt och följaktligen stödja beslutsfattande kring verksamheters framtida förhållningssätt till fenomenet.

1.4 Avgränsningar

Forskningen granskar små och medelstora företag och avgränsas således från stora verksamheter för att bättre passa denna studiens tidsram. Forskningen avgränsas även från att konstatera generella säkerhetsrisker företag utsätts för om fenomenet inte adresseras utan diskuterar endast potentiella säkerhetsrisker. Vidare avgränsas forskningen från att analysera hur företag bör arbeta för att hindra fenomenet från att uppstå.

2 Teoretisk referensram

Detta kapitel syftar till att redogöra för de centrala delarna i ämnet och utgör således grunden för denna studie. Kapitlet inleds med ett avsnitt där teorivalen som gjorts motiveras. Vidare presenteras aspekter om molntjänster och BYOD som arbetssätt för att kunna analysera varför anställda lagrar yrkesrelaterad data i privata molntjänster före verksamhetens lagringstjänst.

2.1 Teorival

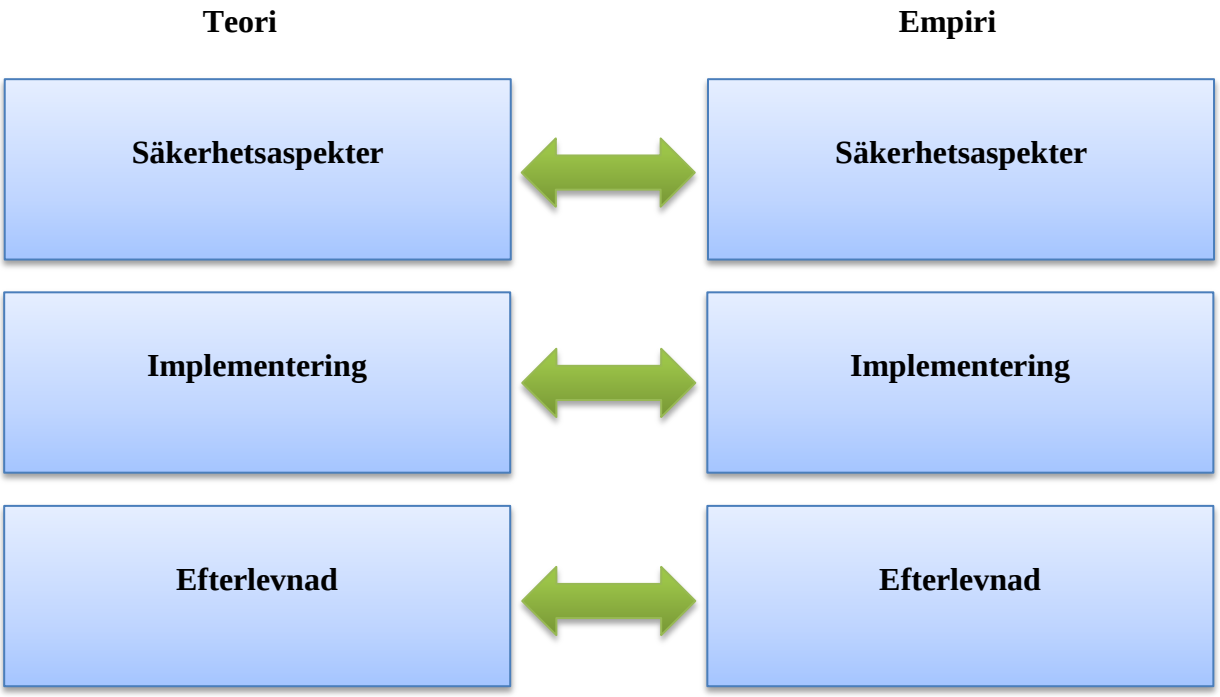
Den teoretiska referensramen är uppdelad i två block som tillsammans redogör för redan publicerad litteratur kring fenomenet för att kunna härleda orsaker av relevans till studiens forskningsfrågor. Då fenomenet förekommer i molnet och hos externa leverantörer avser studien initialt granska molnlagring och dess associerade implikationer för företag där detta arbetssätt förekommer. En arbetsform som innefattar att anställda använder privata molntjänster i yrket identifieras idag som Bring Your Own Cloud (BYOC). Detta är ett aktuellt arbetssätt med enormt inflytande på verksamhetskulturen och anställda (Merrill, 2014) som i skrivande stund endast nyligen börjat utstuderats i litteraturen baserat på vår litteraturgranskning.

Fortsättningsvis beskriver författaren att anställda tidigare använde egenägda enheter i tjänst för ökad produktivitet via smidighet, tillgänglighet och utökade integrationsmöjligheter (Merrill, 2014). Detta arbetssätt har nu flyttats till molnet och kallas BYOC där användaren brukar egna molntjänster i tjänsten för att underlätta arbetet oberoende av enheter och mjukvara menar Merrill (2014) och företaget Dell (2014) som utgör två av flera som identifierat arbetssättet. Då vi anser att tillgängligheten på studier kring BYOC är begränsat ämnar studien se relevanta likheter med BYOD som arbetssätt. Dock kan lagring i privata molntjänster förekomma i verksamheten oberoende av vem som äger enheten som tillgår molntjänsten. Således kommer BYOD som arbetssätt studeras i syfte ett se relevanta likheter till fenomenet utan hänsyn till vem som äger enheten i avseende att bättre kunna besvara forskningsfrågorna.

Vid en första anblick kan frågan om varför anställda lagrar yrkesrelaterad data i externa molntjänster i arbetet förekomma uppenbar. Denna studie önskar att skapa ett mer djupgående svar på forskningsfrågorna genom att granska underliggande orsaker till fenomenet. Ett mer djupgående svar utforskas genom studera fenomenet utifrån tre delmoment; 1) säkerhet, 2) implementering och 3) efterlevnad. Den teoretiska referensramen är indelad i två teoretiska block där modellens delmoment behandlas. Innehållet i den teoretiska referensramen tillsammans med innehållet i den empiriska undersökningen sammanvävs sedan för att se likheter och kontraster för att utvinna ett mer djupgående svar på forskningsfrågorna.

Ingående innebär detta att studien önskar exponera mer djupgående svar till forskningsfrågorna genom att granska verksamheters implementering av policy och strategier för att hantera fenomenet. Har verksamheten etablerade policys för att hantera detta arbetssätt och kan avsaknaden av utformade förhållningsregler vara en anledning till att fenomenet sker? Vad säger teorin om policy för att adressera detta arbetssätt och hur förekommer strategier och policy i näringslivet?

Sista delmomentet som gäller efterlevnad avser kartlägga vad teori anser viktigt för att säkerställa att etablerade policys efterlevs. Policy kontrollerar inte nödvändigtvis fenomenet (Symantec, 2012) utan det kan förekomma obehindrat trots etablerade strategier vilket utgör en av de största säkerhetsriskerna med detta arbetssätt (Miller, Voas, & Hurlburt, 2012). Delmomentet beaktas följaktligen i empirin genom att studera hur verksamheter i näringslivet följer upp etablerade policys. Genom att jämföra teorin med empirin önskar studien exponera underliggande orsaker att angripa för verksamheter som redan har utformade förhållningsregler. Denna modell avser således besvara forskningsfrågorna utifrån anställdas upplevda åsikter men också mer djupgående svar som förankras med verksamhetens strategier för att hantera detta arbetssätt. Den empiriska undersökningen är utformad enligt modellen nedan:



Figur 1 - Modell över teorival och dess koppling till empirin

2.2 Lagring i molnet

Följande kapitel om molntjänster beaktar initialt säkerhetsrisker verksamheten utsätts för då anställda lagrar data i molnet som underbyggs med verkliga exempel hämtade från litteratur och nyhetsartiklar. Vidare granskas tidigare forskning gällande hur verksamheter kan implementera strategier och policy för att minimera identifierade risker. Avslutningsvis studeras undersökningar om hur verksamhetens etablerade strategier efterlevs. Detta upplägg avser forma en helhetsbild för verksamheter vid framtida ställningstagande till detta ständigt växande fenomen som medför signifikanta utmaningar.

Aktuella studier rapporterar ökad användning av molnbaserade applikationer som inte visar något tecken på att minskas (Trustmarque, 2015). I takt med den ökade användningen ökar orosmoment kring säkerhet och dess foglighet. menar företaget Trustmarque (2015). Detta kapitel avser medvetandegöra verksamheter om aktuella säkerhetsrisker genom att skapa en helhetsbild av de orosmoment Trustmarque (2015) hänvisar till. Anställdas tendenser att lagra yrkesrelaterad information i det personliga molnet förekommer inte helt bekymmersfritt för företaget vilket tydliggörs i följande avsnitt.

2.2.1 Säkerhetsrisker med molnlagring

En studie rapporterar att tre av fyra IT-chefer ser säkerhet som största utmaningen när verksamheten flyttar datalagring till molnet (Subashini & Kavitha, 2011). Molnbaserade lagringstjänster kan brytas ut till tre underliggande tjänster eller lager SaaS, PaaS och IaaS. Molnlagringskunder nyttjar alla tre lager i samspel med varandra. Samspelet göms bakom webbläsaren för att reducera komplexiteten för slutanvändaren. De olika tjänsterna utsätts för olika utmaningar vilket mer ingående kartläggs i följande avsnitt för att synliggöra flera av de säkerhetsutmaningarna IT-cheferna refererar till. Avslutningsvis beaktar avsnittet säkerhetsrisker som förefaller samtliga tre tjänster.

Då företag använder externa molntjänster kommer verksamhetsdata skickas och hanteras av leverantören. Speciellt då exponeras data för hackers med uppsåt att stjäla informationen vilket ställer krav på kryptering och säkerhetskonfigurationer i nätverket som då ansvars av leverantören (Subashini & Kavitha, 2011). Verksamheten flyttar ansvaret för mjukvaran och därmed transportsäkerheten av information till leverantören. När informationen väl ska sparas hos leverantörer bör dataintegriteten beaktas, menar författarna. *”Data integrity is one of the most critical elements in any system”* (Subashini & Kavitha, 2011, p. 5). Att bevara integriteten i ett isolerat system uppnås lätt men försvåras snabbt när flera system måste interagera. Mellan leverantören och klienten involveras fler system vilket kompliceras när interaktionen mellan systemen skall fungera samtidigt som tillfredsställande dataintegritet upprätthålls.

En undersökning visar att cirka 70 procent av dataintrång sker utifrån i form av cyberattacker och hackers. Den stora andelen intrång utifrån orsakar samma nivå av skada som resterande andel dataintrång från insidan (Subashini & Kavitha, 2011). Verksamheter ökar således risken för dataintrång utifrån samtidigt som säkerhetsansvaret av dataintrång från insidan flyttas till

leverantören. En skribent för Inforworld argumenterar för att hackare med uppsåt att attackera utifrån angriper användarens kontouppgifter snarare än molntjänsten. Lösenord och hemliga frågor utgör den svaga länken vid användning av molnbaserad IT (Angeles, 2013). Hackaren injicerar skadeprogram som utvinner användarens lösenord till hans/hennes Google Drive där användaren har lagrat verksamhetskänslig data. Således har den omedvetna verksamheten exponerats för datastöld (Samson, 2012b). Skadeprogram som injiceras likt ovan är molnsystemens mest frekventa attack (Younis & Kifayat, 2013). Precis denna risk inträffade då en anställd på Dropbox blev hackad. Den anställda brukade samma svaga lösenord på flera hemsidor som till sin Dropbox. Hackaren lyckades erhålla offrets inloggningsuppgifter från besökta hemsidor vilket således gav tillträde till offrets Dropbox som innehöll email-adresser till Dropbox-kunder, skriver författaren i en annan publikation (Samson, 2012a).

Dataintrång från insidan förekommer mindre frekvent än utifrån men orsakar däremot mer omfattande skada per intrång. Augusti 2012 hackades Vodafones kundregister som exponerade personlig information och bankuppgifter för 2 miljoner kunder. Attacken möjliggjordes med hjälp från insidan likt NSA-läckan som orsakades av Edward Snowden, redogör en skribent (Angeles, 2013).

PaaS avser forma en plattform för kunden att utveckla och husera verksamhetens applikationer på. Detta medför att säkerheten under applikationsnivå såsom nätverk och host ansvarar leverantören för. Till skillnad från SaaS där mjukvaran redan är utvecklad tillsammans med underliggande IaaS och PaaS så erbjuder PaaS en flexibel plattform för kunden att själv utveckla på. Den ökade flexibiliteten kommer till en bekostnad av mindre fullständiga säkerhetsverktyg och säkerhetsförmåga (Subashini & Kavitha, 2011).

Infrastructure as a Service utsätts för olika grader av säkerhetsrisker baserat på vilken molnmodell som levereras. Den huvudsakliga skillnaden mellan den privata och publika infrastrukturen i molnet är att den publika molnleverantören säljer till multipla organisationer, inte bara en. En privat molnleverantör ägnar infrastrukturen unikt åt en organisation och kan således bättre tillgodose organisationens krav på säkerhet och tillgänglighet (Savvas, 2014). Användare som sparar yrkeskänslig information i den privata Dropboxen, Google Drive eller motsvarande använder därmed publik infrastruktur.

Oavsett vilken modell klienten använder så ansvarar leverantören för att reducera eller hindra skadan på den fysiska infrastrukturen som kan orsakas av katastrofer (Subashini & Kavitha, 2011). Hotet från naturkatastrofer eller andra katastrofer varierar geografiskt sätt vilket direkt påverkar risken verksamheten utsätts för när användare lagrar verksamhetenens information i molnet. Utöver nämnda katastrofer så besitter IaaS-lagret fler utmaningar. Molntjänster levereras uteslutande via Internet och ärver därför samma säkerhetsbekymmer (Subashini & Kavitha, 2011). Detta utgör säkerhetsbekymmer som uppstår när data skickas mellan användaren och leverantören oavsett underliggande säkerhetsåtgärder hos respektive part.

Trots att samtliga lager är särskilda kan riskerna ärvas sinsemellan genom deras intima samarbete. Inte helt osannolikt kan en SaaS-leverantör hyra en utvecklingsmiljö av en PaaS-leverantör som slutligen hyr infrastrukturen av en IaaS-leverantör. Var leverantör ansvarar för

säkerheter i den egenägda tjänsten vilket kan skapa inkonsekventa kombinationer av säkerhetsmodeller. Samarbetet mellan olika leverantörer av olika lager skapar förvirring kring vem som bär ansvar vid eventuella problem (Hashizume, Rosado, Fernández-Medina, & Fernandez, 2013).

Molnleverantören sparar företagskänslig data på flera geografiska platser i världen för att erbjuda ökad tillgänglighet och säkerhet till kunden. Detta förekommer inte helt problemfritt alla gånger med lagring utomlands. Flera länder i Europa och södra USA tillåter ej att viss information får lämna landet med hänvisning till lokala lagar om känslig information (Subashini & Kavitha, 2011). The Patriot Act är en av flera lagar som kan försvåra situationen för verksamheten vars anställda sparar i molnbaserade lagringstjänster. *"The Patriot Act allows the US government to demand disclosure of any data stored in any datacenter, anywhere in the world if that system is operated by a US-based company, broadly defined"* (Kushida, Murray, & Zysman, 2011, p. 219). När anställda lagrat data i publika molntjänster så delas leverantörens datautrymme med flera användare. Anställdas data kan då gå förlorad om servers och datacenter innehåller information från andra användare som bestrider The Patriot Act.

Legala ansvar och avgränsningar blir oklara i takt med teknikens oklara avgränsningar. Data finns i molnet och tillgås över hela världen med en internetanslutning vilket väcker frågan om vilken lag som gäller menar verkställande direktör på Rashbaum Associates LCC, en firma specialiserad på lagar rörande elektronisk lagring (Wagreich, 2013). Bara för att en molnleverantör lagrar i Kalifornien behöver det inte betyda att verksamhetens data beaktas endast utifrån Kaliforniens lagar.

Leverantören lagrar dubbletter av kunddata för att erbjuda ökad tillgänglighet och säkerhet till klienten. Detta fungerar som en backup-tjänst vilket avser minska risken att data försvinner eller inte är tillgänglig vid eventuella problem. Känslig företagsdata finns således troligen kvar hos leverantören efter användaren raderat informationen från användarens sida (Younis & Kifayat, 2013). Säkerhetsrisken kan därför leva kvar utan en policy för hur verksamheten arbetar med molnleverantören. Vidare exponeras kundföretaget för risken att obehöriga användare tilldelas behörighet när flera användare delar datautrymme (Younis & Kifayat, 2013). Skribenternas granskning uttrycker fortsättnings oro kring tillgängligheten när molnleverantören lagrar på flera geografiska platser. Molnplattformen Microsofts Azure såg kraftiga försämringar under 22 timmar till följd av problem med nätverksuppgradering. Bandbredden till resterande tillgängliga datacenter överbelastades vilket direkt påverkade tjänstens tillgänglighet och prestanda. Litteraturen hänvisar till flertalet likartade förekomster. MediaMax är en leverantör som erbjuder lagring i molnet som upplevde försämringar likt Microsoft Azure. Under detta tillfälle försökte en kund genomföra ett köp vilket genererade ett systemfel som raderade 45 procent av kundens data (AlZain, Soh, & Pardede, 2013).

Utöver utmaningarna med skiljande regelverk i utlandet kan nya typer av utmaningar frodas utifrån den ökade simplifiering och användarvänlighet som molntjänster erbjuder. Bakom gränssnittet kan leverantören dela data vidare och för att användas som exempelvis

marknadsföring, menar flera skribenter som granskat ämnet (Younis & Kifayat, 2013). Sådan marknadsföring hotar datas integritet vilket således utgör en signifikant säkerhetsbrist. Likt utmaningen med marknadsföringen kan leverantören dölja mjukvarubuggar, bristande hårdvara och attacker utifrån för att reducera egna kostnader (Ren, Wang, & Wang, 2012).

Vidare erbjuder leverantörer som iCloud, Dropbox, Google Drive och Flickr automatiskt säkerhetskopiering. Denna funktion kan kopiera yrkeskänslig data till anställdas personliga moln utan att användaren är medveten. Risken och skadan ökar oerhört när applikationer sammanlänkas. Fler applikationer fungerar exempelvis endast med användarens befintliga inloggningsuppgifter till Facebook vilket försvårar att separera kontona. En digital publikation hänvisar till en användare som länkat sitt personliga Twitterkonto med företagsapplikationen Gizmodo (Baldwin, 2014). Användarens Twitterkonto blev hackat som vidare gav tillgång till verksamhetskänslig data som hanterades av Gizmodo.

Hackeroffret är inte ensam om att besitta äventyrade inloggningsuppgifter. Enligt en omnibus undersökning av 2016 stycken arbetande britter erkänner 15 procent att deras inloggningsuppgifter äventyrats (Trustmarque, 2015). Signifikanta säkerhetsrisker frodas ytterligare då anställda brukar egenägda mobiltelefoner, plattor och datorer i arbetslivet. Då enas och presenteras privat och yrkesrelaterad data i samma enheter och vanligen i samma applikation. Kopplingen mellan privata och yrkesrelaterade applikationer stärks och skillnader suddas ut och göms bakom automatiserade och användarvänliga gränssnitt i molnet.

2.2.2 Implementering av molnlagringsstrategi

För att adressera flera av de säkerhetsriskerna som kartlagdes i föregående avsnitt kan utarbetade strategier och policys hjälpa verksamheten i rätt riktning. Detta kapitel beaktar implikationen av strategier och policys för verksamheten vid lagring i det externa molnet samt vad dessa strategier bör adressera.

Molnet avser presentera komplexa lösningar på ett simpelt och användarvänligt sätt vilket sker på bekostnad av tjänsten transparens. Trots att aktuella molntjänster fungerar bra i vardagligt bruk ägnas få tankar till konsekvenser om problem uppstår. Problem som att molnleverantören kan gå bankrutt, lokala auktoriteter kan konfiskera lagrad data eller data kan utsättas för attacker. Bördan och ansvaret flyttas från verksamheten till molnleverantören vilket komplicerar säkerhetsprocedurer (Rong, Nguyen, & Jaatun, 2013). En välskriven policy om hur verksamheten använder publika molntjänster krävs för att kartlägga riktlinjer för datasäkerhet och dess procedurer. Leverantören och verksamheten som brukar tjänsten bör båda ombesörja säkerheten då ingen riktigt vet vem som står ansvarig alla gånger (Younis & Kifayat, 2013). Författarna argumenterar för att molnleverantörens säkerhetspolicy måste överensstämma med verksamhetens säkerhetspolicy. Verksamhetens interna säkerhetspolicy reglerar tillgängligheten på data i företaget. Dessa säkerhetspolicys bestämmer tillgångar och rättigheter för olika användare i systemet vilket molnleverantören måste återspegla för att upprätthålla företagets interna säkerhetspolicy.

Trots nämnda utmaningar med lagring i molnet har antalet molnanvändare växt med 6 procent senaste halvåret menar Sanjay Beri, VD och grundare av Netskope (Bourne, 2015). Likt kunden ökar anställdas förväntningar på flexibla tjänster och arbetssätt. Nära hälften av anställda väljer att ignorera verksamhetens molnpolicy då det hindrar dem att genomföra jobbet effektivt. Vidare rapporterar 37 procent av intervjuobjekten att de använder icke-auktoriserade applikationer för att kringgå verksamhetens IT-restriktioner (Trustmarque, 2015). Att anställda använder applikationer som inte auktoriserats av organisationen är ingen ovanlighet. Utifrån miljontals användare i Netskope kan företaget påvisa att organisationer använder i genomsnitt 613 olika applikationer varav 90 procent inte är certifierade för företagsmiljö (Bourne, 2015). Den växande trenden av användarens IT-konsumtion i molnet som forskare och IT-ansvariga identifierat liknar framfarten som präglat BYOD-fenomenet. Båda växande trender som väcker frågor kring huruvida företag bör utforma policys för att skydda känslig information utan att motarbeta de anställda.

Litteraturen uppmanar kunden och leverantören att forma ett Service Level Agreement (SLA) innan partnerskapet påbörjas. Precis som människor kräver byggnadskontrakt för att bygga nya hus, förväntas nya bilar komma med garanti. SLA tjänar både som byggnadskontrakt och garanti i molnet. Förändringar och utmaningar angriper från flera fronter som nätverkssäkerhet, lagring, CPU-kraft, databas- och mjukvarutillgänglighet eller via lagstiftningar. Serviceavtalet bestämmer specifika lägstanivåer som krävs för samtliga element i tjänsten (Luis Diaz, 2011). Här finns utrymme för kunden att förhandla villkor med molnleverantören. Detta reducerar risken för att kunden upplever otillfredsställande prestanda och tillgänglighet vilket inträffade kunderna till Microsoft Azure som nämns i tidigare avsnitt

om molnsäkerhet. Avtalet klargör också för påföljande kompensationer om en part inte upprätthåller överenskommelsen.

SLA-avtal erbjuder vanligen garantier kring molntjänstens drifttid men specificerar dåligt gällande datatillgänglighet och dataskydd. Klienten kan förhandla om antalet backup-kopior, var de lagras samt konstatera äganderätt till den lagrade datan. Detta uppmanar en senior analytiker från Enterprise Strategy i en digital artikel (Searchcloudsstorage.techtarget, 2010). Som nämnt tidigare förkommer det oklarheter kring vem som bär ansvar om molnleverantören går bankrutt eller motsvarande. För att kringgå problematiken behöver avtalet husera en klausul som tydligt definierar användarens äganderätt till data (Wagreich, 2013).

Ett sådant avtal hade bringat klarhet om klientens äganderätt trots flera involverade lager och leverantörer som göms i molntjänsten. Fortsättningsvis bör avtalet innefatta avvecklingsstrategier med leverantören. Avvecklingsstrategin besvarar förväntningar kring hanteringen av duplicerad data vid överlämningen till andra leverantörer eller avslut med den nuvarande. Undersökningen Trustmarque lät genomföra visar att 28 procent fortfarande tillgår data från föregående arbetsgivare via mail och molnlagringsapplikationer (Trustmarque, 2015). Tidigare anställda med fortsatt tillgång till känslig verksamhetsdata som e-postadresser och affärskontakter utgör ett stort problem vilket framhåller vikten att en avvecklingsstrategi finns implementerad, menar TeliApps (Schmeiser, 2013). Interna verksamhetspolicy och avtal med molnleverantören bör därför definiera avvecklingsstrategier. Detta rustar verksamheten inför oförutsedda förändringar och försäkrar en lindrigare övergång (Luis Diaz, 2011).

Vidare argumenterar specialister att avtalet bör belysa hur frekvent leverantören säkerhetskopierar data tillsammans med var leverantören geografiska lagrar data. Även om SLA specificerar reglemente och obligationer båda parter måste uppfylla så står avtalet inte över federala lagar. Klienten kan förhandla om geografiskt lämpliga platser utifrån den information verksamheten avser lagra. En strategisk förhandling för att reducera risken att förbundsstatliga lagar kan konfiskera data, exponerar data eller gör data oåtkomligt för verksamheten (Wagreich, 2013). Således kan klienten undvika lagrum likt The Patriot Act som berättigar regeringen att stänga ner data oavsett plats om molnleverantören är baserad i USA. Avtalet bör sträckas längre och hantera eventuella utfall där molnleverantören stäms och verksamheten behöver stå till svars som ägare för den lagrade informationen. Om anställda lagrat känslig information i molnet kan avtalet berättiga verksamheten 10-14 dagar att förbereda svar till domstol om det krävs (Wagreich, 2013).

Det är inte alla molnleverantörer som inkluderar riskförsäkring mot cyberattacker vilket klienten bör hålla i åtanke (Wagreich, 2013). Denna riskförsäkring skyddar mot skador som orsakats av plötsliga nedstängningar och stöld av information. Om molnleverantören inte erbjuder riskförsäkringen kan klienten forma ett eget kontrakt. Företagen kan inte fullständigt skyddas mot cyberattacker oavsett om det är NSA eller statligt ägda organisationer, hävdar en skribent för Thenextweb (Baldwin, 2014). Skribentens uttalande fortsätter att styrkas med aktuella händelser likt dataintrånget på Vodafone och Edward Snowden som läckte NSAs topphemligheter. Utifrån vetskapen kring den bristande säkerheten mot cyberattacker bör

riskförsäkringen ämna reducera risken men framförallt minimera skadan. Handlingsplaner och ansvar bör kartläggas i kontraktet för att minimera attackens inverkan om risken inträffar (Wagreich, 2013).

2.2.3 Efterlevnad av molnlagringsstrategi

Följande avsnitt avser undersöka huruvida säkerhet och relaterad policy efterlevs gällande personligt lagring i molnet utifrån aktuella undersökningar. Detta framförande avser exponera förbättringsområden för verksamheter trots etablerade strategier för att hantera nämnda risker.

Företaget Symantec har genomfört en studie som kartlägger hur anställda i tjänst använder publika molntjänster. Symantecs forskning undersökte 111 anställda tillsammans med 165 IT-chefer för att kartlägga hur anställda följer IT policy som behandlar email, fildelning och lagring/backup. Studien tydliggör avslutningsvis hur anställda handlar utifrån vetskapen om verksamhetens policy (Symantec, 2012). IT-chefernas övervakningsverktyg avslöjar att 81 procent av respondenterna använder publikt molnbaserade lagringstjänster. Symantec argumenterar för att anställda fokuserar på fördelarna molntjänsten erbjuder med ökad produktivitet vilket väger upp för riskerna. Majoriteten av IT-administratörer anser att fördelarna och riskerna verksamheten åtar väger lika (Symantec, 2012).

Likt studien anser flera skribenter att anställa inte är tillräckligt informerade om associerade risker vid IT-konsumtion i molnet. Den bristande informationen är en anledning till att användaren alltid anses vara den svagaste säkerhetslänken (Younis & Kifayat, 2013). En styrkande artikel som publicerats av inforworld.com menar att anställda inte förstår säkerhetsriskerna eller, som studien ovan visar, direkt ignorerar dem. Detta resulterar i svaga lösenord och besök på osäkra hemsidor som installerar skadeprogram på maskinen (Samson, 2012b). Risktagande som äventyrar verksamheten likt exemplet med den anställda på Dropbox eller de 15 procenten som tillkännagav att inloggningsuppgifterna äventyrats.

77 procent av IT-cheferna som deltog i Symantecs undersökning rapporterar att tydliga policy finns utformade gällande lagring i molnet. Nästan hälften av alla anställda rapporterade att de inte kände till någon sådan policy. Trots att majoriteten företag i undersökningen har utformat tydliga policys kring hur anställda skall förhållas mot personlig molnlagring så arbetar hälften utan någon vetskap av förhållningsreglerna. Detta kan ligga till grund för anställdas fokus på molnets möjligheter med effektivisering och flexibilitet i arbetslivet före associerade risker, menar en skribent på Infoworld.com (Samson, 2012b). Nämnda säkerhetsproblem växer i takt med den ökade IT-konsumering i molnet vilket påvisar att problem IT-cheferna identifierat inte kommer försvinna snart. Således bör den identifierade kommunikationssprickan krympas för att reducera verksamhetens risktagande.

Utifrån de anställda som känner till verksamhetens policy mot lagring i molnet erkänner 40 procent att de ändå lagrar i molnet trots tydliga hänvisar till konsekvenser vid regelbrott. Studiens fynd understryker anställdas benägenhet att använda IT i molnet trots definierade konsekvenser.

2.3 Bring Your Own Device

I detta kapitel redogörs för vad tidigare forskning kartlagt om vilka säkerhetsaspekter företag bör ta hänsyn till innan de väljer att implementera BYOD. Fortsättningsvis följer studier som beaktar hur verksamheten bör implementera BYOD så att det sker på ett för företaget säkert sätt. Kapitlet avslutas genom att studera hur företag säkerställer att det implementerade arbetssättet efterlevts. I kort fördelas kapitlet enligt följande fyra punkter:

1. Fördelar och nackdelar med BYOD
2. Säkerhet
3. Implementering
4. Efterlevnad

2.3.1 Fördelar och nackdelar med BYOD

Att låta anställda använda sina privata enheter i tjänsten beskrivs i tidigare forskning som något positivt (Niehaves, Köffer, & Ortbach, 2013). Denna trend benämns som *IT consumerization* och det faktum att det blivit en trend har nu med tiden gjort att företag och organisationer fått upp ögonen för dess associerade säkerhetsrisker. En del hävdar att det har en positiv effekt på den anställdes effektivitet, medan andra hävdar att det kan finnas negativa underliggande effekter som gör att trenden snarare kan få motsatt effekt (Niehaves et al., 2013). Konceptet sägs dels kunna öka anställdas produktivitet då de har relativt lättare åtkomst till företagets interna system. Det sägs även kunna minska företagets kostnader då företaget inte längre behöver budgetera lika mycket för hårdvaruinvesteringar (Lebek, Degirmenci, & Breitner, 2013). I teorin lyfter författarna upp tre av dessa potentiella effekter; 1) ökad arbetsbörda, 2) ökat självstyre och 3) ökad kompetens (Niehaves et al., 2013).

Studien bygger ihop en icke-testad teoretisk modell som redogör för sambandet mellan IT consumerization och den anställdes arbetsprestation (Niehaves et al., 2013). Modellen hävdar att det finns ett klart samband då flera av studiens intervjuobjekt hävdar att de upplevt en ökad stressnivå då de har svårt att skilja på fritid och arbetstid eftersom de hela tiden bär med sig arbetet i fickan. En del av intervjuobjekten hävdar dock motsatsen och menar att det gett dom en ökad grad av flexibilitet;

"Inevitable, I spend a lot of time at 'dead places' where I am not able to do anything except working with my smartphone. By using it, I can start working on open tasks." (Niehaves et al., 2013, p. 47).

Slutligen landar således säkerhetsdiskussionen om BYOD i om det 1)har en övervägande positiv effekt och 2)hur det implementeras på ett säkert sätt.

2.3.2 Säkerhetsrisker med BYOD

Fortsättningsvis beaktas associerade risker med BYOD som arbetssätt i verksamheten. Användningen av privata IT-resurser i arbetet ses i praktiken som en växande trend inom IT consumerization (Schalow, Winkler, Repschlaeger, & Zarnekow, 2013). Forskningen kring denna trend menar författarna är relativt sparsam, men att den forskning som trots allt finns kan kategoriseras in i följande kategorier:

1. Användningen av obehörig personlig media i arbetet
2. Användningen av behörig personlig media i arbetet

Användningen av obehörig personlig media i arbetet adresseras enligt artikelförfattarna i tidigare forskning som *Shadow IT* och/eller *User-driven innovation*. Shadow IT definieras som IT som används i arbetet men vars användande saknar godkännande av IT-avdelningen (Schalow et al., 2013). Den största utmaningen med detta hävdar artikelförfattarna är att få de personliga medierna att matcha gällande säkerhetspolicys, annars riskerar företagen att utsättas för säkerhetsrisker som t.ex. dataintrång.

Den andra kategorin – användningen av behörig personlig media i arbetet – hävdar artikelförfattarna är en ren konsekvens av den första. I och med att organisationer identifierat att anställda vill använda sina privata enheter i arbetet började de arbeta fram policys för att säkerställa att ett sådant arbetssätt går i linje med organisationens ordinarie säkerhetsföreskrifter. För att lyckas implementera detta arbetssätt på ett för företaget säkert sätt menar författarna att organisationer bör applicera något slags mellanliggande säkerhetslager (Schalow et al., 2013). Detta extra säkerhetslager har till uppgift att applicera företagets säkerhetsbarriärer (som t.ex. kryptering) på den privata enheten.

Flera nya trender i informationsåtkomst påverkar organisationers möjlighet att kontrollera och säkra företagskänslig data. Den ständiga ökningen av applikationer innebär att BYOD kan användas på så många olika sätt. Detta beskrivs i tidigare forskning som en säkerhetsrisk då BYOD-användarna i allt större utsträckning erbjuds tillgång till företagskänslig information via en webbläsare på en enhet som inte ägs eller förvaltas av organisationen (Morrow, 2012).

Morrow (2012) presenterar resultatet av en studie där det framgår att 80 procent av de anställda använder någon sorts privat enhet i arbetsrelaterade syften. Studien visade också att 47 procent av de anställda använde deras privata datorer till att lagra företagskänslig data på. 24 procent lagrade samma information på sina smartphones (Morrow, 2012). Oroväckande nog var det inte ens hälften av enheterna som skyddades av företagets säkerhetsbarriärer, vilket Morrow (2012) hävdar är en av anledningarna till att organisationer kommer inse att säkerhetsutmaningarna associerade med BYOD kan väga tyngre än dess uppenbara fördelar.

En av de främsta utmaningarna för organisationer som ger sina anställda möjlighet att använda sina privata enheter i arbetet är att dessa enheter inte hanteras och kontrolleras av företagets IT-avdelning. All företagskänslig data som hämtas via dessa privata enheter skyddas således inte av de säkerhetsbarriär som den normalt sett gör när den hämtas via

företagets enheter (Morrow, 2012). Detta menar artikelförfattaren leder till att företag som tillåter BYOD har mindre kontroll och översyn över informationsflödet.

Det faktum att D:et i BYOD inkluderar mer än bara mobila enheter menar Morrow (2012) ökar säkerhetsriskerna mot företagskänslig data avsevärt eftersom det öppnar dörren för fler inkräktare. För att förebygga dessa menar författaren därför att organisationer bör införa säkerhetskontroller som förebygger dessa risker. Eftersom säkerhetshot så som Keyloggers, Malware och Cyber-attacks lättare kan ta sig in på privata enheter som inte har samma säkerhetskontroller som företagskontrollerade enheter står organisationer inför en rejäl utmaning. Samtidigt som data kan stjälas på detta sätt kan den även stjälas av en anställd. En illvillig anställd kan enkelt stjäla företagskänslig data genom att spara den lokalt eller skicka den till sin privata molntjänst via t.ex. Dropbox. För att säkerställa att detta inte händer hävdar artikelförfattaren att organisationer bör kontrollera data efter att den levererats (Morrow, 2012). Detta arbetssätt kan anses som aningen kontroversiellt då det i praktiken innebär att anställda behöver "skicka bekräftelser" på deras datatrafik.

Lennon (2012) diskuterar den mobila BYOD-trenden och hur de anställdas inställning till IT-säkerhetspolicys bör omvärderas för att matcha de nya mobilitetsmöjligheterna BYOD erbjuder. Denna diskussion bygger på en intervjustudie där författaren intervjuat personal på Letterkenny Institute of Technology där användarna dagligen använder sig av privata mobila enheter i tjänsten.

Intervjustudien syftade till att utvärdera användarens attityd gentemot IT-säkerhet i en miljö där de använder privata enheter samt externa lagringslösningar (vidare benämnt som "BYOD-Cloud"). Studien visade att 68 procent av användarna dagligen använder externa lagringstjänster likt Dropbox för att lagra anteckningar, utvärderingsmaterial samt övrig privat data. Vid en djupintervju visade det sig även att majoriteten av användarna inte visste vilka säkerhetskontroller dessa externa lagringstjänster erbjuder. Användarna antog istället att leverantören stod för säkerheten (Lennon, 2012).

De vanligaste filerna som laddades ner till användarnas enheter är Word, Excel och PDF-filer. Det visade sig dock att en majoritet av användarna även laddade ner .exe-filer, men att endast 47 procent av de tillfrågade använde sig av antivirusprogram (Lennon, 2012). Vidare diskuterar därför Lennon (2012) vikten av att tydligt kommunicera de BYOD-Cloud säkerhetspolicys som existerar så att användarna vet hur de ska förhålla sig till företagets riktlinjer för säkerhet. Detta visas tydligt då befintliga säkerhetspolicys redan existerade, men hela 68 procent av respondenterna var helt ovetande om var de kunde ta del av dessa.

I detta fall hade man alltså misslyckats med att kommunicera sin implementerade BYOD-Cloud säkerhetspolicy. Artikelförfattaren hävdar att de uppenbara effekterna av detta blir att Letterkenny Institute of Technology dagligen utsätts för säkerhetsrisker när anställda brukar sina privata enheter på ett för organisationen ej säkert sätt. Det faktum att 47 procent av respondenterna inte använder antivirusprogram samtidigt som de laddar ner .exe-filer tyder på att de ständigt behöver oroa sig för dataintrång. Lennon (2012) hävdar att detta delvis beror på

att policyn inte kommunicerats ut till de anställda "tillräckligt", samtidigt som han lämnar övriga organisatoriska påverkansfaktorer öppet för tolkning.

Alla dessa säkerhetsaspekter kring BYOD landar i dagens forskning slutligen i en diskussion om det är värt besväret eller ej. I artikeln To BYOD or not to BYOD (Walker-Osborn, Mann, & Mann, 2013) hävdar artikelförfattarna att det är upp till varje organisation som funderar på att implementera ett BYOD-program att noggrant analysera varje säkerhetsaspekt. För att vidare lyckas med en säker implementering av ett BYOD-arbetssätt måste organisationer ta fram säkerhetspolicys som effektivt kommuniceras ut till de anställda så att de efterföljs. Slutligen hävdar artikelförfattarna att organisationer bör ta hjälp av externa säkerhetsexperter som hjälper de implementera BYOD på rätt sätt (Walker-Osborn et al., 2013). Allt för att maximera dess uppenbara fördelar, men även för att minska riskerna det nya arbetssättet medför.

2.3.3 Implementering av BYOD-strategi

När beslutet om att implementera en BYOD-strategi väl fattats i en organisation framgår det i tidigare forskning att en av de främsta framgångsfaktorerna till en lyckad implementering ligger i att få de anställda att börja använda sina egna enheter (Hensema, 2013; Lebek et al., 2013). I litteraturen diskuteras olika potentiella effekter BYOD kan medföra. Här menar de att arbetsbörda ses som en nackdel för de anställda då de tenderar att arbeta utanför ordinarie arbetstider. Vidare hävdar de att den anställdes självstyre ökar då personliga enheter ofta associeras med en högre grad av frihet. Kompetensfaktorn sägs också öka hos den anställde då han/hon är mer bekväm med sin personliga enhet och således kan lösa problem lättare (Hensema, 2013).

I en nyligen publicerad studie (Putri & Hovav, 2014) utvärderas anställdas avsikt att följa organisationens informationssäkerhetspolicy i en BYOD-kontext. Studien belyser motivationsfaktorer och motivationshämmare när anställda använder sina egna enheter i tjänsten. Detta sägs, enligt författarna, vara den första studie som tittar på detta ur ett kontextuellt perspektiv.

Ett exempel på sådan motivationsfaktor är Rogers (1975) Protection Motivation Theory. Denna togs fram i syfte att förstå hur rädslan av att misslyckas med något skall motivera en person till att faktiskt lyckas. I studien (Putri & Hovav, 2014) sägs det att denna teori delvis ökar anställdas foglighet gentemot den implementerade säkerhetspolicyn. Samtidigt menar författarna i samma studie att en upplevd "frihetsförlust" minskar den anställdes avsikt att följa policyn. På ett liknande sätt menar även författarna att den anställdes uppfattning om rättvisa också ökar dennes foglighet gentemot policyn (Putri & Hovav, 2014).

Det framgår även i tidigare forskning att en av de främsta framgångsfaktorerna i implementeringen av BYOD ligger i att skapa en hög grad av acceptans bland de anställda (Lebek et al., 2013). Detta är en förutsättning för att implementeringen skall lyckas då den bygger på den anställdas frivilliga deltagande. Tidigare forskning menar att BYOD ställer nya unika utmaningar på IT-proffs då det omdefinierar förhållandet mellan den anställde och IT-

avdelningen. Som vi konstaterat framgår det i tidigare forskning att de anställdas grad av acceptans inte enbart beror på dess uppfattade fördelar, utan även på dess upplevda farhågor (Lebek et al., 2013). Vägen till en lyckad implementering av BYOD menar tidigare forskning således ligga i att säkerställa att de anställda förstår vilka uppenbara fördelar de själva kommer uppleva med det nya arbetssättet. Samtidigt måste företaget även se till att de anställda inte känner oro för eventuella negativa effekter.

2.3.4 Efterlevnad av BYOD-strategi

När ett företag implementerat ett BYOD-program pekar tidigare forskning på vikten av att säkerställa att det nya implementerade arbetssättet sköts på ett säkert sätt (Miller et al., 2012). Således följer observationer från litteraturen som studerat hur etablerade säkerhetspolicys efterlevs för att blotta förbättringsområden för intresserade verksamheter.

Säkerhetspolicys som inte efterföljs presenteras i tidigare forskning som en av de största riskerna med BYOD, och är därmed även det tyngsta motargumentet mot konceptet (Miller et al., 2012). När privata enheter börjar cirkulera inne på ett företag och anställda börjar använda dessa till att lagra yrkesrelaterad data på uppstår en del säkerhetsproblem som IT-avdelningen aldrig tidigare behövt se till. Tidigare har de trots allt haft full kontroll över alla enheter i nätverket. När ett företag kontrollerar en enhet har de möjlighet att konfigurera den så att den håller den säkerhetsnivå företaget valt att implementera. Detta kan göras genom att t.ex. kryptera enheten och installera programvaror som motverkar virus och skadlig kod, de kan även tvinga användaren att ha enheten lösenordskyddad. Med privata enheter finns inte längre den här möjligheten.

En verksamhet måste därför uppmana användaren att skydda enheten - vilken enligt litteraturen i praktiken kan vara svårt att säkerställa (Miller et al., 2012). Trots att policys tagits fram och satts i bruk för vilka applikationer som är tillåtna på de anställdas personliga enheter så visar en undersökning genomförd av Cisco (Anonymous, 2012) att 69 procent av BYOD-användarna trots detta använde otillåtna applikationer.

Vad säger då litteraturen om hur företag och organisationer bör arbeta för att få det implementerade BYOD-arbetssättet att fungera på ett säkert sätt? Detta kan enligt litteraturen delas upp i två läger, där det ena fokuserar på tekniska aspekter och det andra på "mjuka värden". De mjuka värden som diskuteras i tidigare forskning talar om för organisationer hur de bör gå tillväga för att adressera allt ifrån kulturella skillnader till geografiska aspekter och åldersskillnader. Det görs därför i denna litteraturgenomgång ingen vidare redogörelse för vilka av dessa som är prioriterade, då tidigare forskning inte ger mer klartecken än att företag och organisationer "bör adressera dessa aspekter". Ett exempel på konceptet "hands off" presenteras dock nedan.

Gannett (2012) diskuterar den tekniska aspekten och menar att företag bör implementera tekniska åtgärder som säkerställer att säkerhetsintrång inte kan ske. Detta går i praktiken ut på att man implementerar en rad säkerhetsbarriärer (autentisering, verifiering samt tillgångshantering) som användaren tvingas gå igenom innan han/hon får tillgång till data.

Detta tillvägagångssätt må anses ta lång tid, men det förklaras enligt Gannett (2012) som ett säkert sätt att skydda sin data. Enligt Caldwell (2012) kan en teknisk styrning av en BYOD-implementering delas in i de två kategorierna 1) Hands on eller 2) Hands off. Den första kategorin - Hands on - anser författarna vara en självklar del i implementeringen och innebär i korthet att IT-avdelningen ger sig själv kontroll över BYOD-enheterna genom att implementera MDM (Mobile Device Management).

Mobile Device Management är ett administrationsverktyg som framtagits för att underlätta en verksamhets satsning på mobila enheter, detta genom en rad funktioner som möjliggör allt ifrån konfigurering av inställningar och registrering av nya enheter till att säkerställa att användandet av enheten följer utsatta policys (Sullivan, 2013). Med hjälp av denna tekniska lösning får företag ett kraftfullt verktyg som kan tvinga användarna att följa företagets BYOD-/säkerhetspolicy genom att blocka enheter som inte styrs av MDM. Problemet med vad som är företagets data och vad som är privata data har med MDM lösts genom så kallade remote wipes. Detta innebär att företaget kan tömma enheten på känslig information om så krävs (Caldwell, 2012). Här pekar tidigare forskning (Scarfö, 2012) på den uppenbara nackdelen en "hands on approach" kommer med, eftersom BYOD i mångt och mycket handlar om att låta användarna vara fria att använda sina egna enheter på ett sätt de är vana vid. Scarfö (2012, p. 448) uttrycker det som *"ett företag som vill öka de anställdas produktivitet och reducera kostnader bör tänka på hur villiga användarna är till att ha sin egen enhet med deras privata data på när företaget har så hård kontroll på den som MDM ger"*.

Den andra kategorin - hands off - menar författarna är rena motsatsen till hands on. Detta tillvägagångssätt använder sig av virtuella skrivbord som användaren loggar in på för att på så sätt hålla arbetsrelaterad information inom det virtuella skrivbordet. Det kräver en del omställning av distribution av applikationer men ger i gengäld användaren friheten att använda sin enhet som vanligt och endast bli styrd av företaget när denne begär åtkomst till applikationer och information som tillhör företaget (Caldwell, 2012). Detta anses enligt tidigare forskning (Scarfö, 2012) vara ett effektivt sätt för att separera vad som är privat och vad som är företagsdata - och gör det även svårare för användaren att flytta eller kopiera information till enhetens privata lagringsutrymme.

2.4 Sammanfattning

I ovanstående kapitel har vi redogjort för vad tidigare forskning kartlagt om vilka säkerhetsaspekter företag bör ta hänsyn till innan de väljer att implementera BYOD. Studier som beaktat hur en verksamhet bör implementera BYOD så att det sker på ett för företaget säkert sätt har presenterats. Avsnittet om molntjänster beaktade initialt säkerhetsrisker en verksamhet utsätts för då anställda lagrar data i molnet, vilket underbyggdes med verkliga exempel hämtade från litteratur och nyhetsartiklar. Vidare har även tidigare forskning som granskat hur verksamheter kan implementera strategier och policys för att minimera identifierade risker presenterats. Avslutningsvis i de båda blocken har det presenterats hur verksamheter säkerställer att det implementerade arbetssättet efterlevs. Innehållet i denna teoretiska referensram ligger vidare till grund för den empiriska analysen där vi analyserar varför fenomenet sker, vilket kan användas för verksamheter vid framtida ställningstagande till detta ständigt växande fenomen som medför signifikanta utmaningar.

3 Metod

Följande metodkapitel inleds med en presentation av valet av metodiskt angreppssätt vi applicerat för att besvara forskningsfrågorna. Kapitlet redogör även för hur den teoretiska referensramen framarbetats och hur vi gått tillväga för att samla in den empiriska datan. Vidare redogörs för valet av företag och respondenter i undersökningen. Detta följs av ett avsnitt om analysmetod där vi redogör för hur teorin och empirin ställs i relation till varandra för att besvara forskningsfrågorna. Avslutningsvis återfinns ett avsnitt om kvalitet och metodkritik.

3.1 Insamling av empiri

För att besvara forskningsfrågorna har vi i denna uppsats valt att genomföra intervjuer. Vi har intervjuat sex anställda, tre hos Företag V och tre hos Företag S. Anledningen till att husera relativt öppna intervjuer var för att lättare kunna ta hänsyn till detaljer, nyanser och det unika hos varje intervjuobjekt. Jacobsen et al., (2002) menar att det ofta är mer lämpligt att genomföra en intervjuer när man vill få fram en nyanserad beskrivning av empirin vilket denna studie använder med intentionen att exponera outforskade aspekter. Detta gjordes i intervjuerna genom att ställa öppna frågor som t.ex. *"Hur kommer det sig att du väljer din egen externa lagringstjänst före verksamhetens?"* och *"Kan du vidareutveckla och berätta mera?"*.

Datainsamlingen genomfördes med individuella öppna besöksintervjuer. Öppna intervjuer ämnar reducera potentiella begränsningar på uppgiftslämnaren (Jacobsen, Sandin, & Hellström, 2002) vilket bättre utforskar forskningsfrågorna till skillnad från slutna intervjuer. Vidare riskerar öppna intervjuer att generera väldiga mängder information vilket försvårar en helhetsbild (Jacobsen et al., 2002). Problematiken adresseras i denna studie genom att besöksintervjuerna tilldelades maximalt en timme per person samt att den öppna intervjun strukturerats till en viss grad för att bättre reglera datavolymen och innehållet. Jacobsen et al. (2002) argumenterar för att husera intervjuer mellan en till två timmar för att tillåta djupgående konversationer utan att trötta ut intervjuobjektet. En specifikt avtalad timme för intervju erbjöd vidare ett mjukt avslut med intervjuobjektet vilket annars kan bli problematiskt då personer upplever det trevligt och spännande att ha någon som lyssnar menar författaren (Jacobsen et al., 2002).

De öppna intervjuerna genomfördes med tillhörande intervjuguide för att säkerställa att datainsamlingen ramat in centrala element för att säkerställa en relevant helhetsbild. Guiden fungerade mer likt en checklista med ett fåtal öppna frågor än en specificerad frågelista med ledande svar till följd. Datainsamlingen upprätthåller då fortfarande hög grad av öppenhet samtidigt som enskilda centrala aspekter sätts i fokus (Jacobsen et al., 2002). Intervjuguiden återfinns under kapitel sex och appendix n.

Individuella intervjuer sker antingen över telefon eller ansikte mot ansikte. Intervjuobjekt tenderar att ljuga eller undanhålla sanningen per telefon då detta utgör ett tämligen opersonligt medium (Jacobsen et al., 2002). Besöksintervjuer skapar en högre förtroendefaktor samt att intervjuobjekten tycks ha lättare att prata om känsliga ämnen i person. Vi argumenterade således för att besöksintervjuer lämpar denna studie bättre än telefonintervjuer då forskningsfrågorna undersöker ett potentiellt känsligt ämne för anställda. Intervjuobjekten erbjöds därav också anonymitet vid intervjustarten för att hindra att svaren kan återkopplas till uppgiftslämnaren. Då majoriteten av uppgiftslämnarna önskade anonymitet kommer båda företagen och samtliga personnamn förbli anonyma i denna studie.

Individuella intervjuer beaktar den enskildes inställning, uppfattning och tolkning av fenomenet vilket ger klarhet i hur individen lägger mening i olika förhållande (Jacobsen et al., 2002) vilket tämligen lämpas för att utforska forskningsfrågorna. Fortsättningsvis planerades besöken utifrån intervjuobjektets arbetsplats för att frångå den så kallade *kontexteffekten*. Forskning visar att konstlade omgivningar tenderar att leda till att intervjuobjektet ger konstlade svar (Jacobsen et al., 2002). Intervjuobjekten uppträder ofta annorlunda i ovana eller neutrala miljöer vilket vi adresserade genom att föra intervjuerna på intervjuobjektets arbetsplats.

Slarv vid insamlingen av empirisk data hotar forskningsbidragets trovärdighet (Jacobsen et al., 2002). Skribenten beskriver att de vanligaste felen uppstår vid nedteckning av data och att inspelning under intervjutillfället är alltid att föredra. Att föra anteckningar eller återberätta från minnet kräver avsevärd träning samt utgör en stark sållning av information i insamlingsögonblicket (Jacobsen et al., 2002). Detta försvårar för andra att kontrollera om slutsatserna är riktiga utifrån rådata då forskarna endast filtrerar data som överensstämmer med deras världsbild menar skribenten. För att kringgå nämnd problematik och för att styrka studiens tillförlitlighet så spelades samtliga intervjuer in och transkriberades. Ljudinspelningen och transkriberingen kontrollerades sedan av studiens samtliga författare med avseende att säkerställa rådata och därmed styrka uppsatsens trovärdighet.

3.1.1 Utformning av intervjufrågor

Intervjuprocessen initierades redan innan intervjutillfällena genom att tydligt kommunicera avsikten med intervjun samt forma en översiktsbild. Detta framförande bygger förtroende där tillitsrelationer inte redan etablerats menar Jacobsen et al. (2002). Väl ute på företagen följde korta beskrivningar om oss, vår bakgrund och hur datainsamlingen fortsättningsvis ska användas samt till vilken utsträckning intervjuobjektet önskar vara anonym. Dessa förberedelser gjordes inför alla intervjuer med avseende att förstärka förtroendet under intervjun. Se bilaga 1 för fullständig intervjuguide.

Intervjuer som inleds med alltför precisa frågor riskerar att endast generera svar på det vi anser viktigt vilket vidare gör den öppna intervjumetodiken överflödig (Jacobsen et al., 2002). Därav ställdes genomgående öppna frågor för att fånga intervjuobjektets egna ord och vad de ansåg viktigt. Då intervjuobjekten berörde intressanta ämnen ombads intervjuobjekten vidare utveckla för att bättre förvalta intervjutillfället. Denna form av djupdykning avgör ofta om intervjun ger tillräckligt med information samt berikar intressanta element som önskas utvecklas ytterligare (Jacobsen et al., 2002). Frågorna utforskade intervjuobjektens kännedom gällande:

- Säkerhetsrisker associerade med fenomenet
- Implementerade policys och strategier för att hantera fenomenet
- Hur verksamheten säkerställer att implementerade policys och strategier efterlevs

3.1.2 Urval

Denna undersökning genomfördes med intervjuer med anställda på Företag V och Företag S som har roller både högt och lågt i organisationshierarkin. Syftet med att intervjua anställda i den operativa kärnan och hur de förhåller sig till fenomenet var för att identifiera *varför*, och om de lagrar yrkesrelaterad data i privata molntjänster. Intervjuerna med beslutsfattarna på Företag V och Företag S genomfördes därför i syfte att identifiera underliggande och potentiellt dolda orsaker till varför fenomenet sker inom områdena *säkerhet*, *implementering* och *efterlevnad*. Intervjuerna präglades visserligen av en hög grad av öppenhet, med reservation att vi i förväg i viss utsträckning visste vad vi letade efter.

Jacobsen et al. (2002) beskriver två faser som denna studie applicerat för att göra ett relevant urval av möjliga intervjuobjekt. Initialt behöver den teoretiska populationen fastställas vilket innefattar alla som studien önskat undersöka med obegränsad tid, pengar och analysmöjligheter. Då fenomenet kan utforskas utifrån verksamhetens alla avdelningar och utifrån obegränsat antal perspektiv ämnar denna studie således reducera populationen utifrån följande krav:

1. Anställda som lagrar eller har lagrat yrkesrelaterad data i privata molntjänster
2. Anställda som arbetar på ett företag som erbjuder en egen lagringstjänst
3. Beslutsfattare för verksamhetens strategier och policy gällande fenomenet som brukas av anställda enligt punkt ett och två.

Fortsättningsvis fördelades urvalet till undergrupper. Den första gruppen utgörs av anställda i den operativa kärnan som uppfyller krav ett och två. Den andra gruppen består av beslutsfattande i företagen som ansvarar för policys och strategier rörande verksamhetens förhållningssätt till lagring i det personliga molnet. Datainsamling från beslutsfattare avser kartlägga verksamhetens riskmedvetenhet gällande fenomenet och vidare vilka strategier som implementerats och kommunicerats för att adressera riskerna. Avslutningsvis önskar intervjuerna samla information om hur beslutsfattare säkerställer att nämnda strategier och policys efterlevts.

3.1.3 Företag V och Företag S

Kommande stycke avser forma en bakgrund av studiens respondenter och respektive företag. Studiens respondenter utgörs av sex anställda från de två tekniskt inriktade företagen S och V. Företagen påminner om varandra till storlek och omsättning, men framförallt har de anställda som lagrar yrkesrelaterad data i privata molntjänster. Dock har de två företagen distinkt skilda synsätt på IT-säkerhet gällande molnlagring och BYOD.

Företag S grundades under 1970-talet och beskrivs som ett expansivt It-företag. Företag S arbetar direkt mot slutkund som utgörs primärt av andra företag men underhåller också den privata sektorn till viss utsträckning. Företaget erbjuder kompletta helhetstjänster för kundföretagets hela IT-miljö vilket bl.a. innefattar infrastruktur, datalagring och kommunikation för att nämna några tjänster. S är en ISO-certifierad verksamhet som arbetar utefter näringslivets bästa praxis vilket är en intressant anmärkning då fenomenet likväl förekommer här.

Företag V formades tidigt 2000-tal som likt S är ett blomstrande It-företag som expanderar explosionsartat. Till storleken sett påminner de båda företagen om varandra. S och V har till antalet lika många anställda idag vilket V uppskattas fördubbla inom det kommande året. Organisationen underhåller endast företagskunder som önskar att maximera sin kommunikation och tekniska infrastruktur. Företag V är en relativt ung organisation i förhållande till S och står inför enorma expansioner som inte har etablerat någon IT-strategi eller policy.

3.1.4 Informanterna

Som tidigare nämnt genomfördes samtliga intervjuer i person och på intervjuobjektens respektive arbetsplats. I följande avsnitt kommer informanterna återges utifrån deras roll på företagen för att skapa en mer levande läsning. Nedan följer tabeller med vederbörliga företag för att forma en överblick samt kunna associera intervjumaterialet till respektive informant.

Företag	Informant	Nivå	Datum	Roll	Tid
V	#1	Operativ	2015-04-22	Mjukvaruutvecklare	15 min
V	#2	Operativ	2015-04-22	Interaktionsdesigner	29 min
V	#3	Beslutsfattare	2015-04-22	IT-Chef	30 min
S	#4	Operativ	2015-04-23	Systemtekniker	14 min
S	#5	Operativ	2015-04-23	Serviceansvarig	32 min
S	#6	Beslutsfattare	2015-04-23	Avdelningschef	21 min

Tabell 1 - Intervjuöversikt

Informant #1

Informant ett utgör en av dem som arbetat på företaget längst och arbetar med för nuvarande med utvecklingen av verksamhetens kärnprodukt som mjukvaruutvecklare. Som utvecklare på operativ nivå arbetar informanten mycket med JavaScript och säkerställer att funktionaliteten i produkten fungerar vilket uppgiftslämnaren nu har gjort på företag V i tre år.

Informant #2

Informant två har jobbat på företaget i drygt ett år och är anställd som interaktionsdesigner. Informanten arbetar övervägande med webben men även med applikationer till slutkund där uppgiftslämnaren ansvarar för användarupplevelsen. Informanten jobbar på utvecklingsavdelningen med tjugotalet utvecklare som ensam designer på företaget

Informant #3

Informant tre arbetar på exekutiv nivå och ansvarar för företagets IT-strategier/policy. Informanten ansvarar således för utformning, implementering och efterlevnaden av nämnda strategier vilket inte var genomdrivet vid intervjutillfället.

Informant #4

Informant fyra beskriver en systemtekniker vars arbetssysslor kretsar kring servers, telefoni, teknik och växlar. Informanten fungerar som spindeln i nätet och således arbetar med allt från support, drift och installation av hård- och mjukvara inom nämnda områden.

Informant #5

Informant nummer fem har arbetat på företag S i mer än tio år på operativ nivå och agerar spindel i nätet likt informant fyra fast inom teknisk kundtjänst. Uppgiftslämnaren anser sig besitta stort förtroende från kunder och interna medarbetare. Medarbetare vänder sig ofta till informanten efter rådgivning och problemlösning.

Informant #6

Informant sex arbetar på exekutiv nivå som avdelningschef med flera ansvarsområden. Informanten ansvarar för verksamhetens IT-policy men samtidigt för data-avdelningens resursfördelning, kundkontakt och personalrekrytering. Uppgiftslämnaren har arbetat för företag S i över 21 år.

3.2 Analysmetod

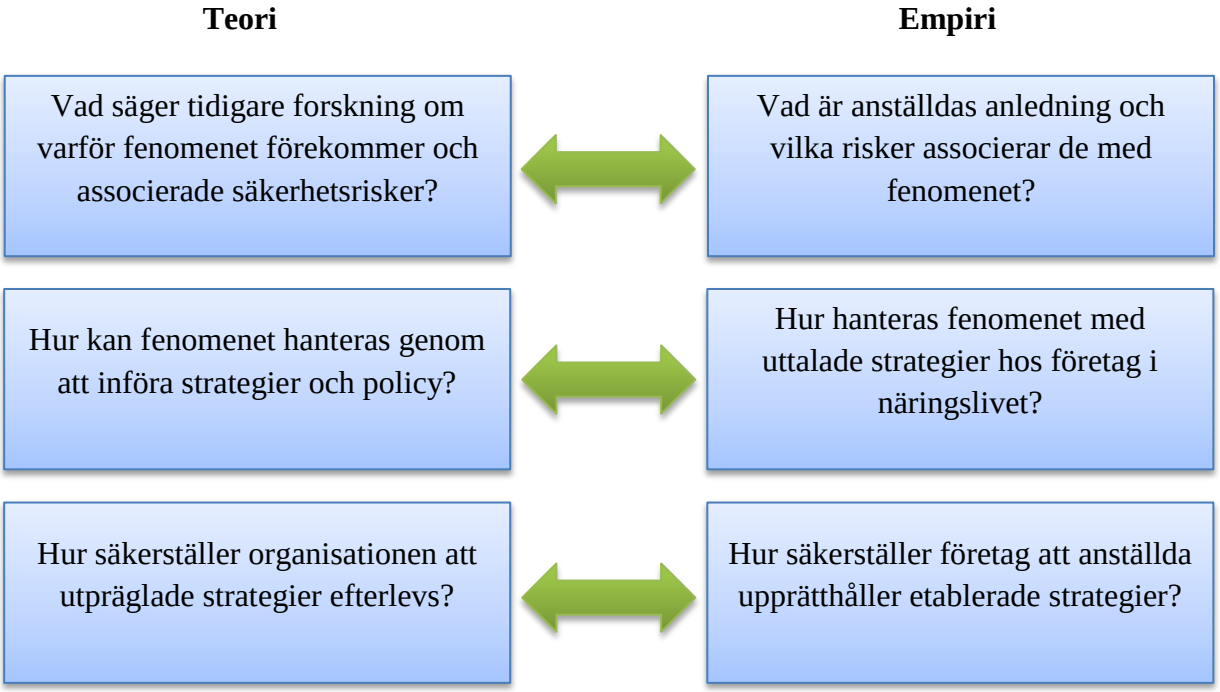
Som nämnt i avsnitt (2.1) ämnar studien undersöka underliggande orsaker till forskningsfrågorna genom att undersöka teorin och empirin utifrån 1) säkerhet, 2) implementering och 3) efterlevnad i relation till fenomenet. Genom att granska forskningsfrågorna utefter den givna modellen kan forskningsfrågorna besvaras utifrån tre delmoment. Att endast se till anställdas åsikter om varför detta arbetssätt förekommer riskerar att ge uppenbara forskningsresultat. Denna analysmetod avser exponera underliggande orsaker till forskningsfrågorna och således göra en djupare förankring vilket förhoppningsvis formar underlag till verksamheter att fatta bättre beslut för att hantera detta arbetssätt. Analysmetoden granskar initialt vad litteraturen identifierat för associerade säkerhetsrisker med fenomenet samt vad anledningen till varför det förekommer.

Detta teoretiska delmoment om säkerhet vävs samman med ett liknande delmoment från empirin som kartlägger anställdas egna svar om vilka påföljande risker detta arbetssätt medför. Fortsättningsvis studeras litteraturen efter hur strategier och policys kan fungera som ett verktyg för att bättre hantera fenomenet. Samma delmoment återfinns i empiravsnittet som undersöker hur verksamheter i näringslivet önskar hantera detta arbetssätt genom etablerade strategier. Det bildas sedan en syntes mellan teori och empiri där vi diskuterar skillnader och slutligen orsaker till att fenomenet förekommer.

För verksamheter som redan har utarbetade förhållningsregler som kommunicerats i verksamheten följer sista delmomentet i teorin som beaktar hur verksamheter säkerställer att nämnda regler efterlevs av anställda. Till följd undersöktes frågan i näringslivet där organisationens beslutsfattare gällande IT-strategier besvarade frågan om hur de säkerställde

att anställda upprätthåller utarbetade strategier. I linje med delmoment ett och två följer en sammanvävning av teori och empiri i delmoment tre för att ytterligare förankra forskningsfrågorna till potentiella orsaker för en rikare analys.

Delmoment ett om säkerhetsrisker ämnar besvara studiens första forskningsfråga genom att exponera potentiella säkerhetsrisker som associeras med lagring i molnet. Delmoment två om implementering tillsammans med delmoment tre om efterlevnad avser besvara studiens andra forskningsfråga om varför fenomenet förekommer.



Figur 2 - Analysmetod

Genom att analysera fenomenet utifrån dessa delprocesser ges en helhetsbild till varför fenomenet sker, snarare än att bara fråga de anställda. På så sätt skildras om det finns några kritiska aspekter som leder till att fenomenet uppstår. Detta ligger sedan till grund för en diskussion om fenomenets potentiella risker.

3.3 Undersökningskvalitet

Oberoende av undersökningsmetod måste undersökningen underkastas en kritisk granskning för att kunna bedöma om dess slutsatser är tillförlitliga eller ej (Jacobsen et al., 2002). Här handlar om att granska undersökningen utifrån ett givet antal kriterier och bedöma dess kvalitet. Detta avsnitt inleds därför med en diskussion kring de källor som använts i bakgrunden och den teoretiska referensramen, för att därefter diskutera kvaliteten av undersökningens insamlade data.

3.3.1 Källkritik

Den teoretiska referensramen i uppsatsen är främst hämtad ur publicerade vetenskapliga artiklar som berör ämnet informatik. I de fall vi använt oss av andra källor såsom vetenskaplig tryckt litteratur, har en granskning av betrodda refererande källor gjorts. Under litteraturgenomgången har vi därför ständigt granskat huruvida källorna kan anses aktuella och tillförlitliga.

Berggren (2008) menar att en första bedömning av källan bör inriktas på om den kan anses legitim eller inte - dvs. om källan är vad den utger sig för att vara. Detta kriterium definieras enligt Berggren (2008) som *yttre kritik*, något som i denna uppsats hanterats genom att till största del använda publicerade artiklar hämtade från kända och betrodda samlingsdatabaser för artiklar såsom mångciterade verk på Google Scholar, AIS Electronic Library (AISeL) eller via länkningsverktyget LU-linker vid Lunds Universitet. I kombination med *yttre kritik* menar Berggren (2008) att det även finns aspekter kopplade till källans innehåll som också måste granskas kritiskt utifrån följande fyra punkter: *tendenskriteriet, samtidskriteriet, realkriteriet* och *beroendekriteriet* (Berggren, 2008; Thurén, 2003).

För att undvika att bli påverkad av en ideologisk övertygelse, politisk ställning eller förvanskning, vilket i efterhand kan vara svårt för läsaren att detektera (Berggren, 2008), har vi i stor utsträckning arbetat med att stärka resonemangen i tidigare forskning med fler än en källa.

Samtidskriteriet staterar att förstahandskällor är att föredra då information i litteratur annars riskerar att vara felaktig eller förvanskad (Berggren, 2008). För att hantera denna problematik utgörs den litteratur och de källor som använts av förstahandskällor. Detta innebär att resonemang från olika undersökningar i första hand är hämtade från sin originalkälla för att säkerställa den tolkning andrahandsförfattare gjort verkligen stämmer.

Vidare hävdar Berggren (2008) att den inre kritiken även behöver analyseras utifrån beroendekriteriet. Detta innebär att en källa som bygger på en annan källas resonemang inte kan styrka källans uppgifter. *”En lögn blir ju inte sann för att den upprepas av många olika uppgiftslämnare”* (Berggren, 2008). Detta motverkas i denna uppsats då det går hand i hand med resonemanget om samtidskriteriet, dvs. det faktum att samtliga resonemang bygger på originalkällan.

Realkriteriet handlar om att de källor som används måste kritiskt granskas efter vilket årtal de publicerades (Berggren, 2008). Detta är extra viktigt inom informatik eftersom den tekniska utvecklingen starkt kan påverka en källas relevans. Denna problematik har hanterats genom att värdera årtalet på källan utifrån den information som inhämtats samt om tidsaspekten gett informationen rimlig relevans.

3.3.2 Validitet och reliabilitet

Validet påvisar huruvida sannolikt det är att forskningens slutsatser hänger ihop med forskningens undersökning. Forskningsbidragets validitet beaktas utifrån intern och extern validitet (Jacobsen et al., 2002) vilket denna studie hanterat till viss mån. Författaren argumenterar för att den interna validiteten kan styrkas genom att konfrontera enskilda personer med centrala rön och slutsatser från undersökningen. Således konfronterades uppgiftslämnaren efter centrala påståenden för att säkerställa att intervjuobjektet känner igen sig utifrån vår egenbildade uppfattning. Därav minskas sannolikheten att materialet förvrängs vilket slutligen kan influera resultatet. För att kritiskt undersöka att källorna besitter den riktiga informationen bedöms därför källans närhet till fenomenet. Jacobsen et al. (2002) menar att informationen från uppgiftslämnaren kan färgas och förvridas i högre grad ju längre bort intervjuobjektet kommer från fenomenet. Denna studie samlade data endast utifrån förstahandskällor, dvs. individer som refererar till händelser de själva upplevt eller varit med om vilket ökar trovärdigheten att intervjuobjekten avger den riktiga informationen menar Jacobsen et al. (2002). Fortsättningsvis argumenterar författaren för att denna inre validitet inte kan garantera att informationen är riktig utan endast värdera källans förmåga att ge riktig information.

Den externa validiteten beskriver till vilken grad studiens iakttagelser kan generaliseras Det är svårt att generalisera antydanden på en större population som grundas utifrån ett fåtal stickprov (Jacobsen et al., 2002). Antalet stickprov i studien utgörs endast av en handfull enheter för att kunna gå på djupet vilket således blir icke representativt för populationen. Den externa validiteten kan styrkas något genom att argumentera för frekvent återkommande synpunkter utifrån oberoende enheter menar Jacobsen et al. (2002). Skribenten poängterar avslutningsvis att sådan argumentation endast ökar sannolikheten för att synpunkten kan generaliseras men kan aldrig bevisas.

Avslutningsvis upplyser Jacobsen et al. (2002) att extern validering kan styrkas genom kontroll mot sakkunniga eller mot annan teori och empiri. Giltigheten kan då beprövas vid jämförelse av de egna slutsatserna mot andra undersökare och undersökningar. Denna studie besitter samstämmighet med två aktuella studier som beaktat fenomenet utifrån ett exceptionellt mycket större urval. De beaktade studierna har genomförts av företagen Symantec och Trustmarque vars resultat återspeglas i denna forskning. Detta argumenterar för att giltighet stärks ytterligare även om jämförande studier använt andra metoder (Jacobsen et al., 2002). Denna jämförelse ökar studiens validitet men bekräftar därav inte att detta forskningsresultat är sant, menar Jacobsen et al. (2002).

Reliabilitet ser till hur tillförlitliga resultaten är genom att kritisera undersökningsmetoden (Jacobsen et al., 2002). Skribenten menar att studiens tillvägagångssätt kan påverka resultatet vilket sker i någon utsträckning genom alla slags undersökningar då de undersökta utsätts för stimuli och signaler från undersökaren. Intervjuobjektet påverkas av intervjuarens kroppsspråk, klädstil och utseende vilket kallas för intervjuareffekten (Jacobsen et al., 2002). Denna effekt adresserades bitvis genom att efterfråga företagens klädkod inför besöksintervjuerna i syfte att minska en slagsida på studiens intervjudata.

Svaren från intervjuerna kan påverkas om intervjuerna var planerade eller överraskade (Jacobsen et al., 2002). En överraskande intervjumetodik lämpas bäst när studien önskar samla spontana åsikter och känslor för att undvika planlagda synpunkter vilket hade varit intressant att genomföra då studiens forskningsfråga kan vara känslig att besvara. För att inte förekomma besvärliga och bryta in i uppgiftslämnarens privatliv, så planerades besöken i god tid innan. En uppgiftslämnare efterfrågade studiens intervjuguide inför besöket med avsikt att förbereda svaren. Uppgiftslämnaren erhöll inga direkta frågor förutom forskningsfrågorna men informerades om att intervjun vidare kommer beakta säkerhet, implementering och efterlevnad i relation till forskningsfrågorna. Det finns inget klart svar på hur olika kontexter påverkar intervjun menarJacobsen et al. (2002) men detta framförande gjordes med intentionen att skapa en trygg intervjumiljö för att kunna besvara potentiellt känsliga frågor utan att erbjuda förutsättningen för fullständigt planlagda svar.

3.4 Metodkritik

Denscombe (2009) hävdar att det är av största vikt att undersökningen är fullständig i det avseende att samtliga uppgifter som är relevanta för forskningsfrågan måste tas med i undersökningen. I intervjuguiden bygger därför frågorna på den teori som presenteras i den teoretiska referensramen, vilket innebär att det kan finnas påverkansfaktorer till fenomenet som eventuellt inte tagits upp i intervjuerna. Denna problematik anses vara delvis hanterad då insamlingen av data skedde genom semistrukturerade intervjuer vilket gav intervjuobjekten möjlighet att delvis själva styra intervjuerna i olika riktningar. En ren konsekvens av detta blir därför att även analysmetoden kan kritiseras eftersom den inte nödvändigtvis tar hänsyn till samtliga påverkansfaktorer kring varför fenomenet sker.

4 Empirisk analys

I detta avsnitt presenteras och analyseras den data som samlats in. Att teori och empiri redovisas och analyseras i samma avsnitt beror på en önskan om att skapa ett bättre flöde i texten men också för att undvika upprepningar. Avsnittet är strukturerat utifrån de delmoment som presenterats i analysmetoden och avslutas med en sammanfattande analys av fenomenets orsaker.

4.1 Säkerhetsrisker

Det första steget i den empiriska analysen analyserar varför de anställda, enligt de själva, väljer att aktivt lagra yrkesrelaterad data i privata molntjänster. Detta görs genom att vi inledningsvis presenterar informanternas egna reflektioner kring fenomenet och dess säkerhetsrisker. Trots att de flesta verkar införstådda med att de utsätter företagen för säkerhetsrisker när de lagrar yrkesrelaterad data i privata molntjänster gör de det ändå. Analysen fortsätter därför med ett avsnitt där vi presenterar hur de arbetar i praktiken, något som sedan för oss in på ett avsnitt där BYOD:s inverkan på fenomenet diskuteras. Vidare analyseras om det finns några säkerhetspolicys för hur anställda skall förhålla sig till externa lagringsmöjligheter, samt vilka potentiella risker som kan kopplas till avsaknaden av en fullt fungerande sådan.

4.1.1 De anställdas egna reflektioner kring fenomenets säkerhetsrisker

I samtliga intervjuer gavs de anställda möjlighet att själva reflektera över vilka säkerhetsrisker företaget utsätts för när antingen de själva eller någon annan i organisationen lagrar yrkesrelaterad data i privata molntjänster. Den gemensamma nämnaren bland informanterna som arbetar på operativ nivå var att de alla var medvetna om att de utsätter företaget för någon sorts risk. Mjukvaruutvecklaren säger t.ex:

> "Företag V är ett så pass litet företag så än så länge tror jag inte att det är några problem. Men när ett företag blir större och större så tänker man att det blir ett större problem." (Mjukvaruutvecklaren, rad 84).

Med detta förtydligar han senare att han menar att det skulle vara svårare att hitta "läckan", dvs. personen som lagrade yrkesrelaterad data i sin privata molntjänst. Fokus låg här med i att konstatera att ju större företaget är - desto större risk. När Interaktionsdesignern ges tillfälle att själv reflektera, poängterar han istället hur smidigt det är att ständigt ha tillgång till allt snarare än att reflektera kring fenomenets säkerhetsrisker.

> "[...]men det är otroligt smidigt att vi har gått över till att alla kör samma molnlösning. Det innebär att jag har en mapp på företaget som alla har tillgång till om de vill kolla på

> designrelaterade grejer. Det är otroligt smidigt på det sättet. Det var bökigt tidigare när inte alla körde Drive tidigare och delade med sig saker t.ex. dokument. Det var väldigt komplext och meckigt.” (Interaktionsdesignern, rad 55)

När Systemteknikern får ordet uttrycker han en oro att man inte vet vem som tittar på data som lagras på t.ex. Dropbox.

> “Ja, alltså jag kan väl känna så att man vet ju inte vem som tittar på data som ligger på Dropbox och Microsoft. Det ligger ju på deras servers och vi vet ju inte vad de gör med den.” (Systemteknikern, rad 98)

> “[...]jag tycker bara att det är olustigt att de har möjligheten att gå in och se data.” (Systemteknikern, rad 102)

Den andra informanten på Företag S – Serviceansvarig – hävdar att han själv inte lagrar yrkesrelaterad data i någon privat molntjänst (Serviceansvarig, rad 10). När han får reflektera fritt kring fenomenet diskuteras det främst vad som skulle kunna hända om den yrkesrelaterade data hamnade i fel händer och hur det skulle kunna skada företagets varumärke. När han får en följdfråga på varför någon anställd skulle kunna tänkas förbise företagets säkerhetspolicys svarar han kort *“Jag kan tänka mig att folk använder detta för att det är så enkelt.”* (Serviceansvarig, rad 82). Trots detta vill han påstå att företaget erbjuder så pass bra lagringsmöjligheter att han har svårt att se att det skulle finnas incitament till att frångå etablerade policys.

> ”I: Så om jag har förstått dig rätt så är de två största riskerna som du ser är att känslig information kan läcka och företags varumärke tar stryk av det?
> O: Ja det är ju bara det spontant nu. Företag S vi står för att vi ska vara professionella och säkerheten är a och o, det ska inte komma i fel händer. ” (Serviceansvarig, rad 47-48).

> “Ja, men om någon gör så här så känner jag väl mer eller mindre att den arbetaren inte tar sitt ansvar. Vi har fullt med lagringsmöjligheter här, dem tycker jag ska nyttjas.” (Serviceansvarig, rad 44).

På det stora hela framgår det i intervjuerna att det finns en grad av riskmedvetenhet hos de intervjuobjekt som arbetar i den operativa kärnan. I intervjuerna med IT-chefen och Avdelningschefen, som båda är beslutsfattare, framgår det dock att riskerna med att lagra yrkesrelaterad data i privata molntjänster upplevs som större orosmoment. Det framgår i teorin att de inte är ensamma om detta orosmoment då vi tidigare konstaterat i avsnitt (2.2.1) att tre av fyra IT-chefer ser säkerhet som största utmaningen med datalagring i molnet. En intressant infallsvinkel är att det framgår i intervjuerna att beslutsfattarnas riskmedvetenhet tenderar att vara relativt högre än hos de operativa informanterna. Hos Företag S är de oroliga för att någon obehörig skall få tillgång till data som är av direkt värde för företaget (som t.ex. kundregister), något som i sin tur potentiellt skulle kunna skada verksamhetens varumärke då de själva erbjuder lagringstjänster.

> “Man sparar ju kund-ägd data och använder det på ett privat sätt som då åsidosätter vårt säkerhetstänkande mot kunden, vårt avtal mot kunden, som gör att det sedan kan användas

> på ett felaktigt sätt. Kunden måste kunna lita på att den information vi tillhandahåller, det som tillhör kunden, stannar här hos oss.” (Avdelningschefen, rad 8).

Den gemensamma nämnaren i intervjuerna med de båda beslutsfattarna är att de båda uttrycker oro för hur fenomenet skulle kunna skada deras verksamheter om t.ex. en anställd slutar hos något av företagen. Avdelningschefen på Företag V spekulerar i att en säljare enkelt skulle kunna ta med sig information till nästa företag och använda denna i konkurrenssyfte.

> “Det är ju alltid risker med om säljare slutar och tar med sig information som gör att de kan konkurrera eller ta med kunder till andra företag.” (Avdelningschef, rad 14).

Mjukvaruutvecklaren och Interaktionsdesignern från Företag V framhäver smidighet och att fenomenet inte är ett stort problem i dagsläget, medan Serviceansvarig är införstådd med dess associerade säkerhetsrisker och därför inte alls lagrar yrkesrelaterad data i någon privat molntjänst. Vi ser dock att Systemteknikern även han lagrar i sin privata molntjänst, trots att han uttrycker oro för att data eventuellt kan hamna i fel händer. Hur kommer det sig då att han ändå lagrar i sin privata molntjänst?

4.1.2 Fenomenet i praktiken

När fenomenet studerades i praktiken visade det sig att 75 procent av de intervjuade operativa anställda lagrade yrkesrelaterad data i deras privata molntjänster före verksamhetens uttalade lagringstjänst. Intervjuerna åskådliggör en stor spridning i användandet hos de intervjuade individerna och förekommer generellt i mindre utsträckning hos Företag S än på Företag V. Serviceansvarig kan tolkas som tämligen riskmedveten då han flera gånger i intervjun påstår vilka säkerhetsrisker som kan associeras med fenomenet, och att han därför aldrig lagrat i någon privat molntjänst i anställningen.

> ”Inte en enda megabyte, antingen har jag ett USB minne med mig om jag skulle behöva ta någon information ifrån min laptop som jag har hemma, vilket är min jourdata. Jourdatorn och USB-minnet är båda ägda av företaget, jag har därifrån tagit två VPN- cert med mig från företaget till hemmet för att sedan radera det i hela mitt liv. Aldrig molntjänster.” (Serviceansvarig, rad 10).

I citatet nedan berättar respondenten att han gör privata ärenden i webbläsaren, på vad uppgiftslämnaren anser vara seriösa sidor. Även utifrån antagandet att användarens besökta sidor är betrodda väcks orostankar kring webbläsarens och hemsidornas säkerhet då respondenten tillgår företagets server via en VPN-tunnel. I linje med litteraturen med hänvisning till avsnitt (2.3.4) förkommer denna tekniska VPN-lösning som en föredömlig skyddsåtgärd för att motarbeta säkerhetsintrång. VPN-tunneln fungerar likt en god säkerhetsbarriär men anses ta lång tid. Som beaktat i avsnitt (2.2.1) om gemensamma säkerhetsutmaningar i molnet riktas angrepp utifrån vanligen till användaren och inte molntjänsten. Troligen angriper hackare alltså respondentens inloggningsuppgifter via besökta webbsidor och således potentiellt exponerar den yrkesrelaterade data som uppgiftslämnaren tillgår via jourdatorn.

> "Ja du kan surfa på den datorn. Den surfgrejen jag gör på den, om det är så att folk har problem med att man är ute och surfar exempelvis på blocket, aftonbladet eller någon seriös sida, jag går aldrig in på någon oseriösare sida. Det är en ren dator, det finns ingenting på den. Den används enbart till att arbetas på, jag har min andra dator till att gå in på mer oseriösa sidor. Jag skiljer helt och hållet på företaget och på mig själv." (Serviceansvarig, rad 16).

I kontrast till ovanstående respondent så lagrar Mjukvaruutvecklaren, Interaktionsdesignern och Systemteknikern yrkesrelaterad data direkt i privata molntjänster. Nämnda respondenter resonerar likt Mjukvaruutvecklaren som argumenterar för att den privata lagringen förekommer men inte i någon stor utsträckning (Mjukvaruutvecklaren, rad 10).

> "Jag kan säga direkt att jag gör det inte så mycket just nu. Jag gjorde det mycket tidigare, då använde jag Google-lösning" (Interaktionsdesignern, rad 2).

> "Jag tycker, jag gör inte det ofta, de gånger de har hänt så har jag gjort det för att jag har en laptop och står typ i en källare och jag ska bara ta en backup på en växel." (Systemteknikern, rad 16).

Mjukvaruutvecklaren som arbetar som utvecklare på Företag V förklarar att samtliga utvecklare använder Github som är inbäddat i deras arbetssätt. Uppgiftslämnaren menar att Github är kodares version av molntjänst (Mjukvaruutvecklaren, rad 70-80) och således inte behöver andra molntjänster i samma utsträckning längre. Interaktionsdesignern som använder en Google-lösning enligt ovan vidareutvecklar att han endast använder privata molntjänster i arbetet via mobiltelefonen (Interaktionsdesignern, rad 44). Till följd uppger intervjuobjektet att han arbetar hemifrån på den privatägda datorn och sköter samtliga arbetsrelaterade ärenden via webbläsaren.

Respondenterna som lagrar yrkesrelaterad data privat använder en rad olika molntjänster. Interaktionsdesignern använde Google Drive vid intervjutillfället för att spara skisser via mobiltelefon och dator. Likt Interaktionsdesignern lagrar Systemteknikern i externa lagringsmedium. När Systemteknikern arbetar ute hos kund använder han vanligen Microsofts molntjänst, OneDrive, för att lagra samt synkronisera inställningar och konfigurationer som är specifika för kundens IT-lösning (Systemteknikern, rad 16-30). Mjukvaruutvecklaren använder också utomstående molntjänster likt föregående respondenter men lagrar data på en egenägd server hemma hos informanten.

> "Jag använder något som heter AeroFS som är ganska likt Dropbox fast att man hostar servern själv hemma så får man så mycket plats man vill och gratis." (Mjukvaruutvecklaren, rad 16).

Mjukvaruutvecklaren använder en molntjänst som tillåter användaren att lagra data på en privatägd server i hemmet. Respondenten kringgår mycket av det risktagande som associeras med det publika molnet som diskuteras i avsnitt (2.2.1) men ansvarar samtidigt för datasäkerheten själv. IT-ansvariga med god riskmedvetenhet hade troligen ifrågasatt huruvida respondentens egenägda server och infrastruktur i hemmet upprätthåller en önskvärd säkerhetsnivå enligt värdföretaget och hur lyder avtalet mellan respondenten och AeroFS?

Två riskmedvetna frågeställningar som snabbt hade blottat associerade säkerhetsrisker med intrång, exponering via marknadsföring och legala ansvar som alla beaktas i avsnitt (2.2.1). Fortsättningsvis berättar informanten att han huvudsakligen lagrar programinställningar för terminaler, kom-ihåg-listor och information om olika projekt han varit involverad i (Mjukvaruutvecklaren, rad 22-28). Informanten frambringar att han förut lagrade känsligare information i molnet utan att vidareutveckla vad informationen gällde.

Hur kommer det sig då att anställda lagrar yrkesrelaterad data privat enligt dem själva? Det råder samstämmighet gällande flera aspekter mellan informanterna när studiens centrala forskningsfråga besvarades. Samtliga respondenter som privat lagrar yrkesrelaterad data hävdar att värdföretaget inte erbjuder en bra motsvarande lösning. Systemteknikern beskriver utmaningar med verksamhetens motsvarighet vilket vidare besvarar frågan om varför:

> "[...]backuptjänsten som körs varje dag klockan nio, tar den backup. Men det är ju inte så att jag kan logga in med ett konto och ha en mapp där jag lägger grejer och bara synka det på ett par minuter för att sedan hämta upp det på en annan. [...] Ja, vi har ju typ en backup tjänst men det är ju ingen synktjänst på så sätt såsom Dropbox eller OneDrive." (Systemteknikern, rad 86).

Systemteknikern som jobbat ute på kundens arbetsplats och behöver synkronisera data på plats för att senare tillgå samma data från andra enheter och platser. Företag S erbjuder en intern backup-tjänst som säkerhetskopierar var morgon klockan nio och kan nås utifrån via dator med specificerad VPN-tunnel vilket uppgiftslämnaren anser vara omständigt och tidskrävande. Uppgiftslämnaren saknar en omedelbar synkroniseringsfunktion som erbjuds av Dropbox eller OneDrive. I linje med Systemteknikern beskriver båda respondenterna från Företag V att organisationen inte erbjuder något bra lösningsförslag för deras behov.

> "Nej vi hade inga bra lösningar såsom jag upplevde det då för att spara saker i molnet och inte lokalt på datorn. [...] Jag behöver ju det, det är ju väldigt tråkigt om en disk kraschar, och man inte får tillbaka all data. Så det är ju ett sätt att säkra sitt arbete." (Interaktionsdesignern, rad 16).

Skiljt från övriga respondenter återkommer Interaktionsdesignern till den upplevda säkerheten med externa molntjänster. Genom att använda Google Drive så berättar uppgiftslämnaren att arbetet säkerhetskopieras vilket är viktigt för uppgiftslämnaren men också för verksamheten vid överlämning till andra anställda. Respondenten ser fördelar med att lagra data i molnet istället för utspritt över flera lokala enheter. Utöver den upplevda säkerheten beskriver informanten en ökad tillgänglighet och smidigheten som underlättar det dagliga arbetet, något som verkar vara den återkommande anledningen till varför intervjuobjekten lagrar yrkesrelaterad data i privata molntjänster. Fördelarna med ökad tillgänglighet och smidighet påträffas i samtliga intervjuer. Mjukvaruutvecklaren och Interaktionsdesignern från Företag V jobbar ibland hemifrån och nedan beskriver Interaktionsdesignern hur det externa molnet underlättar hans arbete.

> "Det är en stor fördel med att använda Drive, om inte företaget skulle ha Drive, och man jobbar som jag exempelvis där man jobbar med APPAR och tar fram mockups, illustrerade skärmbilder. Då är det otroligt smidigt att slänga in de i en Drive mapp ta ut dem och se det

> som ett interface där. Det är även smidigt att kunna plocka upp det hemma om man inte kände att man blev klar på jobbet, eller att göra något på kvällen sen när man kom hem. Det fyller ju även funktionen att komma åt material på andra enheter.(Interaktionsdesignern, rad 20)

> "[...] Smidigt. Hemifrån så finns det ju inget alternativ, jag skulle ju kunna be om att få låna en laptop härifrån men det känns otroligt stökigt. Bara för att kolla mailen eller någon fil på Google Drive." (Interaktionsdesignern, rad 46)

Utöver nämnda fördelar berättar Interaktionsdesignern att arbetet kan lätt demonstreras och delas till flera användare i företaget för snabbare feedback. Respondenten menar att tillgängligheten förkortar hans arbetsprocesser avsevärt då andra användare kan granska skisserna direkt i molnet utan att respondenten behöver skicka filer via Outlook eller motsvarande.

Samtliga användare argumenterar för fördelar om smidighet för att underlätta det dagliga arbetet då värdföretaget inte erbjuder en egen lagringstjänst eller att lagringstjänsten som erbjuds kräver flertalet tidskrävande moment. Tidskrävande moment som de anställa effektiviserar genom att använda externa molntjänster vilket förkortar ledtider och reducerar flaskhalsar i arbetet. Utöver smidigheten önskar samtliga respondenter en ökad tillgänglighet. Genom att spara arbetet i molntjänsten kan arbetet återupptas senare oberoende av plats och enhet vilket är värdeskapande för anställda som jobbar vidare hemifrån eller utanför kontoret. Systemteknikern och Interaktionsdesignern beskriver vikten av att kunna spara arbetet på en enhet för att senare fortsätta arbetet på andra oberoende enheter. Systemteknikern som arbetar som systemtekniker behöver spara kundens systemkonfigurationer på plats för att vidare fortsätta arbetet på en annan dator på företaget (Systemteknikern, rad 16). Slutligen upplever en av respondenterna en ökad säkerhet i arbetet då data säkerhetskopieras i molnet och behöver således inte oroas för att data går förlorad vid en hårddiskkrasch (Interaktionsdesignern, rad 15-18).

Användarna identifierar främst fördelar som molntjänsterna erbjuder för att underlätta deras eget arbete vilket är en sanning baserad på intervjuobjektens åsikter. Användarnas åsikter formar en uppskattad sanning som delvis fungerar som svar till studiens forskningsfråga. Vi argumenterar dock för att detta endast utgör ena sidan av myntet till varför fenomenet sker och kan bättre begripas genom att studera fenomenet mer djupgående.

4.1.3 Bring Your Own Cloud

Efter att ha konstaterat att tre av informanterna aktivt lagrar yrkesrelaterad data i privata molntjänster ställde vi följdfrågan om de har tillgång till samma data på deras privatägda enheter. Det visar sig att Mjukvaruutvecklaren använder en firmatelefon som inte har tillgång till molntjänsten, men att han har tillgång till data på sin privata dator i hemmet. När han blev tillfrågan om han har tillgång till molntjänsten på telefonen svarar han *"Nej, bara på datorn där hemma"* (Mjukvaruutvecklaren, rad 44).

När Interaktionsdesignern får samma fråga framgår det att han har tillgång till molntjänsterna han lagrar yrkesrelaterad data i från både sin privata mobil och dator. En synnerligen intressant detalj är att det tydligen är få anställda hos Företag V som har en mobiltelefon som ägs av företaget. *"[...]det är få personer här som springer runt med en telefon som ägs av företaget"* (Interaktionsdesignern, rad 36). När vi frågade informanterna varför de lagrar yrkesrelaterad data i sina privata molntjänster framgick det att en av de främsta anledningarna var möjligheten till tillgänglighet. Något som i detta fall visar hur BYOD som koncept möjliggör fenomenet.

> "Nej min egen dator använder jag väl inte riktigt. Eller jo, det kan jag ju göra såvida om jag ska kolla på interface. Ja, jag använder min privata dator och telefon i tjänsten såvida att jag testar med den ibland. Jag håller grejer på Drive. Kollar på grejer i Drive gör jag även på min privata dator, men jag är rätt så bra på att inte arbeta hemifrån dock. Jag försöker att inte ta med mig jobbet hem." (Interaktionsdesignern, rad 44).

I kontrast till informanterna på Företag V visar det sig att samtliga informanter hos Företag S endast använder verktyg i tjänsten som ägs av företaget. Både mobiltelefoner och datorer. När vi däremot frågar Systemteknikern om han har någon privat molntjänst installerad på dessa visar det sig att han kör Dropbox på mobiltelefonen och Microsoft OneDrive på datorn. Den yrkesrelaterade data han kan tillgå privat är däremot bara den som ligger på OneDrive. Som påvisat i avsnitt (2.1) påvisar även detta hur trenden med BYOC påverkar informantens arbetssätt.

> "[...]på telefonen har jag Dropbox och på laptopen OneDrive. Men Dropboxen på mobilen använder jag enbart privat till bilder och på OneDriven på laptopen det är där jag lägger backup-filerna." (Systemteknikern, rad 76).

Som tidigare diskuterat framgår det i intervjuerna att de båda beslutsfattarna har en relativt högre grad av riskmedvetenhet än de operativt anställda informanterna. Det framgår dock i intervjun med Serviceansvarig att även han vill tro att han arbetar på ett för företaget säkert sätt. När han blir tillfrågad om han använder någon privat enhet i tjänsten, alternativt någon privat molntjänst, förklarar han hur han aktivt arbetat med att se till att detta inte sker.

> "[...]Det finns inget som synkas eller används. Det är till och med så pass att jag har gått in och avaktiverat de så att de inte går igång, jag har stoppat tjänsterna överhuvudtaget. Jag vill inte ha något som ligger latent i bakgrunden och som kan ta och sno information, sen finns det ingen information på telefonen eller på plattan som skulle kunna vara utan det är precis en uppkoppling till våra servers." (Serviceansvarig, rad 68).

4.1.4 Företagens lagringstjänst

En gemensam nämnare hos informanterna som väljer att lagra yrkesrelaterad data i privata molntjänster hävdar alla att det är tack vare dess tillgänglighet. Frågan är då - är företagens lagringstjänst så pass otillgänglig, och kan detta vara en av anledningarna till att fenomenet sker? Mjukvaruutvecklaren, som till vardags arbetar som kodare, lagrar all sin kod i GitHub. Som tidigare nämnt är det inte koden som tillgås hemifrån, utan endast inställningar och

diverse listor. En av anledningarna till att han lagrar dessa inställningar och listor i sin privata molntjänst kan därför vara att det inte finns någon lagringsmöjlighet i det verktyget som han annars arbetar i till vardags.

När vi frågar Interaktionsdesignern vad företaget erbjuder för lagringstjänst framgår det att de i dagsläget kör Google Drive. Detta visar sig dock vara ett relativt nyligen officiellt uttalat arbetssätt. Han berättar att innan företaget implementerade detta lagrade nästan alla i sin privata Google Drive, och att man sedan delade dokument och mappar med varandra (IT-chefen, rad 49-56). I intervjun med IT-chefen framgår det att det i framtiden kommer implementeras tydliga säkerhetspolicys för hur de anställda skall arbeta med detta, men att det idag finns oskrivna riktlinjer som anställda ändå bör anamma. Detta var Interaktionsdesignern dock helt ovetande om.

> "Ja innan hade vi ju ingen officiell Google koppling. De som då behövde en bra lösning körde dom ändå." (Interaktionsdesignern, rad 53).

Hos Företag S ser dock situationen lite annorlunda ut. I intervjun med Serviceansvarig berättar han att företaget har egna lagringsservers och att han egentligen inte har någon information som han behöver lagra. I princip allt han arbetar med är i realtid, vilket han hävdar är en anledning till att han inte behöver lagra något. Det som faktiskt behöver lagras läggs direkt på företagets server som han i sin tur kan tillgå från sin jourdator (Serviceansvarig, rad 73-74). Trots företagets bra lagringsmöjligheter väljer dock Systemteknikern att aktivt lagra yrkesrelaterad data i sin privata molntjänst.

4.1.5 Policys

En av de mest intressanta observationerna under intervjuerna med de informanter på Företag V som lagrar yrkesrelaterad data i sin privata molntjänst är att de båda saknar någon som helst medvetande om det finns säkerhetspolicys för deras arbetssätt eller ej. När Interaktionsdesignern tillfrågas detta svarar han:

> "Nej vad jag vet så finns det inte det. Jag kan inte minnas att jag har läst någon sådan grej, så jag tror inte att vi har någon policy för detta." (Interaktionsdesignern, rad 38).

Även Systemteknikern erkänner att han inte riktigt har koll på hur företagets säkerhetspolicy kring detta ser ut.

> "Jag ska vara ärlig och säga att jag kan ju inte den innantill och utantill. Det var länge sedan jag läste den så jag vet inte, men jag skulle gissa att det står någon rad om detta men det är inget jag har reflekterat över." (Systemteknikern, rad 48).

Serviceansvarig som istället inte alls lagrar yrkesrelaterad data i någon privat molntjänst hävdar dock att det finns tydliga regler och policys som självklart skall följas (Serviceansvarig, rad 48).

När vi intervjuar beslutsfattaren hos Företag V framgår det att han faktiskt i dagsläget arbetar med att utforma en säkerhetspolicy för hur anställda skall förhålla sig till privata molntjänster. Den är dock under utformning och är alltså inte vara implementerad i verksamheten ännu. Han menar att policyn kommer reglera så att alla dokument och allt som tillhör företaget ska ligga inom deras egen molntjänst, men att det kommer vara svårt att styra om anställda får tillgå denna från privata enheter. Här framgår en del av hans oro att anställda enkelt kan tillgå företagets data från privata enheter, trots att de implementerat en policy för att företagets data ska ligga i en av företaget kontrollerad miljö. En anställd kan t.ex. enkelt logga in på företagets Google Drive på sin privata dator i hemmet och kopiera filer. Helt utan företagets vetskap.

> "Vi kommer väl att tillrätta oss efter i den form som jag tidigare beskrev i frågan. Att vi har en policy att vi ska ha våra dokument allt som tillhör vårt företag ska ligga inom våra cloudtjänster. I vår lagringstjänst inte på extern lagringstjänst som inte drivs av företaget har överblick över. Privatinloggning kommer säkerligen att förekomma, det är väldigt svårt att styra att de inte får logga in privat just i webbläsare och så vidare." (IT-chefen, rad 26).

I intervjun med Avdelningschefen påstår han att alla anställda får signera en policy som säger att de inte får använda någon privat molntjänst i arbetet. Policyn reglerar tydligt att allt skall ligga på företagets server.

> "Det står ju att informationen som vi kommer i kontakt med ska stanna här, att vi har tystnadsplikt. Att vi förvaltar och vårdar den informationen som rör sig inom bygget, mellan kund och kontakt med oss. Vi har lagringsutrymme för varje användare på våra servers. Det är där vi ska spara information som då rör arbete och tekniskt utövande. När det berör IT-avdelningen så sparas allt på en gemensam låst databas där rättigheter finns ställda vem som får använda vad och vart saker ska sparas." (Avdelningschefen, rad 24).

4.1.6 Reflektion kring potentiella säkerhetsrisker

I avsnitt (2.2.1) diskuteras säkerhetsutmaningar associerade med användningen av molntjänster i arbetet. I och med att Mjukvaruutvecklaren, Interaktionsdesignern och Systemteknikern alla använder molntjänster i arbetet utsätter de potentiellt respektive företag för dessa säkerhetsrisker. Eftersom de tillgår yrkesrelaterad data via molntjänster på privatägda enheter ligger de utanför företagets skyddsbarriär. Detta innebär i teorin att de har betydligt mindre skydd mot hackare som eventuellt vill komma åt deras data. Allt detta sker utan att Företag V och S kan motverka riskbilden. En av de största utmaningarna med fenomenet blir således att motverka att den yrkesrelaterade datan hamnar i fel händer.

Att den yrkesrelaterade datan skulle hamna i fel händer behöver nödvändigtvis inte bero på att en hackare tagit sig in och stulit data. Det framgår i avsnitt (2.2.1) att molntjänster så som Google Drive automatiskt gör data tillgänglig så fort användaren är inloggad. Låt oss säga att Interaktionsdesignern loggar in på sin molntjänst på en enhet som han sedan lånar ut till en familjemedlem. Familjemedlemmen kan då i sin tur vara försumbar och dela med sig av innehållet utan att veta om konsekvenserna. Att anställda brukar egenägda mobiltelefoner, plattor och datorer i arbetslivet innebär att den privata och yrkesrelaterade datan lätt

presenteras i samma applikation. Gränsen mellan vad som är privat och vad som är yrkesrelaterat tenderar därför att suddas ut.

Det diskuteras i avsnitt (2.2.1) om gemensamma utmaningar med lagring i molntjänster. Det framgår där att molnleverantörer ofta backar upp kunddata för att erbjuda ökad tillgänglighet och säkerhet till sina kunder. Det är därför troligt att data finns kvar hos molnleverantören efter användaren raderat informationen från användarens sida. Även detta kan potentiellt utsätta Företag V och S för säkerhetsrisker eftersom nämnda informanter lagrar företagens data i privata molntjänster.

I intervjun med Mjukvaruutvecklaren har vi tidigare konstaterat att han enbart använder en firmatelefon i tjänsten och att han inte har någon molntjänst som han lagrar yrkesrelaterad data installerad på denna. Istället loggar han in på molntjänsten på sin privata dator i hemmet. I avsnitt (2.3.1) diskuteras fördelar och nackdelar med BYOD som arbetssätt, något som ofta beskrivs som något positivt. En av de främsta fördelarna som diskuteras är just tillgängligheten BYOD medför. Vidare diskuteras det i avsnitt (2.3.2) om säkerhetsaspekter associerade med BYOD, bland annat diskuteras utmaningar med användningen av obehörig personlig media arbetet (dvs. IT som används i arbetet men vars användande saknar godkännande av IT-avdelningen). Att få de personliga medierna att matcha gällande säkerhetspolicys beskrivs som en utmaning som, om den inte adresseras, riskerar att utsätta företaget för potentiella dataintrång. I fallet med både Mjukvaruutvecklaren och Interaktionsdesignern saknar deras användande av privata molntjänster (som brukas på deras privatägda enheter) godkännande av IT-avdelningen hos respektive företag. Vilket helt i linje med de resonemang som förs i teorin om detta potentiellt utsätter företagen för dataintrång.

I kontrast till Mjukvaruutvecklaren och Interaktionsdesignern tillgår Systemteknikern sin privata molntjänst på en enhet som kontrolleras av företaget. Enheten ligger således inom företagets skyddsbarriärer vilket innebär att han inte utsätter företaget för lika direkta risker som Mjukvaruutvecklaren och Interaktionsdesignern. Det diskuteras dock i avsnitt (2.3.2) att BYOD potentiellt kan vara mer än bara smartphones och att dess associerade säkerhetsrisker därför kan vara lika påtagliga om en anställd lagrar yrkesrelaterad data i en privat molntjänst. Oavsett om det är på en företagskontrollerad enhet eller inte. I en relativt nyligen publicerad studie som diskuteras i samma avsnitt innebär detta att organisationer troligen kommer inse att säkerhetsutmaningarna associerade med BYOD kan komma att väga tyngre än dess uppenbara fördelar. Vad skulle t.ex. hända om Systemteknikern loggade in på sin privata molntjänst på en offentlig dator, för att sedan inse att han blivit hackad och hackaren injicerat data i molntjänsten som den vägen tar sig innanför företagets skyddsbarriärer?

Vidare diskuteras det i avsnitt (2.3.2) om vikten av att företag bör ha säkerhetspolicys på plats som reglerar hur användarna bör förhålla sig till användningen av molntjänster. Det läggs även vikt vid att dessa policys bör omvärderas för att matcha de nya mobilitetsmöjligheterna BYOD erbjuder. Det framgår i en studie som presenteras i samma avsnitt att hela 68 procent av användarna dagligen använder externa lagringstjänster likt Dropbox för att lagra privat data. Ungefär samma siffra som informanterna på operativ nivå som lagrar yrkesrelaterad data i privata molntjänster. I studien framgår det att användarna inte visste vilka

säkerhetskontroller dessa externa lagringstjänster erbjuder, de antog istället att leverantören stod för säkerheten. I intervjuerna med informanterna fann vi att majoriteten av de operativa anställda inte hade någon som helst aning om att det ens fanns en säkerhetspolicy, än mindre hur de skulle förhålla sig till lagring i molnet. Risken med att inte ha en tydligt formulerad och kommunicerad policy på plats blir därför hos Företag V och S att deras anställda som lagrar yrkesrelaterad data i privata molntjänster fortsätter utsätta företagen för risken att deras data potentiellt hamnar i fel händer.

Arbetet med att identifiera och bedöma eventuella risker associerade med fenomenet måste rymmas inom för företaget rimliga ramar. När informanterna lagrar yrkesrelaterad data på t.ex. Google Drive finns det såklart en liten sannolikhet att Googles datalagringscenter skulle kunna utsättas för en naturkatastrof. Vilket i sin tur skulle kunna leda till att den anställdas yrkesrelaterade data skulle gå förlorad. Sannolikheten för detta må vara försumbar, men det är än dock en del av riskanalysen.

Slutligen diskuteras det i avsnitt (2.3.2) om det är värt risken att implementera BYOD eller inte. Det framgår att det är upp till varje organisation att noggrant analysera varje säkerhetsaspekt innan de tillåter anställda lagra data i privata molntjänster eller inte. Det framgår i samma avsnitt att detta i en perfekt värld endast skulle fungera på ett för företaget säkert sätt om företaget arbetar fram en säkerhetspolicy kring detta som till 100 procent efterlevs. Konsten att implementera en policy som efterlevs till 100 procent skulle dock visa sig i teorin vara lättare sagt än gjort.

4.2 Implementering

När vi i intervjuerna frågade de operativa informanterna på vilket sätt deras verksamheter implementerat IT-säkerhetspolicys framgick det hos Företag V att detta inte alls skett. Mjukvaruutvecklaren berättar att det finns en policy, men att de anställda på utvecklingsavdelningen inte bryr sig om den. De anser sig vara tillräckligt kompetenta för att veta vad som är säkert och inte (Mjukvaruutvecklaren, rad 51-58).

Interaktionsdesignern är dock helt övertygad om att, om det nu finns en policy, den inte alls kommunicerats ut till de anställda. Han berättar istället att det finns en tillbakalutad icke uttalad policy om hur detta bör skötas, men att det var öppet accepterat att anställda använde sin privata Google Drive i tjänsten.

> "Vi kör ganska layed back. Det är väldigt öppet att folk körde Drive, det var inget hemlighetsmakeri." (Interaktionsdesignern, rad 42).

I avsnitt (2.2.2) diskuteras vikten av att implementera strategier och policys i en verksamhet när de bestämt sig för att använda molntjänster i arbetet. I samma avsnitt lyfts det även fram vad dessa strategier och policys bör adressera. Det framgår bland annat att för att detta arbetssätt skall fungera på ett för företaget säkert sätt bör molnleverantörens säkerhetspolicy överensstämma med verksamhetens säkerhetspolicy. Syftet med detta, enligt teorin, är för att upprätthålla företagets interna säkerhetspolicy. Det framgår även i samma avsnitt att nära hälften av alla anställda väljer att aktivt ignorera verksamhetens molnpolicy då det hindrar dem att genomföra sina arbetsuppgifter effektivt. Avsnittet visar även resultatet från en studie som rapporterar att 37 procent av respondenterna använder icke-auktoriserade applikationer för att kringgå verksamhetens IT-restriktioner. Hittills i intervjustadiet levde vi med uppfattningen att Företag V inte hade någon särskild implementerad säkerhetspolicy och att de därför, i linje med vad som framgår i avsnitt (2.2.1), potentiellt utsatte företaget för risker. När vi sedan får tillfälle att lyssna på företagets IT-chef - IT-chefen – visar det sig att de i dagsläget arbetar med att ta fram en policy för hur anställda skall förhålla sig till molntjänster. Denna är dock inte implementerad än.

> "[...] Ja vi håller precis på att upprätta den här så det finns faktiskt inte i dagsläget så att de anställda kan läsa sig till vad som gäller egentligen." (IT-chefen, rad 24).

Längre fram i intervjuprocessen frågar vi om de har någon klar strategi för att implementera den nya säkerhetspolicyn. Det enda vi får till svars då är *"[...]ja bra fråga. Vi har inte riktigt kommit så långt. Vi kommer definitivt att gå ut på intranätet att vi har kommit med en ny policy och att alla ska läsa igenom den."* (IT-chefen, rad 38). I avsnitt (2.3.3) framgår det att en av de främsta framgångsfaktorerna för att implementera ett nytt arbetssätt, i detta fall användandet av BYOD och molntjänster, ligger i att skapa en hög grad av acceptans av den implementerade säkerhetspolicyn. Med detta i åtanke kan vi konstatera att en av orsakerna till att både Mjukvaruutvecklaren och Interaktionsdesignern aktivt väljer att lagra yrkesrelaterad data i privata molntjänster beror på att Företag V inte har någon implementerad säkerhetspolicy de kan acceptera och arbeta efter.

När vi besöker Företag S får vi en helt annan bild om varför fenomenet sker hos dom. I intervjun med Systemteknikern berättar han att det finns en policy för hur de ska förhålla sig till molntjänster samt att den finns att tillgå på intranätet. Han verkar dock osäker och påstår att han kanske borde kolla upp detta.

> "Ja jag tror det men jag vet ju inte som sagt. Det kanske jag borde kolla upp."
> "Hur får du den här informationen?"
> "Den finns på intranätet. Det är väl typ det.
> "Så gå dit om du vill veta, typ?"
> "Ja faktiskt." (Systemteknikern, rad 50-54).

Serviceansvarig däremot, som är helt övertygad om att han arbetar på ett för företaget säkert sätt, ger en hel utläggning om vad som står i policyn och var de kan tillgås. Han berättar att policyn finns på intranätet och att varje nyanställd bör vara bekant med vad som står där.

> "Anställda har fått introducerat när de kommer hit att här har vi ett intranät, bekanta sig med det och här har du all information som du behöver veta. Samt även att det är så att vi har en hel del säkerhetsgrejer installerade på våra datorer som gör att vi inte kan installera alla möjliga program eller så att säga. Vi har som sagt en strikt företagspolicy som finns på intranätet och om du vill ha vidare information så är det bara att vända sig till våra IT-tekniker som du också kan få detta förklarat för dig." (Serviceansvarig, rad 52).

Det framgår alltså att Företag S har en uttalad säkerhetspolicy för hur anställda skall förhålla sig till molntjänster samt att denna enkelt kan tillgås på företagets intranät. När vi intervjuar IT-chefen på Företag S berättar han även att varje anställd får signera i början av anställningen att de läst och förstått innehållet i denna policy. De har dessutom årliga möten och genomgångar av alla policys och regler som gäller. De har även ett introduktionsmöte för alla nyanställda där de går igenom ovan nämnda punkter (Avdelningschefen, rad 35-42).

Svaret på frågan om varför Systemteknikern aktivt väljer att lagra yrkesrelaterad data i sin privata molntjänst beror alltså inte på att det inte finns några säkerhetspolicys hos Företag S. Svaret kan istället utläsas i avsnittet nedan där vi analyserar hur Företag S istället arbetar för att säkerställa att dessa policys faktiskt efterlevs.

4.3 Efterlevnad

Slutligen analyseras företags tillvägagångssätt för att säkerställa att de implementerade strategierna efterlevs. Frågan var primärt riktad till IT-chefen och Avdelningsansvarig som ansvarar för företagens respektive IT-strategi och policy. Avdelningschefen är på Företag S argumenterar för att efterlevnaden är svårkontrollerad om anställda har intentionen att lagra i privata molnet (Avdelningschefen, rad 43-52). Informanten menar att tillfälliga lagringar som inte genomgår verksamhetens regelbundna backups blir svåra att spåra. Företag S uträttar regelbundna backups på användarnas klienter i systemet vilket erbjuder möjligheten till att observera datatrafiken. Avdelningschefen förtäljer att trafiken aktivt bevakas men kan inte vidare ingående besvara vad för typ av beteende som kan identifieras.

> "Jag kan inte svara eller jag vet inte riktigt hur det fungerar helt tekniskt, där har jag människor som är intresserade och tillägnade för att bara utföra detta arbete. Men vi kan se väldigt mycket." (Avdelningschefen, rad 48).

Till följd uppger informanten att inga aktiva handlingar uträttas för att studera detta fenomen. Baserat på informella diskussioner utanför intervjun berättar avdelningschefen om vikten kring att anställa rätt människor till företaget. Chefen rekryterar riskmedvetna människor med *sunt förnuft* och en personkemi som fungerar bra med de redan etablerade medarbetarna och arbetsrutinerna.

Just avsaknaden av uppföljningen av implanterade strategier och policys utgör en av de största riskerna som associeras med BYOD med hänvisning till avsnitt (2.3.4). Företaget förlorar således kontrollen över hur enheterna och tjänsterna används vilket betyder att företaget inte längre kan säkerställa den säkerhetsnivå som etablerats i verksamhetens IT-säkerhetspolicy. Precis detta uppenbarar sig på Företag S som trots etablerade strategier och policy för hur enheter och tjänster skall användas i tjänsten, har anställda som aktivt lagrar i privata molntjänster. Systemteknikern som jobbar på Företag S uppger att det troligen finns etablerade policys för hur anställda skall hantera egenägda enheter och externa tjänster i yrket

> "Jag ska vara ärlig och säga att jag kan ju inte den innantill och utantill. Det var länge sedan jag läste den så jag vet inte, men jag skulle gissa att det står någon rad om detta men det är inget jag har reflekterat över." (Systemteknikern, rad 48)

Informanten är som påvisat inte ensam om att förbise verksamhetens policy om lagring i molnet med hänvisning till avsnitt (2.2.3). Avsnittet påpekar att 40 procent ändå lagrar i molnet trots tydliga hänvisar till konsekvenser vid regelbrott. Som beaktat tidigare är Interaktionsdesignern ovetande om att Företag V har en etablerad IT-säkerhetspolicy gällande detta arbetssätt, vilket företaget inte har, men väljer likt Systemteknikern att ignorera eventuella förpliktelser för att underlätta det egna arbetet. Systemteknikern berättar att verksamhetens IT-säkerhetspolicy återfinns på företagets intranät om anställda är intresserade men inga stickprov förekommer för att säkerställa att anställda följer dem (Systemteknikern, rad 50-58). IT-chefen som ansvarar för Företag S IT-säkerhetspolicy medger att ingen implementeringsplan finns utformad men överväger att publicera framtida policy och strategier på intranätet likt Företag S. Problematiken återupprepas ytterligare i litteraturen

med hänvisning till avsnitt (2.3.4) som påvisar att 69 procent använder otillåtna applikationer trots uppmaningar från verksamheten. Bevisligen säkerställer detta tillvägagångssätt inte att policyn efterlevs.

Under intervjutillfället med beslutsfattaren på Företag V som idag inte implementerat någon IT-säkerhetspolicy gällande lagring i externa molntjänster identifierades en god riskmedvetenhet. IT-chefen ansvarar för verksamhetens IT-säkerhetspolicy och diskuterar hur företagets framtida IT-säkerhetspolicy kan följas upp för att säkerställa efterlevnaden i Företag V.

> "Allting är beroende på vilken policy vi tittar på. I policyn kommer det till exempel att stå att ditt lösenord ska innehålla x antal karaktärer och innehålla olika former versaler och tecken och så vidare, att det ska löpa ut efter ett visst antal dagar och att du får testa ett antal gånger innan det låser sig. Detta kan ju kontrolleras genom att du inte kan byta till samma. De här formerna av policys är ju ganska lätta att de inte behöver kontrolleras på sådant vis utan de sköter ju sig själva. Däremot som jag pratade om upphovsrättsmaterial som filmer och musik det förekommer ju att man inte får lov att installera program på datorerna. Det sköts scanning på dator för att kontrollera efter en gemensam lista på tillåtna installerade program och avvikelser därtill." (IT-chefen, rad 40).

Informanten hävdar att efterlevnaden inte säkerställs om verksamheten inte är restriktiv i tillgången. Respondenten syftar till restriktioner som reglerar tillgången på viss data i företaget eller restriktioner som förhindrar att anställda inte själv kan ladda ner program på exempelvis, datorn. Beslutsfattaren menar att även detta blir exceptionellt svårt med hänvisning till stora företag som infört extremt komplexa lösningar för att bevara dokument innanför företagets väggar vilket straffar arbetsprocessen (IT-chefen, rad 39-48).

> "Ja det hämnar jobbet extremt mycket som sagt var. [...] Ja även om man gör restriktiv till att inte ge tillgång utanför våra IP ranger så att säga, så har du fortfarande en kameramobil med dig och kan ta ett kort på skärmen. Det är jätte svårt." (IT-chefen, rad 46)

Uppgiftslämnaren hävdar att organisationer måste balansera säkerhet med tillgänglighet. Säkerhetsaspekterna kan inte fullständigt ignoreras till fördel av ökad tillgänglighet då det kan skada företaget mer än vad man tror.

> "Det vore ju en underbar värld om vi levde utan problem, men så är inte fallet. Till en viss grad behöver man ha frihet men till en viss grad så behövs säkerhet och det måste finnas båda två och mötas. Det får inte bli för svår jobbat men det får inte släppas för långt från verkligheten. Så att vems om helst från utsidan kan se insidan, då kan det snabbt gå fel." (IT-chefen, rad 48)

Båda beslutsfattarna argumenterar för en gråzon i arbetet som lägger tillit till anställda vilket erbjuder många av de fördelar som förknippas med arbetssätten. I avsnitt (2.3.4) emfaseras vikten av att säkerställa att ett nytt implementerat arbetssätt sköts på ett för företaget säkert sätt. I det här fallet innebär det att företagen annars riskerar att fullständigt tappa kontrollen över de anställdas användande av externa lagringstjänster. Anställdas vilja att ignorera eller aktivt förbise verksamhetens policys för en ökad produktivitet, smidighet och tillgänglighet

blottas tydligt vid jämförelse av empirin och teorin med hänvisning till avsnitt (2.2.3). Utifrån samma teoretiska avsnitt och med anknytning till detta avslöjade Symantecs studie att 81 procent av anställda lagrar i externa molntjänster vilket endast 38 procent bekänner. De operativa informanterna bekräftar fler risker med detta arbetssätt men riskerna övervägs av de anställdas upplevda fördelar. Till följd av informationen ovan och i linje med beslutsfattarna konstateras svårigheterna för verksamheten att fullständigt kontrollera att implementerade säkerhetspolicy efterlevs. Intressanta diskussioner kan således istället föras om huruvida verksamheter kan stödja dessa arbetssätt istället för att motverka dem utan att fullständigt överge säkerheten.

4.4 Sammanfattande analys

I följande avsnitt sammanfattas de kärnargument som diskuterats i analysen och bygger tillsammans svaret på studiens forskningsfrågor.

4.4.1 Den operativa kärnan har ordet

När fenomenet studerades i praktiken visade det sig att tre av de fyra intervjuade operativa anställda lagrade yrkesrelaterad data i deras privata molntjänster. Hur kommer det sig då att dessa aktivt väljer att lagra yrkesrelaterad data i privata molntjänster? Det råder samstämmighet gällande flera aspekter mellan informanterna när studiens centrala forskningsfråga besvaras. De hävdar nämligen att de arbetar på detta sätt för att respektive företag inte erbjuder en tillräckligt bra motsvarande lösning. Systemteknikern behöver t.ex. synkronisera data direkt ute hos kund, men företagets VPN-lösning synkroniserar bara en gång per dygn. Detta upplever han som en omständigt och tidskrävande lagringsmöjlighet. Mjukvaruutvecklaren och Interaktionsdesignern beskriver att Företag V inte heller erbjuder en tillfredställande lösning. Kärnan i de anställdas incitament till att lagra yrkesrelaterad data i deras privata molntjänster beror på de privata molntjänsternas relativa tillgänglighet och smidighet i förhållande till företagets lagringstjänst. Det påvisas även vilken inverkan BYOD har på fenomenet då både Mjukvaruutvecklaren och Interaktionsdesignern tillgår sina molntjänster från privata enheter - vilket således ökar tillgängligheten.

Användarna identifierar främst fördelar som molntjänsterna erbjuder för att underlätta deras eget arbete vilket är en sanning baserad på intervjuobjektens åsikter. Användarnas åsikter formar en uppskattad sanning som delvis fungerar som svar till studiens forskningsfråga. För att till fullo kunna besvara frågan om varför fenomenet sker analyserades också verksamheternas implementering och efterlevnad av IT-säkerhetspolicys. Tillsammans med de anställdas egna incitament formar detta svaret på forskningsfrågan.

4.4.2 Vikten av att kommunicera en IT-säkerhetspolicy

I teorin diskuteras vikten av att implementera strategier och policys i en verksamhet när de bestämt sig för att använda molntjänster i arbetet. I de fall anställda redan använder privata molntjänster i arbetet rekommenderas därför verksamheter implementera säkerhetspolicys. På så sätt kan de lättare hantera de säkerhetsrisker de eventuellt kan utsättas för när anställda lagrar i privata molntjänster.

När vi i intervjuerna frågade de operativa informanterna på vilket sätt deras verksamheter implementerat IT-säkerhetspolicys för detta framgick det att det hos Företag V inte alls skett. Detta skulle visa sig stämma när vi i intervjun med IT-chefen får reda på att det i dagsläget arbetar med att ta fram en policy för hur anställda skall förhålla sig till molntjänster. Denna är dock inte implementerad än. Han tillsammans med Mjukvaruutvecklaren berättar dock att det finns en icke uttalad policy som är “tillbakalutad” men att det var öppet accepterat att anställda använde sin privata Google Drive i tjänsten.

Svaret på varför Mjukvaruutvecklaren och Interaktionsdesignern lagrar yrkesrelaterad data i privata molntjänster före verksamhetens egen lagringstjänst blir således tydlig. Detta beror på att:

1) Företagets egen lagringstjänst inte är lika tillgänglig och smidig likt deras privata molntjänst.
2) Det finns en total avsaknad av IT-säkerhetspolicy som reglerar användandet av privata molntjänster.

En av anledningarna till att fenomenet sker hos Företag S beror också på att företagets egen lagringstjänst inte är lika tillgänglig och smidig som Systemteknikerns privata molntjänst. Den andra anledningen skulle dock visa sig bero på hur Företag S arbetar med att säkerställa att deras IT-säkerhetspolicys efterlevs. Det framgår nämligen i intervjuerna med samtliga informanter på Företag S att det finns tydliga policys som reglerar användandet av molntjänster i arbetet. Det framgår också att det inte genomförs några kontroller som säkerställer att anställda kontinuerligt upprätthåller de säkerhetsrutiner som återfinns i dessa. Man har visserligen årliga möten där policys etc. diskuteras, men det är inget som sker i realtid. Detta för oss därför in på den intressanta diskussionen om efterlevnad, vilket både i teorin och praktiken visar sig vara en stor utmaning.

4.4.3 Det räcker inte att ha säkerhetspolicyn på intranätet

Som konstaterat ovan har Företag S tydligt informerat anställda hur de ska lagra yrkesrelaterad data i tjänsten. Detta görs dock enbart i anställningens inledande fas då de ges tillgång till de policys som finns och var de senare kan tillgås – på intranätet. De har även årliga möten där de diskuterar de policys som finns och eventuella ändringar. Trots detta har Systemteknikern dålig kännedom om innehållet i dessa policys och eventuella sanktioner, och lagrar därför yrkesrelaterad data i sin privata molntjänst.

Det diskuteras i litteraturen vikten av att följa upp att de anställda faktiskt följer etablerade riktlinjer och policys. De årliga mötena som hålls på Företag S kan därför tolkas som en bristfällig uppföljning som istället i princip fyller en checkbox och skapar en illusion av säkerhet. Utifrån detta kan vi dra slutsatsen att det är viktigt att säkerställa att implementerade policys efterlevs då implementeringen i sig bevisligen inte säkerställer att fenomenet adresseras.

4.4.4 Potentiella säkerhetsrisker

Utöver riskerna som informanterna själva identifierat kartläggs flera signifikanta risker i anknytning till de operativas arbetssätt. I avsnitt (2.2.1) diskuteras t.ex. säkerhetsutmaningar associerade med användningen av molntjänster i arbetet. I och med att Mjukvaruutvecklaren, Interaktionsdesignern och Systemteknikern alla använder molntjänster i arbetet utsätter de potentiellt respektive företag för dessa säkerhetsrisker. Eftersom de tillgår yrkesrelaterad data via molntjänster på privatägda enheter ligger de utanför företagets skyddsbarriär. Detta innebär i teorin att de har betydligt mindre skydd mot hackare som eventuellt vill komma åt deras data. Allt detta sker utan att Företag V och S kan motverka riskbilden. En av de största säkerhetsriskerna med fenomenet är därför risken att data kan hamna i fel händer.

Interaktionsdesignern och Systemteknikern använder väletablerade publika molntjänster i arbetet som Dropbox, Google Drive och OneDrive vilket utsätter både Företag V och S för en ökad risk till skillnad från Mjukvaruutvecklaren som använder AeroFS. Sannolikheten för dataintrång utifrån såväl som inifrån ökar hos väletablerade molnleverantörer. Väletablerade leverantörer administrerar fler kunder som brukar samma infrastruktur och blir då ett mer åtråvärt mål att angripa.

5 Slutsats

I detta avslutande kapitel besvaras undersökningens forskningsfrågor. Avslutningsvis innehåller kapitlet ett avsnitt med våra egna reflektioner kring fenomenet och rekommendationer för framtida forskning.

5.1 Fenomenets potentiella risker och dess orsaker

I uppsatsens inledande kapitel ställde vi följande forskningsfrågor:

Vilka potentiella risker kan associeras med lagring i externa molntjänster?

Varför väljer anställda att lagra yrkesrelaterad data i privata molntjänster före verksamhetens egen lagringstjänst?

För att besvara forskningsfrågorna genomfördes intervjuer hos två företag med dels anställda i den operativa kärnan och dels med beslutsfattare hos respektive företag.

Svaret på vilka potentiella risker som kan associeras med lagring i externa molntjänster kretsar i denna studie kring det faktum att den yrkesrelaterade datan riskerar att hamna i fel händer. Det framgick i intervjun med IT-chefen, när han gavs tillfälle att själv reflektera över fenomenets associerade säkerhetsrisker, att den största risken anses vara dataintrång. Detta är något som även diskuterats i teorin och som ses som den främsta säkerhetsrisken hos Företag V och S. Eftersom Företag V är ett mindre företag som dagligen arbetar med att vinna marknadsandelar på en redan tuff marknad riskerar ett dataintrång hindra deras framfart avsevärt. Även Företag S riskerar att sättas i en svår situation om de skulle utsättas för dataintrång då många av deras affärsrelationer bygger på säkerhet.

Orsakerna till varför anställda lagrar yrkesrelaterad data i privata molntjänster före verksamhetens egen lagringstjänst visar sig i denna studie bero på olika orsaker hos de båda företagen. När vi frågade de anställda som aktivt lagrar yrkesrelaterad data i privata molntjänster hos Företag V och S framgår det att de gör detta tack vare molntjänsternas relativa tillgänglighet och smidighet i förhållande till företagens egen lagringstjänst. Det visar sig även att det inte finns någon implementerad IT-säkerhetspolicy som reglerar användandet av privata molntjänster i arbetet på Företag V, något som i tidigare forskning anses vara ett måste. Anledningen till att Mjukvaruutvecklaren och Interaktionsdesignern lagrar yrkesrelaterad data i privata molntjänster före verksamhetens lagringstjänst beror därför på att:

1) Företagets egen lagringstjänst inte är lika tillgänglig och smidig likt deras privata molntjänst.

2) Det inte finns någon IT-säkerhetspolicy som reglerar användandet av privata molntjänster i arbetet.

Anledningen till att Systemteknikern hos Företag S lagrar yrkesrelaterad data i sin privata molntjänst skulle dock visa sig bero på hur företaget arbetar med att säkerställa att deras implementerade IT-säkerhetspolicy efterlevs. Denna policy reglerar nämligen tydligt att det är företagets lagring som gäller, inget annat. I teorin framhävs vikten av att säkerställa att implementerade säkerhetspolicys faktiskt efterlevs, vilket endast sker i begränsad mån hos Företag S. Man har visserligen årliga möten där policys diskuteras och säkerhetsåtgärder installerade, men det görs inga andra kontroller som säkerställer att dessa efterlevs. Anledningen till att Systemteknikern lagrar yrkesrelaterad data i sin privata molntjänst beror därför på att:

1) Företagets egen lagringstjänst inte är lika tillgänglig och smidig likt hans privata molntjänst.
2) Det kontrolleras och säkerställs inte att Systemteknikern följer den etablerade policyn.

Det underlag som nu lagts fram kan vidare användas av företag då det ger en insikt vad som kan orsaka fenomenet. Vi ser att avsaknaden av en säkerhetspolicy leder till att anställda lagrar yrkesrelaterad data i privata molntjänster. Studien visar också att en implementerad säkerhetspolicy inte garanterar att fenomenet adresseras, utan visar även på vikten av att företag måste säkerställa att policyn efterlevs.

5.2 Egna reflektioner kring fenomenet och rekommendationer för framtida forskning

I den empiriska analysen diskuteras det kort om de anställdas grad av riskmedvetenhet har någon påverkan på att fenomenet sker eller inte. Det visar sig att de båda beslutsfattarna vi intervjuade båda kunde tolkas som att de hade en hög grad av riskmedvetenhet, samtidigt som de inte lagrar någon yrkesrelaterad data i någon privat molntjänst. Mjukvaruutvecklaren, Interaktionsdesignern och Systemteknikern lade ingen större vikt vid vilka säkerhetsrisker de eventuellt utsatte företaget för utan fokuserade snarare på hur smidigt och lättillgängligt de kunde arbeta med privata molntjänster. I kontrast till övriga i den operativa kärnan så uppfattades Serviceansvarig som tämligen riskmedveten och, enligt honom själv, inte använde privata molntjänster. Vi ser därför ett svagt samband om att låg riskmedvetenhet gör att anställda ser mer till fenomenets fördelar istället för konsekvenser vilket hade kunnat studeras närmare för att vidare besvaras.

En annan aspekt som diskuterats i uppsatsen är vikten av att säkerställa att en implementerad policy efterlevs. Efter att ha träffat de anställda på Företag S ställer vi oss kritiska till hur de arbetar med att säkerställa att deras policys efterlevs. Vi tycker nämligen att det är intressant att utåt sett skylta med att de har tydliga policys och kontroller för att dessa säkerställs, men att det sedan visar sig att deras anställda inte alls följer dessa. Är det möjligen så att säkerheten kanske inte är värd uppoffringen det krävs i form av tid, pengar, resurser och dess inverkan det skulle innebära för de anställdas dagliga arbetssätt? Observationen ger sken av att de vill upprätthålla en säkerhetsfasad, men att det kostar för mycket för att den faktiskt skall vara där.

Denna uppsats är av deskriptiv art, vilket innebär att vi i slutändan enbart presenterar *varför* fenomenet sker. Vi uppmanar därför framtida forskning till att analysera *hur företag skall arbeta för att säkerställa att fenomenet inte sker*, alternativt *hur företag kan upprätthålla en tillräckligt hög grad av säkerhet trots att anställda lagrar yrkesrelaterad data i privata molntjänster.*

6 Appendix n

6.1 Bilaga 1 – intervjuguide (operativa kärnan)

6.1.1 Intervjufrågor till anställd

1. Introduktion (om oss och uppsatsen)
    a. David och Andreas
    b. Uppsatsen och dess syfte
    c. Varför har vi valt att prata med just dig?
2. Om intervjuobjektet
    a. Vad har du för roll?
    b. Hur länge har du arbetat för företaget?
    c. I vilken utsträckning är det OK att vi återger dig i den slutgiltiga publikationen?

6.1.2 Kärnfrågor

3. Hur kommer det sig att du lagrar yrkesrelaterad data i privata molntjänster?
    a. Berätta mer, utveckla, kan du berätta mer om det?
4. Säkerhet
    a. Ser du några risker för verksamheten om personal sparar data i privata molntjänster?
5. Implementering
    a. Finns det regler eller policys för hur du borde förhålla dig till lagring av yrkesrelaterad data i molnet?
    b. Hur får du den informationen?
6. Efterlevnad
    a. Följer du dessa regler?
    b. Har du någon egen reflektion kring detta?

6.1.3 Frågor för att styrka BYOD:s likheter/inverkan/parallell till fenomenet

7. Använder du din privata telefon/laptop i tjänsten?
    a. Hur kommer det sig?
    b. Har du någon molntjänst installerad på denna?
8. Vad erbjuder företaget för lagringstjänst?
    a. Berätta mer om den

6.2 Bilaga 2 – Intervjuguide (beslutsfattare)

1. Introduktion (om oss och uppsatsen)
    a. David och Andreas
    b. Uppsatsen och dess syfte
    c. Varför har vi valt att prata med just dig?
2. Om intervjuobjektet
    a. Vad har du för roll?
    b. Hur länge har du arbetat för företaget?
    c. I vilken utsträckning är det OK att vi återger dig i den slutgiltiga publikationen?

6.2.1 Kärnfrågor

3. Säkerhet
    a. Ser du några risker för verksamheten om personal sparar data i privata molntjänster?
4. Implementering
    a. Finns det regler eller policys för hur anställda borde förhålla sig till lagring av yrkesrelaterad data i molnet?
    b. Hur kommuniceras den information till de anställda?
5. Efterlevnad
    a. Hur säkerställer ni att dessa regler och policys efterlevs?

6.2.2 Allmänna frågor

6. Vad erbjuder företaget för lagringstjänst?
    a. Berätta mer om den
7. Har du någon egen reflektion kring detta fenomen?

6.3 Bilaga 3 – transkriberingar

6.3.1 Informant #1 - Mjukvaruutvecklaren

1. I: Till vilken uträckning är det okej att vi återger dig i vår publikation sen?
2. O: Ja hur mycket ni vill.
3. I: Namn, roll, företag?
4. O: Ja
5. I: Vilken är din roll här på företaget?
6. O: Jag är ju utvecklare här och har varit det i tre år nu, jag är en av dem som har varit här längst.
7. I: Vad får du göra då?
8. O: Ja allt möjligt, men det är mycket fokus på telefoni delarna. Jag sitter mycket med Javascript och ser till att telefonsamtal kommer fram.
9. I: Hur kommer det sig att man sparar yrkesrelaterad data i din privata lagringstjänst likt Dropbox, Google Drive eller motsvarande?
10. O: Jag gör det inte jätte mycket egentligen. Men det gör jag för att enkelt kunna komma åt det hemifrån om jag skulle behöva jobba hemifrån en dag. Vi har ju egentligen ingen bra företagslösning för det, som är lätt att komma åt.
11. I: Om jag uppfattar dig rätt så ger det dig en mer tillgänglighet och underlättar ditt arbeta?
12. O: Ja
13. I: Vad är det som du lagrar?
14. O: Det är egentligen inte något som har så mycket med jobbet att göra utan mer inställningar till program som används så att de är synkade på alla mina datorer.
15. I: Vad är det för molntjänst du använder?
16. O: Jag använder något som heter AeroFS som är ganska likt Dropbox fast att man hostar servern själv hemma så får man så mycket plats man vill och gratis.
17. I: Du hade lagrat tidigare körde du AeroFS då också? Och då av samma anledningar?
18. O: Ja
19. I: Hur hade det fungerat om du inte hade fått lagra i ditt privata moln yrkesrelaterade grejer?
20. O: Ja i de sakerna sparar jag ju egentligen inte yrkesrelaterade grejer
21. I: Men inställningarna då?
22. O: Ja till program, till terminalen vilka färger den ska ha till exempel.
23. I: Okej så det är mer som någon form av memo, så att du ska komma ihåg inställningar?
24. O: Ja
25. I: Är det en kod?
26. O: Nej det är ju inte kod liksom
27. I: Har det i någon utsträckning varit yrkeskänslig data som du sparat privat?
28. O: Ja det har jag gjort, jag har haft lite textfiler. Lite kom ihåg grejer, punktlistor och sådär av olika projekt som jag har hållit på med här.

29. I: Utifrån verksamhetensperspektiv ser du några risker med att man lagrar på detta viset?
30. O: Absolut, att lagra företagsdata på något annat än vad företaget tillhandahåller är inte så bra
31. I: Vad är det som inte är bra menar du?
32. O: Ja men om min server där hemma skulle bli hackad eller någonting, så känslig information är dumt att spara.
33. I: Vet du om företaget har någon uttalad policy eller regler för hur anställda ska förhålla sig till just det här fenomenet som vi beskriver?
34. O: Det vet jag faktiskt inte om vi har. Vi har nog ”tänk” som policy
35. I: Alltså typ tänk dig för?
36. O: Ja precis, tänk var inte dum. Vissa företag har ju att det inte är okej att ta med USB hem från jobbet, vi har inget sådant.
37. I: Det är liksom upp till var och en?
38. O: Ja precis. Vi kommer ju åt våra datorer via VPN också om vi vill så vi behöver ju inte spara i molnet.
39. I: Men det är enheter som ni själva är ägare till?
40. O: Nej, det är jobbets.
41. I: Mobiler också?
42. O: Nja nej eller typ. Företaget äger halva min telefon eller de har betalt halva.
43. I: Har du tillgång till din molntjänst på telefonen?
44. O: Nej bara på datorn där hemma
45. I: Men datorn du använder hemifrån är din?
46. O: Ja det är min
47. I: Och där arbetar du med AeroFS som huserar båda företagsdata dsv inställningarna och dina privata ärenden?
48. O: Ja
49. I: Och lite listor som nu är borta?
50. O: Ja precis de finns inte kvar
51. I: Följdfrågan är nu om det fanns en policy hur kommuniceras den, hur får ni reda att det finns en policy? Eller du kanske inte känner till det i och med att det inte finns någon uttalad policy?
52. O: Vi har ju lite grejer med policygrejer gällande IT.
53. I: Jag lyssnar gärna.
54. O: Vi är ju på utvecklingsavdelningen bryr sig inte så mycket om dem men det är mer för säljare och supporten vad som får installeras på datorn och sådant. Det är IT-avdelningen som ska installera det.
55. I: Hur kommer det sig att man inte bryr sig på utvecklingsavdelningen?
56. O: För att vi kan hantera våra egna datorer.
57. I: Ni anses vara tillräckligt kompetenta för det?
58. O: Ja.
59. I: Vi har ju redan frågat om du använder en egen telefon i tjänsten som du har svarat på men kan istället fråga hur kommer det sig att du använder din egen telefon i tjänsten?

60. O: Jag använder ju den inte i tjänsten egentligen.
61. I: Du gör inte det?
62. O: Nej, jag ringer aldrig några i tjänsten.
63. I: Du ringer inga arbetsrelaterade samtal?
64. O: Nej, jag har ju en fast telefon på mitt skrivbord också.
65. I: Okej så det är egentligen där du ringer från?
66. O: Ja, och mitt fasttelefonnummer är kopplat till min mobil. Så om någon ringer in på mitt fastanummer så kopplas det automatiskt till min mobiltelefon.
67. I: Har Företag V någon funktion så att de kan remote wipea din telefon?
68. O: Nej vi har en beta som inte används.
69. I: Vad har Företag V för lagringstjänst till er?
70. O: Vi kör Github till all kod.
71. I: [Namn] var också inne på det tidigare han sa att det var mer inbäddat i ert arbetssätt och på så vis så behövde man inte tänka på mycket över hur man ska lagra utan genom att det ingår med github i ert arbetsätt så…
72. O: Precis, på så vis kommer all kod dit så kan man hämta ut koden hemifrån också om man vill
73. I: Och det gör du från din privata dator?
74. O: Om jag jobbar hemifrån så ja. Annars vad har vi mer? Vi har ju inte så mycket annan lagring som vi behöver.
75. I: Du delar aldrig med dig av något som inte gör sig bra i Github?
76. O: Nej, vi har ju i stort sett bara kod.
77. I: De som du jobbar närmst är mest intresserade av kod och därav att det endast delas kod sinsemellan, det finns inget annat som är uppe på tapeten?
78. O: Nej allt det där finns i Github
79. I: Github är ju en kodares version av molntjänst
80. O: Ja det är ju verkligen det.
81. I: Har du några spontana funderingar över det här fenomenet som vi har pratat om?
82. O: Med företagsdata i molnet?
83. I: Ja eller just för er användare att det inte finns några riktlinjer för vad som får läggas upp på ens privata Dropbox? Ingen reflektion över det?
84. O: Nej inte direkt då vi är så pass små, Företag V är ett så pass litet företag att än så länge tror jag inte att det är några problem. Men när ett företag blir större och större så tänker man att det blir ett större problem.
85. I: Vad är det som blir ett problem då tänker du?
86. O: Det blir ju fler människor att lita på och om det skulle läcka ut något så kan det vara svårare att hitta vem som är läckan.
87. I: Framförallt så kanske det som läckt ut skadar mer desto större företaget är?
88. O: Ja precis, så är det ju.

6.3.2 Informant #2 - Interaktionsdesignern

1. I: Vi kommer att utforska frågan om hur det kommer sig att man lagrar yrkesrelaterad data på det privata molnet.
2. O: Jag kan säga direkt att jag gör det inte så mycket just nu. Jag gjorde det mycket tidigare, då använde jag Googlelösning, bara så att ni vet.
3. I: Det är okej, då får vi prata lite om hur de agerade då tänker jag. Jag tänkte börja med att höra vem du är och vad du har för roll här på företaget?
4. O: Jag är interaktionsdesigner här på Företag V och jobbar mycket med webben men nu även APPAR också till slutkund. Så jag är interaktionsdesigner och har ansvaret för användarupplevelse. Jag jobbar på utvecklingsavdelningen och är ensam designer på företaget hitintills med ett tjugotal kodare. Vi kommer få in ytterligare en designer nu till sommaren.
5. I: Hur länge har du varit på företaget?
6. O: Lite mer än ett år.
7. I: Till vilken utsträckning är det okej att vi återger dig i vår publikation sen?
8. O: Det är helt lugnt
9. I: Till namn och till roll?
10. O: Ja helt okej
11. I: Då kör vi igång men då får vi basera dina frågor litegrann till ditt tidigare för det händer inte nu om jag förstår?
12. O: Nej inte särskilt mycket. Tidigare hade vi Microsoft, vi körde Outlook men Microsoft hade ingen vettigt lösning för det där tror jag att många upplevde och många av oss var Google användare annars så vi körde Google Drive vid sidan om.
13. I: Du sa Outlook skickade du då så för att du skulle kunna nå det hemifrån, alltså att den fungerade som din molntjänst?
14. O: Aha Outlooken, eller vad menar du? Nej, den var nog helt orelaterad till. Vi hade ju ingen bra lösning för att lagra saker på nätet, filer och så med Microsoft. Det hade i alla fall sin egen lösning men den var så dålig så jag har glömt bort vad den heter och det var ingen som använde den om vi nu ens hade tillgång till den.
15. I: Så då skulle du vilja säga att den största anledningen till att du sparade privat yrkesrelaterad data privat var att företaget inte hade en lösning?
16. O: Ja, de hade inte så bra lösningar. Nej vi hade inga bra lösningar såsom jag upplevde det då för att spara saker i molnet och inte lokalt på datorn.
17. I: Behövde man spara i molnet?
18. O: Jag behöver ju det, det är ju väldigt tråkigt om en disk kraschar, och man inte får tillbaka all data. Så det är ju ett sätt att säkra sitt arbete. Jag sitter ju och gör mycket skisser och sådant. De andra killarna sitter ju och synkar sin kod mot Github så de har mer automatiserat, inbäddat i deras arbetsprocess att det lagras någonstans. Det har ju inte jag i och med att jag håller på med skisser och grafiska grejer så min output är ju att jag visar det för folk hur det ska se ut. Men det är ju inte inbäddat och det finns inget som forcerar min arbetsprocess och säkerhetsställer att det lagras någonstans. Vilket såklart är väldigt bra om jag skulle lämna företaget och överlämna till någon, då är det ju väldigt bra om allt finns på ett ställe mer än att finns på min dator.

19. I: Jag tänker är det bara från ditt eget perspektiv, från en anställd, den enda fördelen med att spara i din privata Drobox för säkerheten, om datorn skulle krascha eller att det skulle försvinna? Jag menar ser du inga andra fördelar med detta i ditt arbete?
20. O: Jo fördelen med Google Drive för mig är att det väldigt smidigt att plocka upp det på en annan enhet. Det är en stor fördel med att använda Drive, om inte företaget skulle ha Drive, och man jobbar som jag exempelvis där man jobbar med APPAR och tar fram mockups, illustrerade skärmbilder. Då är det otroligt smidigt att slänga in de i en Drive mapp ta ut dem och se det som ett interface där. Det är även smidigt att kunna plocka upp det hemma om man inte kände att man blev klar på jobbet, eller att göra något på kvällen sen när man kom hem. Det fyller ju även funktionen att komma åt material på andra enheter.
21. I: Kan du inte se någon annan fördel bortsett från säkerhet och att det underlättar ditt arbete genom att du kan presentera det på fler enheter?
22. O: Nej det gör jag nog inte egentligen. Jag har ju nu under min tid i arbetslivet sett att det är smidigt att komma åt. Nej annars tycker jag inte att jag ser några stora fördelar med.
23. I: Ser du någon risk för verksamheten när du sparar yrkesrelaterad data privat?
24. O: Ja det är väl inte särskilt bra man bör skilja på privat och företagsgrejer. Nu ska jag dock poängtera här så att detta inte blir missvisande när jag har gjort detta på jobbet så har jag registrerat ett nytt konto hos Google så jag har inte kört till min egna privata på det sättet, utan har lagt det på ett nytt konto under mitt namn. Så jag blandade inte ihop det med mina privata grejer egentligen för jag använder det väldigt mycket även privat. Men självklart för företaget är det en nackdel att man synkar grejer via lösningar och tjänster som inte de har koll på.
25. I: Vad tänker du är en risk med det?
26. O: Ja dels att jag kan sno. Företag V inga etablerade policys på det sättet och vi arbetar kanske inte så mycket med konfidentiella grejer, hemligstämplade, men det är ju ett problem om jag synkar det till min privata Drive som jag har på telefonen och skulle tappa telefonen då är det ju lätt för andra att komma åt data och dokument som de egentligen inte borde komma åt. Så det är ju ett problem, av en olyckshändelse så kan andra få tillgång till information. Ett annat problem är ju att jag själv skulle kunna säga upp mig, springa iväg och göra något sådant som inte företaget vill. De är ju främst de två grejerna.
27. I: Så du menar att då har du fortfarande tillgång till företagets data trots att du är uppsagd?
28. O: Ja så är det ju, jag kan ju ha lagt det på min privata data hemma och det har ju företagets inte någon aning om. Så det är väl framförallt för företagets räkning som jag kan se att det är negativt.
29. I: Jag funderar lite på om ni har fått någon firmatelefon eller om detta sker på din privattelefon?
30. O: Nej vi har inga firmatelefoner men vi har väldigt bra erbjudande att man kan få köpa en telefon via företaget. Eller rättare sagt om du köper en telefon så kan du få avdrag för den. Men det är fortfarande din privata telefon, vi har inga jobbmobiler på det sättet.

31. I: Så ni är fullständiga ägare till den här mobilen?
32. O: Ja
33. I: Det är mer än förmån att få rabatterat pris på en mobil?
34. O: Ja, precis. Det är väl en form av löneförmån. Vi äger fortfarande mobilerna.
35. I: Jag tänker mer utifrån ett säkerhetsperspektiv från företag vilket innebär ännu mindre koll?
36. O: Ja de är få människor här som springer runt med en telefon som ägs av företaget. Det kanske är i testsyfte möjligtvis.
37. I: Du berörde det lite innan men jag ställer frågan ändå, finns det regler eller policys för hur anställda borde föra sig gällande detta just att vi kan spara i privata lagringstjänster?
38. O: Nej vad jag vet så finns det inte det. Jag kan inte minnas att jag har läst någon sådan grej, så jag tror inte att vi har någon policy för detta.
39. I: Vi kanske kan hoppa nästkommande fråga då den var hur kommunicerar företaget ut denna policy till de anställda?
40. O: Ja om jag skulle svara något där så om det finns någon så kommuniceras den inte ut speciellt bra.
41. I: Det finns ingen internt förhållningsätt såsom ”man borde”?
42. O: Vi kör ganska layed back. Det är väldigt öppet att folk körde Drive, det var inget hemlighetsmakeri.
43. I: Du nämnde att du använde din privattelefon men använder du din privata dator i tjänst?
44. O: Nej min egen dator använder jag väl inte riktigt… eller jo det kan jag ju göra såvida om jag ska kolla på interface. Ja, jag använder min privata dator och telefon till tjänsten såvida att jag testar med den ibland, jag håller grejer på Drive. Kollar på grejer i Drive gör jag även på min privata dator, men jag är rätt så bra på att inte arbeta hemifrån dock. Jag försöker att inte ta med mig jobbet hem.
45. I: Hur kommer det sig att du använder dina egna verktyg i tjänsten?
46. O: Smidigt. Hemifrån så finns det ju inget alternativ, jag skulle ju kunna be om att få låna en laptop härifrån men det känns otroligt stökigt. Bara för att kolla mailen eller någon fil på Google Drive.
47. O: Nu är ju allt där så det brukar inte vara några problem med att behöva installera program. Men den stökiga delen är ju att jag bara kan göra det på min dator hemma eftersom att allt är cloudbaserat. Det finns ingen anledning att behöva kånka med mig 2 kg dator hem. Om jag hade arbetat mer hemifrån så hade jag kanske gjort det, då kanske jag hade velat ha en mer dedikerat dator till just jobb, men jag arbetar inte särskilt mycket hemifrån.
48. I: På de privata enheterna som du använder i tjänsten då telefonen och till viss mån dator, har du någon molntjänst installerad på de här enheterna?
49. O: Ja det har jag men det är bara på mobilen som den molntjänst jag har installerad som jag gör arbetsrelaterade grejer på. Hemma på dator gör jag allt via webbrowser när det har med jobbet att göra.
50. I: Vad erbjuder företaget för lagringstjänst?

51. O: Till oss anställda? I så fall är det ju Google Drive. Vi kör deras lösning Gmail, Google, Drive och allt som följer med så that's it.
52. I: Det är också efter att de har tagit bort den här Microsoft lösningen?
53. O: Ja innan hade vi ju ingen officiell Google koppling. De som då som behövde en bra lösning körde dem ändå.
54. I: Har du några egna reflektioner över allt vad som nu har pratats om?
55. O: Nej det har jag väl inte men det är otroligt smidigt att vi har gått över till att alla kör samma molnlösning. Det innebär att jag har en mapp på företaget som alla har tillgång till om de vill kolla på designrelaterade grejer. Det är otroligt smidigt på det sättet. Det var bökigt tidigare när inte alla körde Drive tidigare och delade med sig saker t.ex. dokument. Det var väldigt komplext och meckigt.
56. I: Den här nuvarande lösningen, har ni möjlighet att logga in på den på era privata enheter?
57. O: Ja det gör ju jag. Google synkning idag kan ju ha en rad konton kopplade till en enhet så jag har företagets konto kopplat till den och till andra APPAR.
58. I: Använder du något verktyg som bara är ägt av företaget som du arbetar på?
59. O: Ja, datorn som jag använder här på plats.

6.3.3 Informant #3 – IT-chefen

1. I: Till vilken utsträckning är det okej att vi återger dig i den slutgiltiga publikationen?
2. O: Att företaget är anonymt och att jag som person är anonym.
3. I: Uppfattat... då kör vi igång. Vi börjar med en fråga som berör säkerhet, hur kommer det sig att anställda lagrar yrkesrelaterad information på sin privata molnlagringstjänst likt Dropbox, Google Drive eller likvärdiga. Och om man tittar på säkerhet där hur ser du som beslutsfattare kring vad finns det för risker för verksamheten när personal gör på det här viset?
4. O: Beroende på verksamhetens natur så finns det ju olika risker, det kan ju läggas dokument som är knutna till externa kunder eller interna anställda med personuppgifter. Det finns ju alla sorters möjliga risker. Säg att HR-avdelning skulle lägga ut ett dokument som innehåller personuppgifter på anställda på sin egen Dropbox då tappar ju företaget kontrollen och bryter mot PUL-lagen exempelvis. Det är ju ett exempel men det är också kundbasering, kunder så att säga, som det finns kontakt mot kund eller offererar en offert till kund eller kommunikation mellan kund och företag som ligger på utsidan också det är inget som kanske trotsar lagen som sådan men det är kanske däremot något som går emot företagets policy. Man vill inte dela med sig av sina egna kunder till sin konkurrent eller att man vill ha det publikt, erkänd av alla. Så det finns definitivt risker, speciellt om personen i fråga sedan lämnar företaget och går till ett annat konkurrerande företag så kan personen då ta med sig kundbas.
5. I: Då blir han en direkt konkurrent som besitter kundregister så att säga?
6. O: Ja precis, helt riktigt.

7. I: Och du nämnde just en säkerhetsrisk att det, vad ska vi säga, ligger utanför företagets armar att de har informationen sparad privat vilket gör att det kan läcka, på så vis?
8. O: Det är ju en säkerhetsrisk generellt om det inte ligger på företagets cloud eller vad man vill kalla det. All dokumentation härrörande till företaget ska ligga inom företagets ramar som är föreskrivet till de anställda. Allt utanför där bryter man egentligen emot företagets policy men det förekommer ju frekvent på ganska många företag.
9. I: Det är ju det vi ser också…
10. O: Ja men precis.
11. I: Det är därför vi tittar på det hur det kommer sig. Men nu när vi har frågan uppe vill du laborera kring varför du tror att detta förekommer?
12. O: Jag skulle jätte gärna vilja det men jag tror inte att jag kan det för jag tror att det är en ganska svår fråga ibland. Sitter du på företaget med Microsoft Office miljö och har en skydrive och kanske använder en skydrive privat och man har inte sett att man är inloggad fel på t.ex. på Crome så kan man ha diverse konton där användare kan ha varit fel inloggade och inte uppmärksammat det på en gång. Så jag tror att det kan vara en del av problemet, ett misstag. En annan del är ju direkt uppsåt att man vill ha det där i stället för att man tycker det är ju bättre, jag kanske ska lämna snart osv.
13. I: En av de största cloudbovarna till sett från säkerhetssidan är mycket det du talar om att du har en privatmiljö till exempel att du är inloggad med ditt privata på webbläsaren och har besökt diverse sidor och har inloggningsuppgifter sparade. Sen är det lätt att ta sig an utifrån som en hackare eller hur du nu tar dig an det, sen sitter du på jobbrelaterade ärenden på samma telefon/padda/dator. Då har de helt plötsligt tillgång till din företagsvärld. Så det är lite något du försöker?
14. O: Ja absolut. Det behöver ibland inte vara så delikata dokument som sådan som en hackare kommer åt kanske men utan bara det att den kommer åt det. Beroende på vad det är för dokument, det kan ju också i längden skada företaget att de vart hackade så lätt med lösenord eller dålig underhållen brandvägg. Det finns alla olika sorters aspekter där men jag tror att det är farligt för företaget om man får det blir ett rätt så stor skada på namnet om sådant sker oftast. Man tänker att de var de som den här hackaren lyckades, vi ska nog välja ett annat företag.
15. I: Man kan tänka sig att anställda vill argumentera att det inte är så stort företag och att den informationen som jag besitter är inte jätte stora affärshemligheter således så tycker jag att det inte är speciellt viktigt, men då reflekterar de inte över risken det gör med varumärket. De kanske tänker att det finns någon uttalad policy som typ tänk efter vad du gör nu, men de tänker inte riktigt i den utsträckningen att det egentligen kan skada företaget.
16. O: Varumärket är ju extremt viktigt, om man klarar av att bygga upp ett varumärke som blir väldigt känt Coca Cola, Apple, Microsoft så är det väldigt känsligt att man får just…
17. I: Det blir mer åtråvärt om är skyddade…
18. O: Ja precis, helt klart. Man blir ju säg att du tycker om kaffe från X men Y ligger närmare, du går över gatan men Y låg på vägen och du bara åh kaffe men nej stort

skillnad. Man går långt för att man känner igen varumärket, så märket är ju väldigt värdefullt.

19. I: Innan jag går vidare till nästa fråga vi har ju nämnt att säkerhetsrisker som finns är att det kan läcka och att varumärket kan skadas. Ser du någon annan risk med att anställda gör såhär?
20. O: Nja, det finns säkert någon men jag kan inte komma på det på rak arm. Inte mer än vad jag nämnt faktiskt.
21. I: Då kommer vi till en ledande fråga finns det regler eller policy för hur anställda bör förhålla sig emot det här fenomenet i det här företaget?
22. O: I dagsläget inte direkt.
23. I: Inte direkt, går det att utveckla?
24. O: Absolut. Ja vi håller precis på att upprätta den här så det finns faktiskt inte i dagsläget att de anställda kan läsa sig till vad som gäller egentligen och det är ju mitt uppdrag här att se till så att det ska komma på plats.
25. I: Okej, hur är tanken att den här policyn i så fall ska vara uppbyggd? Hur begränsad kommer den att vara eller hur kommer ni att ställa er till fenomenet?
26. O: Vi kommer väl att tillrätta oss efter i den form som jag tidigare beskrev i frågan. Att vi har en policy att vi ska ha våra dokument allt som tillhör vårt företag ska ligga inom våra cloudtjänster, i vår lagringstjänst inte på extern lagringstjänst som inte drivs av företaget har överblick över. Privatinloggning kommer säkerligen att förekomma, det är väldigt svårt att styra att de inte får logga in privat just i webbläsare och så vidare.
27. I: Det är Google Drive som ni kommer att ha som företagets lagringstjänst i molnet?
28. O: Ja
29. I: Ser du några problem att det är under ett gränssnitt som Google Drive erbjuder kan förena både den privata sfären och företagssfären, under samma gränssnitt?
30. O: Du menar alltså att Gmail?
31. I: Jag menar jag kan ju sortera mina mail från konton i samma inkorg
32. O: Ja precis, det ser jag givetvis. Jag skulle inte tillåta en sådan stor integration för att just selektera och göra till mindre möjligt till att göra fel.
33. I: Anställda, vi har ju tittat mycket i litteraturen och andra intervjuobjekt som har sagt att, detta ger en väldigt stor tillgänglighet?
34. O: Tillgänglighet för individen, ja
35. I: Precis, det underlättar för dem att utföra arbetet, så vi ser att de är villiga att kringgå policyn för att det hindrar deras arbetssätt för mycket.
36. O: Att anställda är villiga att kringgå policy så är det väl tyvärr med mycket men en policy är ju där för att följas. I beroende på vilken utsträckning man bryter den så blir det ju sanktioner efter graden där också definitivt. Annars är det ju svårt att upprätthålla en bra policy.
37. I: Policyn håller på att formas som jag förstår det, hur kommer den att kommuniceras ut till företaget?
38. O: Den kommer att kommuniceras, ja bra fråga, vi har inte riktigt kommit så långt. Vi kommer definitivt att gå ut på intranätet att vi har kommit med en policy och att alla

ska läsa igenom den här. Nyanställda kommer att få den till sig i en form återstår att se i vilken form om PDF eller ja det är ännu osäkert där.

39. I: Vi har ju mycket i litteratur om policys rent generellt sätt hur man kommunicerar eller i princip hur man implementerar en policy påverkar väldigt mycket på hur de efterlevs så att det är väl delvis därför som vi tittar på det. Som sagt även fast det finns en policy så är det en väldigt stor procentenhet som inte känner till policyn och därför tycker vi att det är kul eller intressant att titta på just hur det kommuniceras. Följdfrågan här blir ju, du har antagligen svårt att svara på det också i och med att ni inte har en policy implementerad än, hur säkerhetsställer ni att er policy efterlevs?
40. O: Allting är beroende på vilken policy vi tittar på. I policyn kommer det till exempel att stå att ditt lösenord ska innehålla x antal karaktärer och innehålla olika former versaler och tecken och så vidare, att det ska löpa ut efter ett visst antal dagar och att du får testa ett antal gånger innan det låser sig. Detta kan ju kontrolleras genom att du inte kan byta till samma. De här formerna av policys är ju ganska lätta att de inte behöver kontrolleras på sådant vis utan de sköter ju sig själva. Däremot som jag pratade om upphovsrättsmaterial som filmer och musik det förekommer ju att man inte får lov att installera program på datorerna. Det sköts scanning på dator för att kontrollera efter en gemensam lista på tillåtna installerade program och avvikelser därtill.
41. I: Jag tänker mer på hur man tänker säkerhetsställa att arbetssättet här efterlevs utifrån policyn?
42. O: Du kan ju inte säkerhetsställa det på så vis om du inte restriktiv i tillgången till exempel Google Drive bara från det interna nätet. Det är ju så du kan göra restriktiv, säg om du inte gör det så kan inte göra restriktiv så kan du göra så att personer inte kan ladda ner programmet på sin hemdator exempelvis. Extremt svårt, det finns stora företag som har försökt att hålla just dokument innan företagets väggar men det blev extremt komplexa lösningar och väldigt svår jobbat.
43. I: Det hämnar ju arbetsprocessen
44. O: Ja det hämnar jobbet extremt mycket som sagt var
45. I: Det är ju detta som gör det så svårt, det kommer alltid att finnas en möjlighet för anställda att kunna ha yrkesrelaterad data på sin privata molnlagring
46. O: Ja även om man gör restriktiv till att inte ge tillgång utanför våra IP ranger så att säga, så har du fortfarande en kameramobil med dig och kan ta ett kort på skärmen. Det är jätte svårt.
47. I: Du tillgår ju via din privata telefon eller dator och då är du direkt utanför företagets säkerhet och den integritet som ni har byggt upp. Då tar man sig på sig an en allt mycket större risk och tittar man på tidigare intervjuobjekt så ser de fördelar med tillgängligheten istället för att det är en risken.
48. O: Ja men det ska vara en balansgång där. Man måste ju ha en balansgång man kan inte släppa på alla säkerhetsaspekter in favor av tillgängligheten tror jag för det kan komma tillbaka och skada företaget mer än vad man tror. Det vore ju en underbar värld om vi levde utan problem, men så är inte fallet. Till en viss grad behöver man ha frihet men till en viss grad så behövs säkerhet och det måste finnas båda två och mötas. Det får inte bli för svår jobbat men det får inte släppas för långt från

verkligheten. Så att vems om helst från utsidan kan se insidan, då kan det snabbt gå fel.

49. I: Vad erbjuder företaget för lagringstjänst och berätta lite mer om den?
50. O: Vi erbjuder Google Drive som lagringstjänst, vi uppmanar att inte direkt spara på datorn av säkerhetsskäl. Det ska också ingå i policyn som ska komma ut. Allt lagras på Google Drive eller lokalt på datorn.
51. I: Är alla enhetliga att de använder Google Drive?
52. O: Vad jag väl tror idag är att allt just ligger runtomring. Om du skapar ett dokument i Google Drive så blir det ju i Googleformat, du kan inte spara det på samma sätt som du gjorde i ett Officedokument, Word, Excel och så vidare. Det är lättare att arbeta med när man väl sitter med det, du har ju allt i tabbarna i Crome. I Office har du ju olika program, du kan ju givetvis ha det i tabbar också om du kör det liveversionen.
53. I: Du sa lite att Skydrive användes tidigare och att man då föredrog att använda sin privata istället för Skydrive?
54. O: Ja att de använde Google Drive
55. I: Ja precis
56. O: Ja och det var ju av den orsaken som vi valde att gå över från Office till Google Drive då det var så pass skilda läger så att säga och i ett företag så går ju inte det. Man hade uttalat att man skulle arbeta där fast företaget hade svårt att efterfölja det själva så sitter du i befattningsstolen och inte efterföljer det själv så är det ju rätt svårt att få ner det till resten av de anställda också.
57. I: Nu har vi en avslutande fråga har du några egen reflektion över vad vi har pratat om idag? Något du själv tänker på? Tänker att det här är kanske viktigt att tänka på eller så?
58. O: Nja alltså det är ju, jag tror att om du också har den aspekten i det hela att det beror på vad man är av för generation. Jag tror att om man är av en yngre generation idag runt tjugo års ålder så tror jag att man har en mer öppen vy på det hela man kanske inte tänker så mycket ur säkerhetsbanan. Var av att jag tror att en äldre generation är mer konservativa, allt på gott och ont så att säga. Så där någonstans så måste man ju mötas men det är ju alltid så i generationer. När jag var tjugo tänkte man på ett sätt och de som var äldre tänkte på ett annat sätt. Tidigare så inrättade man sig men jag tror i dagens läge så är det inte så det krockar liksom men också på gott och ont. Jag tycker att alla ska få säga sitt och bidra sitt. Idag kommer det in teknik som yngre lär sig extremt snabbt och lättare än de äldre tror jag.

6.3.4 Informant #4 - Systemteknikern

1. I: I vilket utsträckning är det okej att vi återger dig i vår uppsats sen?
2. O: Hur menar du med namn och så?
3. I: Ja…, och roll, företag.
4. O: Du kan ju säga att jag är IT- tekniker men inte namn
5. I: mm… okej men så det är bra där?
6. O: Ja
7. I: Okej, bra och då kommer vi ju till nästa fråga vad har du för roll? Vill du utveckla det litegrann?
8. O: Systemtekniker är väl egentligen min titel och jag gör väl lite i allo servers, telefoni och växlar
9. I: Du gör servers och telefoni? Är det rent fysiskt eller är det mjukvara?
10. O: Jag håller på med support, drift, installation
11. I: Rätt stora spektra då alltså?
12. O: Ja det är det mesta, felsök.
13. I: Det blir väl lite spindeln i nätet roll när man är på ett mindre företag?
14. O: Ja det blir ju lite så
15. I: Jag hoppar direkt in på kärnfrågan för att jag vet att du har lite med tid: hur kommer det sig att man sparar yrkesrelaterad data på egna molntjänster?
16. O: För att vi själva inte har någon sådan tjänst. Jag tycker, jag gör inte det ofta, de gånger de har hänt så har jag gjort det för att jag har en laptop och står typ i en källare och jag ska bara ta en backup på en växel. Till exempel så lägger jag den där och synkar för att sedan kunna hämta upp den smidigt här i korrekt mapp, sen tar jag bort den
17. I: Okej så om jag lyssnar på dig så är det för att underlätta ditt arbetssätt?
18. O: Ja
19. I: Och någon form av tillgänglighet för dig?
20. O: Ja, att istället för att man ska behöva lägga in på en FTP, för att sedan lägga upp, komma hit här, logga in på FTP, dra ner den, ta bort den. Det är så många steg.
21. I: Istället för att bara sätta allt där på vilken enhet du vill dra ner den på för att sedan köra igång?
22. O: Ja, precis
23. I: Snabbare arbetssätt, mer tillgängligt?
24. O: Ja precis. Sen är klart, det är inte bara att göra det ju men…
25. I: Jag undrar bara varför?
26. O: Jag kan tycka det är mer osäkert att mail den.
27. I: Är det bara för att du? Nu ska vi veta att du är väldigt tekniskt kunnig och det ska vi ju ha i åtanke när vi transkriberar detta, du är inte en normal intervjuare här. Men du tänker att protokollen på mail ser mer klenare ut än för att molntjänster?
28. O: Ja, absolut, för det är ju ändå krypterat när du synkar det.
29. I: Att ladda upp till typ Dropbox för att du vet att det är krypterat?
30. O: Inte Dropbox, utan Onedrive.
31. I: Det är väl Microsofts lösning?

32. O: Ja men det är det.
33. I: Och mailen är inte det också krypterat i någon utsträckning eller det kanske bara är en svagare kryptering?
34. O: Nej, det är det ju inte. Man skickar det ju ändå i klartext, eller det beror på vad servern har för stöd och så men normalt sätt så är det ju klartext
35. I: Leder in på nästa fråga som du har svarat lite på: men vad ser du för risker och då tänker jag utifrån verksamheten när anställda lagrar såhär?
36. O: Risken är väl typ om någon skulle hacka något av dessa konton
37. I: Vare sig det, det privata eller företagskontot tänker du på eller?
38. O: Ja, alltså det är väl egentligen ingen större risk för om vi säger att det är en backup på en växel. Vad ska folk med den till? Alltså de kan se hela confen, de kan ju i och försäg om de installerar rätt program och om de importerar den på rätt sätt och så.
39. I: Men dom har svårt för att använda dem?
40. O: Ja eller så de vet anknytningarna och får reda på deras direktnummer men det är inte så att det är lösenord eller en databas.
41. I: Inga yrkeshemligheter?
42. O: Ja precis det är ju inte sådana grej utan mer backupfiler av växlar.
43. I: Så det är inget större risktagande på verksamheten?
44. O: Nej det är det ju inte.
45. I: Jag kör på här, finns det regler eller policy för låt säga vad vi bör för oss till…
46. O: Du menar vår egen företagspolicy?
47. I: Ja
48. O: Jag ska vara ärlig och säga att jag kan ju inte den innantill och utantill. Det var länge sedan jag läste den så jag vet inte, men jag skulle gissa att det står någon rad om detta men det är inget jag har reflekterat över.
49. I: Men du tror att det finns en policy och att den benämner detta?
50. O: Ja jag tror det men jag vet ju inte som sagt… det kanske jag borde kolla upp.
51. I: Följdfrågan här blir ju ganska uppenbar: hur får du den här informationen till dig, hur förmedlas den till dig?
52. O: Den finns på intranätet. Det är väl det.
53. I: That’s it? Du går dit in om du vill veta, typ?
54. O: Ja faktiskt
55. I: Och slutfrågan där angående säkerhetsbiten är väl hur säkerställer företaget att ni efterlever den här policyn som du tror finns?
56. O: Inte så bra
57. I: Annars hade du vetat att den har funnits? Det kanske säger sig själv! De stickprovar inte? De kollar inte data?
58. O: Nej
59. I: Det är alltså tillit? De förväntar att ni tänker er för?
60. O: Ja, absolut
61. I: Jag hade ett långt snack med [informant 6] också, han uttryckte att han litade väldigt mycket på de anställda också.
62. O: Ja precis, ja det gör han ju, men alltså, ja...

63. I: Vi glider in på sista avsnittet och där börjar vi frågan med: använder du någon privatägd telefon/data/padda eller sådan här enhet i arbetet?
64. O: Nej
65. I: Så alla verktyg du använder, i form av enheter, är företagsägda?
66. O: Ja de är dem absolut, både mobilen och laptop, de är det jag använder.
67. I: Mobilen, använder du den privat sen?
68. O: Ja det gör jag ju.
69. I: Fungerar laptoppen också så?
70. O: Nej har jag bara är på jobbet, den stannar på jobbet.
71. I: Den bor här och den lever här?
72. O: Ja, det gör den, men mobilen bor där hemma också.
73. I: Har du något annan enhet i tjänsten förutom mobil och laptop tänker jag?
74. O: Nej
75. I: Finns det någon molntjänst installerade på dem? Då tänker jag mig även på de för installerade är det inloggning på dem så att säga?
76. O: Ja på telefonen har jag Dropbox och på laptoppen har jag Onedrive. Men Dropboxen på mobilen är bara privat, det är ju bara bilder så att säga som synkas upp där, och Onedriven på laptoppen det är där jag lägger backup-filerna.
77. I: Frågan som du redan har svarat på där men hur kommer det sig att du har dessa molntjänster nedladdade?
78. O: Ja det är ju för att smidigheten.
79. I: Vad erbjuder företaget för lagringstjänst?
80. O: Alltså vi har ju ingen sådan tjänst.
81. I: Som hade underlättat för dig på ”on the go” menar du?
82. O: Ja precis.
83. I: Men har ni någon form av tjänst i detta sammanhang tänker jag?
84. O: Ja vi har ju typ en backup tjänst men det är ju ingen synktjänst på så sätt såsom Dropbox eller Onedrive.
85. I: Vad är fördelen med synktjänst då menar du?
86. O: På backuptjänsten som körs varje dag klockan nio, tar den backup. Men det är ju inte så att jag kan logga in med ett konto och ha en mapp där jag lägger grejer och bara synka det på ett par minuter för att sedan hämta upp det på en annan. Det är ju en mer synktjänst med backup i kan man ju säga. Men vår backup tjänst är ju mer SQL databaser och så klart rena filer men det är inte riktigt samma grej. Vi har varit inne på om vi skulle skaffa en sådan tjänst för använda när vi är ute och så. Men det har inte hänt så mycket. Kunderna kör ju också av Dropbox.
87. I: Så kunderna använder också Dropbox?
88. O: Ja de gör de. Absolut!
89. I: Vad hade varit möjligt, om vi föreställer oss att Dropbox och Drive inte hade funnits på en sekund. Hur är det tänkt att ni skulle lagrat då, om du är ute på fält?
90. O: Ja då får man ha allt på servern och köra VPN in.
91. I: Det går, men det är bökigt, och det tar längre tid?
92. O: Ja
93. I: Och du kan inte plocka upp det på alla enheter sen, eller hur fungerar det?

94. O: Eller jo det kan man men då måste man ha igång VPN och så…
95. I: Det låter drygt.
96. O: Ja det är ju det, det är just den smidigheten man saknar, upp med filerna så synkar det.
97. I: Jag har inte så mycket mer kvar men har du någon egen reflektion du vill få sagt utifrån allt vi har pratat om, någon reflektion?
    O: Ja, alltså jag kan väl känna så att man vet ju inte vem som tittar på data som ligger på Dropbox och Microsift. De ligger ju på deras servers och vi vet ju inte vad de gör med den.
98. I: Du menar att de kanske säljer till marknadsförare eller så?
99. O: Ja det är ju ett agreement som lyder att vi får göra vad vi vill med data och man bara okej gör det. Det är ju det jag inte gillar med tjänsterna.
100. I: Ser du någon risk med det utifrån företaget?
101. O: Nej det gör jag inte men jag tycker bara att det är olustigt att de har möjligheten att gå in och se data. Och sen finns det ju andra tjänster likt Dropbox där allt är krypterat och företaget inte har möjligt att ta tillgång till data, det är krypterat för dem också. Det är ju förvisso inte så ofta jag använder sådana tjänster i arbetet.

6.3.5 Informant #5 - Serviceansvarig

1. I: Till vilken utsträckning är det okej att vi utger dig i den slutgiltiga publikationen?
2. O: Etthundratio procent
3. I: Vi kan ju börja med att du kan berätta vad du har för roll i företaget?
4. O: Jag är spindeln i nätet på servicedesk. Jag knyter alla punkter och alla vänder sig till mig med alla problem. Jag är den som ordnar och donar jag är den som knyter ihop påsen. Jag är den som i stort sätt, ska inte säga ansiktet utåt för det ser man inte i telefonen, men man hör den i alla fall. Jag är rösten utåt från Företag S när det ringer in på servicedesk.
5. I: Du menar att inne på företaget kommer många och frågar dig hur gör vi här, lite spindeln på det vis? Och så sitter du ut mot kunden?
6. O: Absolut, jag ordnar, donar och löser. Jag ska inte säga ett stort, men jag känner att jag har ett rätt så stort förtroende både från kunderna och från medarbetare härinne.
7. I: Hur länge har du arbetet på företaget?
8. O: Mer än tio år.
9. I: Hur kommer det sig att anställda sparar yrkesrelaterad data i molntjänster, sett från din del?
10. O: För min del gör jag aldrig något sådant. Inte en enda megabyte, antingen har jag ett USB minne med mig om jag skulle behöva ta någon information ifrån min laptop som jag har hemma, vilket är min jourdata. Jourdatorn och USB-minnet är båda ägda av företaget, jag har därifrån tagit två VPN- cert med mig från företaget till hemmet för att sedan radera det i hela mitt liv. Aldrig molntjänster.
11. I: VPN-cert det gör att du går via en tunnel hemma för att nå företagsdata som är på företaget?
12. O: Ja precis
13. I: Så att du kan tillgå det på företagsägda datorn när du sitter i hemmet? Förstår jag dig rätt?
14. O: Ja, jag tar hand om jouren och arbetar därför hemifrån. Det var en gång ett cert som hade löpt ut och jag kunde i molnet ta med mig datorn hit här och där installerades den här nyckeln. I annat fall så använder jag aldrig några molntjänster inte Google Drive, ingen form av Dropbox, ingenting. Jag har alla mina grejer på min dator eller på de servers vi har här.
15. I: Den jourdatorn som du tar med hem, surfar man på det också?
16. O: Ja du kan surfa på den datorn. Den surfgrejen jag gör på den, om det är så att folk har problem med att man är ute och surfar exempelvis på blocket, aftonbladet eller någon seriös sida, jag går aldrig in på någon oseriösare sida. Det är en ren dator, det finns ingenting på den. Den används enbart till att arbetas på, jag har min andra dator till att gå in på mer oseriösa sidor. Jag skiljer helt och hållet på företaget och på mig själv.
17. I: Sker det någon form av inloggning av någon form, förstår att det finns till VPN klienten, men tänker loggar du inte in på Företag S hemsida eller någon annan form av inloggning till exempelvis till webbläsaren på den datorn?
18. O: Till något annat?

19. I: Ja bortsett från VPN då. Typ intranätet?
20. O: Det är bara till företaget. Jag håller helt strikt bara till min tunnel, till min grejer. Det finns inget annat på den, så fort det ska ske någon icke yrkesrelaterat så har jag min andra bredvid och då sköter jag det på den.
21. I: Om vi vinklar frågan vi opponerar att du sitter och tar emot ett samtal och du har en liten lista med folk som du ska ringa upp till på eftermiddagen för att du inte har hunnit. Du lägger dem i Dropox för att du skulle behöva nå de sen då du ska ut till kund. Tänk dig det scenariot, vad hade varit din anledning då tänker du? Om du hade satt dig i någon annans skor
22. O: Då är det ju så att med de system som jag har så finns… du menar alltså ifall om jag inte hade hunnit ringa femton samtal?
23. I: Ja
24. O: Och sedan ska jag hinna ringa upp de, men jag har inte hunnit på jobb, så får jag göra det efter jobb eller så kallat på övertid hemifrån. Är det så du menar?
25. I: Ja det behöver inte nödvändigtvis vara just kundnummer, att du tar med dig jobbet men när du gör det så har du lagt det privat?
26. O: Nej det händer inte
27. I: Ja det vet vi men om det hade hänt. Om du sätter dig i någon annans skor som gör det. Vad tror du hade varit anledningen till att göra det?
28. O: Om jag säger såhär med de system som vi har så hade jag enkelt kunnat logga på den vi har här och tagit ut de nummer härifrån, de hade funnits i min egen Företag S mail. Jag hade lagt ett mail till mig själv och sedan hade jag avverkat de där.
29. I: Vad ser du för risker för verksamheten om man sparar privat?
30. O: Allt
31. I: Du får gärna utveckla
32. O: Riskerna är att det kommer i fel händer. Absolut.
33. I: Hur tänker du?
34. O: Det är så att ingenting är säkert idag som ligger ute offentligt på nätet. Dropboxkonton kan hackas och om du har läst alla användarvillkoren där så är du nog inte så bekväm för att överhuvudtaget veta vad som ger Dropbox rätt att använda all informationen till. Jag antar att du är rätt så påläst på detta i och med att du ställer frågan.
35. I: Vi har det i litteraturen i vilket fall
36. O: Frågan är har du läst det?
37. I: Inte användarvillkoren men vi har läst om säkerhetsrisker
38. O: Ja precis, användarvillkoren är inte jätte roliga. Ett av de här användarvillkoren ger de rätt att kunna granska och kolla innehållet som finns i de privata Dropboxens, precis vilken som helst. Vilket jag ser som en säkerhetsrisk. Det ligger som sagt inte så bekvämt för företaget att tillhandhands och därför tycker jag att det inte är någon bra lösning. Likadant med Google Drive.
39. I: Okej, företagsdata kan nås av Dropbox men vad skulle det vara för problem menar du?
40. O: Där finns, vi har ju hand om stora företag, det finns många kunder som har hemliga telefonnummer och VIP-nummer som skulle kunna komma ut och bli offentliga. Det

är ju inte så kul om VIP- nummer kommer ut till offentligheten, det skulle börjas ringas dit när de inte får tag på vår kund på vanliga sättet. Säkerhetsrisk är det ju kanske inte men det är ju ändå information som inte ska nå ut till andra kunder. Det finns ju en anledning till att det finns VIP-nummer finns, för att man ska kunna nå kunden i serviceyrke så att säga i servicevägnar, det är en grej. Mailuppgifter till exempel andra mail som skickas ut och lagras, inga lösenord ges ut härifrån över telefon eller något sådant, men lagrar man detta är det straffbart höll jag på att säga. Det kan nås av andra, det kommer i fel händer.

41. I: Innan jag lämnar frågan finns det någon annan risk du känner spontant finns utifrån verksamhetens sätt?
42. O: Du menar alltså från Företag S sida sett eller från?
43. I: Ja från Företag S sett blir det ju då
44. O: Ja men om någon gör såhär så känner jag väl mer eller mindre att den arbetaren inte tar sitt ansvar. Vi har fullt med lagringsmöjligheter här, dem tycker jag ska nyttjas. Följer man inte de rutiner vi har här då tycker jag att den personen borde bli visad att här lagrar vi och så vidare. Huruvida de har tänkt att göra med de anställda som inte följer det är inte på mitt bord så att säga. Men jag tycker som så, att så länge vi har så fina servers och fina lagringsmöjligheter som vi har här så tycker jag att det är framförallt internt det ska tas. Vi kan både koppla upp på mobilen och telefoner, vi kan ju koppla upp på plattor och datorer. Jag menar med den sidan sedd så tycker jag har vi så fina möjligheter så ska det inget annat nyttjas.
45. I: Så om jag har förstått dig rätt så är de två största riskerna som du ser är att känslig information kan läcka och företags varumärke tar stryk av det?
46. O: Ja det är ju bara det spontant nu. Företag S vi står för att vi ska vara professionella och säkerheten är a och o, det ska inte komma i fel händer.
47. I: Finns det regler och policy för hur man bör förhålla sig till privat molnlagring i tjänsten?
48. O: Ja det finns regler. Det finns en strikt företagspolicy, den ska följas.
49. I: Hur får man tag på den här informationen eller hur blir den tilldelad er anställda?
50. O: Den här finns tilldelad på vårt intranät. Den ska vara fullt uppdaterad om vad som vi får lov att göra och vad som vi inte får lov att göra.
51. I: Hur vet anställda om detta?
52. O: Anställda har fått introducerat när de kommer hit här att vi har ett intranät, bekanta dig med det och här har du all information som du behöver att veta. Samt även att det är så att vi har en hel del säkerhetsgrejer installerade på våra datorer som gör att vi inte kan installera alla möjliga program eller så att säga. Vi har som sagt en strikt företagspolicy som finns på intranätet och om du vill ha vidare information så är det bara att vända sig till våra IT-tekniker som du också kan få detta förklarat för dig.
53. I: Hur säkerställer man att detta når ut och att alla anställda tagit sig till detta?
54. O: Det görs stickprovskontroller
55. I: Hur följer ni dessa regler, det vill säga hur säkerhetsställer företaget att de här reglerna efterföljs?
56. O: Det är ingen fråga för mig.
57. I: Okej, det närmsta svaret där som du kan ge är kanske att det görs stickkontroller?

58. O: Det är såhär vi har fått en strikt företagspolicy och den här ska ni hålla. Vi ska ju följa denna företagspolicy just när vi nyttjar nätet och vi har ju ett x antal gånger fått lov att fråga om vi får lov att använda andra program som till exempel vi bad om att få byta webbläsare till Crome. De lyssnar väldigt mycket på oss för det är ju ändå vi som i slutänden sitter som slutanvändare. Vi har en dialog att det här fungerar bättre, de lyssnar på oss, och vi är ju slutanvändarna av produkten om vi använder det för att kunna arbeta effektivt så måste vi ju ha bra system kom klaffar med varandra. Sen om det gäller andra program om folk vill använda exempelvis Messenger eller ICQ eller vad nu. Det finns ju väldigt bra verktyg såsom Google Earth, där vi kan se mycket vart folk bor. Det är ju saker såsom Hitta.se, mäta sådan här saker, men det finns ju inget geografiskt sett som har fotograferat så bra och som kan underlätta när vi ska räkna ut vart en kund bor samt hur det ser ut. Vissa kartor är väldigt buggiga Google Earth är inte det. Det är exempelvis en applikation som jag har fått gå in och fråga om jag får lov att använda.
59. I: Använder du privattelefon eller annat enhet det vill säga dator eller surfplatta i tjänsten? Det vill säga att du äger den.
60. O: Nej jag har företagets telefon. Jag använder ingenting privat. Jag har ett privat abonnemang på telefonen som företaget äger. Jag använder mitt privata abonnemang när jag ringer på arbetstelefonen. Jag har en platta nämligen också som jag arbetar på. Denna plattan arbetar jag också på och där är mitt företags abonnemang och den ringer jag också ut ifrån. Sen speglar jag ju allting.
61. I: Vill du utveckla det, jag tror inte att alla användarna…?
62. O: Det jag arbetar med där alltså att jag speglar min användning med mail. Så det enda jag själv använder är företagsplatta, företagstelefon och jourdatorn där hemma äger företaget.
63. I: När du säger speglar, vad menar du då?
64. O: Mailen till exempel, jag har ju all mail på telefonen och på plattan så kör vi så kallat Imapp där så speglar jag detta. Det enda jag släpper till av data är min surf på min telefon som jag själv betalar för och det har jag själv bestämt att betala för. Så att så är det.
65. I: Har du någon molntjänst installerad på de här apparaterna som du använder?
66. O: Nej, det har jag inte
67. I: Och med det sagt du har inte aktivt installerat något nytt? Det som ligger, ligger där?
68. O: Ja man får ju säga att det ligger ju förinstallerade sådana här men de finns inga konton på dem. Det finns inget som synkas eller används. Det är till och med så pass att jag har gått in och avaktiverat de så att de inte går igång, jag har stoppat tjänsterna överhuvudtaget. Jag vill inte ha något som ligger latent i bakgrunden och som kan ta och sno information, sen finns det ingen information på telefonen eller på plattan som skulle kunna vara utan det är precis en uppkoppling till våra servers.
69. I: Har ni Wipe? Så att de remote wipar tänker jag?
70. O: Det har jag faktiskt ingen aning om, jag vet inte ens vad det är för något.
71. I: Det är att man från företagets sett kan tömma din telefon oavsett vart den är?
72. O: Nej det är ingenting vi har. Absolut inte.
73. I: Sista frågan blir ju vad erbjuder företaget för lagringstjänst och berätta mer om den?

74. O: Företaget har egna lagringsservers och det är inte mycket information som jag behöver lagra. Jag jobbar med allt realtid, jag har inte så att jag behöver dokumentera med foto eller sådana här saker. Men vad det gäller skrivelser, offertförfrågningar läggs det på och lagras på våra egna servers. Det gör jag antingen på jourdata, då lägger jag de direkt på min del av servern som jag har. Om ni i så fall undrar varför jag gör detta är för jag vet hur det fungerar, jag vet om att jag kommer på att jag gjorde en offertförfrågan på jobb men den ligger på jourdatorn där hemma då vet jag om att jag når den ändå. Om det är något jag inte är färdig med och måste komplettera med information, sparar jag den där och kan plocka upp den här på jobb istället.
75. I: Har du någon egen, något du själv tänker på angående detta, någon tanke som växt spontant av det vi diskuterat?
76. O: Jag tycker det är bra att det uppdagas med molntjänster och sådana saker. För att med tanke på de säkerhetsproblem som finns, jag menar inte problem på det viset utan att det endast är ett användarnamn och lösenord som behövs så tycker jag att det är en klen säkerhet på detta. Du kan sniffa det och få reda på lösenord.
77. I: Vad menar du med sniffa?
78. O: Jag menar om du kör med wifi till exempel, ja då kan de ju sitta folk och sniffa fram både användarnamn och lösenord.
79. I: Litteraturen säger att det är den största risken som molntjänster utsätts för.
80. O: Ja precis. Ett enkelt användarnamn och lösenord tycker jag inte är någonting som ska vara så lätt att få tillgång till. Jag tycker att det borde göras likt chip eller remote inloggning likt bankid, jag tycker det är vansinnigt enkelt säkerhet idag på detta här.
81. I: Som förbises för att öka tillgängligheten kanske?
82. O: Ja jag kan tänka mig att folk använder detta för att det är så enkelt, IT kunnandet är inte så högt i Sverige om jag säger så. Alla ungdomar har väl i allmänhet ett dåligt men ändå mycket bättre säkerhetstänk än vad äldre har. Man har ju sett skräckexempel där det sparas utan eftertanke och allt blir offentligt. Vi som nu kan detta med IT vet också vilka farhågor och riskzoner som finns. I och med att jag jobbar på ett företag som har rätt mycket med säkerhet att göra så är jag väldigt up to date med vad som är säkert och inte säkert, jag brukar faktiskt upplysa kunderna med att det där är inte säkert. Därför borde det bli mer säkert, med accessnyckel eller liknande.

6.3.7 Informant #6 - Avdelningschefen

1. I: Till vilken uträckning är det okej att få återge dig i den slutliga publikationen?
2. O: Det har jag inget problem med
3. I: Så roll, namn och företag är helt okej?
4. O: Ja
5. I: Jag hoppar rakt in i kärnfrågan här och det första gäller säkerhet. Som vi har diskuterat så har vi tittat på fenomenet hur det kommer sig att anställda lagrar yrkesrelaterad data i sin privata Dropbox eller motsvarande. Då är frågan till dig ser du några risker för verksamheten när anställda gör såhär?
6. O: Ja
7. I: Vill du gräva lite djupare på det? Vad ser du för risker?
8. O: Man sparar ju kundägd data och använder det på ett privat sätt som då åsidosätter vårt säkerhetstänkande mot kunden, vårt avtal mot kunden, som gör att det sedan kan användas på ett felaktigt sätt. Kunden måste kunna lita på att den information vi tillhandahåller, det som tillhör kunden, stannar här hos oss.
9. I: Och detta är extra känsligt för er förstår jag då ni erbjuder lagringstjänster till kunder? Risken som du ser med det då är om de i förtroende lagrar hos er, och om en anställd sparar information på sitt privata moln så ser du risken med att om det läcker så tar ert varumärke stryk? Ser du någon annan risk än att det påverkar ert varumärke?
10. O: Ja jag ser ju även att vårt kundregister lagras på ett annat sätt. Kundregistret och företagsregistret är ju ett värde för företaget, det är där vi har våra inkomstkällor och det vill man ju inte ska sparas eller komma i fel händer.
11. I: Så om jag förstår dig rätt, om det lagras på något annat ställe kan företaget inte ge den säkerheten som ni normalt sätt utlovar?
12. O: Ja
13. I: Innan jag går vidare till nästa fråga, ser du någon annan risk eller vad tänker du rent spontant?
14. O: Det är ju alltid risker med om säljare slutar och tar med sig information som gör att de kan konkurrera eller ta med kunder till andra företag. Det är ju inte säkert att de företagen väljer att arbeta med säljaren eller teknikern men det är ju en risk som finns. Det kan ju vara så att företaget har ett gott samarbete med just den personen.
15. I: Risken är då att om säljarna går till ett nytt företag då besitter de information om era kunder och blir då en direkt en konkurrent?
16. O: Ja de kan ju rikta erbjudande som gör att det blir mer fördelaktigt att välja den nya arbetsgivaren eller konstellation av säljande tjänst, utövande av teknik.
17. I: Finns det regler eller policy hur man ska förhålla sig till detta inom företaget?
18. O: Ja
19. I: Vill du utveckla det litegrann, om hur de ser ut på ett övergripande plan?
20. O: Ja det finns ganska många. Ett helt A4 där var och en anställd har fått signera hur vi använder data och informationen som vi kommer i kontakt med dagligen
21. I: Alla anställda får signera under den här policyn som säger att vi inte får använda en tredjeparts lagring så att säga?

22. O: Det står ju att informationen som vi kommer i kontakt med ska stanna här, att vi har tystnadsplikt. Att vi förvaltar och vårdar den informationen som rör sig inom bygget, mellan kund och kontakt hos oss.
23. I: Inom bygget menas då på Teleoffice ägda enheter och tjänster?
24. O: Ja på det sättet som vi säger till att det ska lagras på. Vi har lagringsutrymme för varje användare på våra servers. Vi har Sharepoint där vi lagrar gemensamt all information om kunder, kontakter och säljvärden. Det är där vi ska spara information som då rör arbete och tekniskt utövande. När det berör IT-avdelningen så sparas allt på en gemensam låst databas där rättigheter finns ställda vem som får använda vad och vart saker ska sparas.
25. I: Förekommer det privatägda enheter i tjänsten dvs. telefoner/paddor/datorer?
26. O: Ja
27. I: Omfattar policyn de här enheterna också för jag tänker exempelvis om jag har min privata telefon i arbetet och ringer upp en kund med min privatägda telefon är det något som policyn behandlar?
28. O: Det gör den inte. Nej den behandlar inte det så i princip kan du ringa från din privatägda telefon till en kund i ett jobbärende. Men de som har behov av att ringa i jobbet har en telefon tillgänglig via arbetet, så alla verktyg finns tillhands. Men jag vet att det förekommer till exempel om det är dålig täckning och att täckning finns hos annan operatör att teknikerna ringer till kund från sin egen telefon.
29. I: Följdfrågan blir ju om du ser någon risk med detta?
30. O: Risken där är ju vad jag kan se finns är ju att teknikern/säljaren frontar med sitt egna nummer, då kanske man blir störd eller headhuntad. Men det är mer att det skapar ett band till en telefon som inte är associerad med oss. Jag ser ingen annan uppenbar risk.
31. I: Med band menar du att man förenar den privata världen litegrann med…?
32. O: Nej jag menar mer den säljande personen.
33. I: Men ingen risk för företaget?
34. O: Nej inte samtalet i sig. Det bedömer inte jag i vilket fall.
35. I: Hur kommuniceras policyn till de anställda? Hur blir de informerade att bortsett från signeringen?
36. O: Vi har möten och genomgång om alla policyers och regler som gäller, varje år på ett gemensamt möte och sedan har vi grupp - och informationsmöten. Men även introduktionsmöte för alla nyanställda där vi går igenom de här punkterna. Det visste du inte?
37. I: Nej, men jag visste att det var mycket i görningen när jag ISO- certifierade mig här hos er för fyra år, det var då intranätet kom upp för mig, ni hade säkert haft det en längre tid men det var först då det kom för alla anställda. När vi stod inför ISO-certifieringen så hänvisades vi dit men det fanns inget som säkerhetsställde att jag hade tagit del av det, alltså att jag inte ska lagra mina arbetsärenden i mina privata lagringstjänster. Det stod säkert någonstans…
38. O: Men du tittade inte på det?
39. I: Nej, och jag visste inte vart jag skulle hitta det.

40. O: Från det att du slutade här så är det krävd signering att man har tagit del av de policys som finns. Alla har fått möjlighet att kunna läsa de, alla har fått möjlighet att titta på de och signera dem. Nu sitter vi och håller på med ett arbete som gör att vi förändrar inte vårt förhållningssätt men att vi skärper kraven på hur säkerheten ska hanteras och vilka privilegier en anställd har och inte har, möjligheter, rättigheter osv. Det är ett arbete som pågår.
41. I: Det är inte fullt utvecklat ännu?
42. O: Nej rör sig om några månader
43. I: Hur säkerhetsställer Företag S att era policys eller kanske regler snarare att de efterföljs?
44. O: Det här med att spara i privatmedier, egna sätt, egna cloud-tjänster eller dylikt. Efterlevnaden är ju svår att kontrollera om man gör det på ett sätt där man har baktankar med att göra ett och annat. Du kan ju skriva eller göra egna dokument och lyfta ut… men då är det ju riktigt utstuderat. Om detta hade uppmärksammats så hade ju det varit spårbart. Både användaren på datorn, våra regelbundna backups och vi har ju övervakning på varje klient i systemet. Vi kan ju titta på vad som har försiggått om vi vill göra det, om vi ser något i trafiken.
45. I: Är det något ni aktivt bevakar?
46. O: Ja
47. I: Skulle den identifiera om jag som anställd har lagrat exempelvis om jag skulle ringa upp en kund och skulle ut till kunden på eftermiddag, drar ner informationen i Dropboxen för att smidigt få tillgång till det i telefonen hos kunden?
48. O: Jag kan inte svara eller jag vet inte riktigt hur det fungerar helt tekniskt, där har jag människor som är intresserade och tillägnade för att bara utföra detta arbete. Men vi kan se väldigt mycket.
49. I: Ni kan se väldigt mycket men det görs inget aktivt för att kolla på just detta fenomen?
50. O: Nej
51. I: Det finns verktyg för att titta på det men det är inget aktivt som görs?
52. O: mm… vi litar på personalen men det går ju att se trender. Om det är data som av olika anledningar går på fel håll. Men vi har inte behövt att använda detta ännu. Men det finns alltid en risk.
53. I: Jag har inga mer frågor men är det något du rent spontant känner att du vill få sagt något som berör det vi pratat om? Eller något som du känner att detta kan man mer titta på?
54. O: Det ligger ju delvis i tiden för att det våra kunder, företag i synnerhet är ute efter och frågar hur vi sparar. Hur vi säkerhetsställer att deras data är säkert, själva företagsdata i sig är en sak och kundkontakterna, vad vi gör med kunden är en sak. Alla kommer ju inte åt den, det är ju låsta utrymmen, fysisk låsta utrymmen och rättigheter på hög nivå för att göra djupare manövrar med kundens data. Men kunderna är väldigt måna med att data ligger här, detta är varför man kanske väljer oss för att de vet att vi har fysisk lagring här och på två andra orter som inte är nämnda. Man vill inte spara i det gemensamma molnet.

55. I: Vill inte kunden nå det, vad ska man säga, på språng? Eller man har inte det behovet?
56. O: En del, vad ska man säga, bryr sig inte om data ligger i molnet och om servern står i Ryssland, USA eller i Europa. Men en del bryr sig och vet om att data blir en offentlig handling om man lämnar ut det och försöker därför fightas emot det, men kan inte hela vägen ut då de vet att det är så tekniken ser ut idag. Jag kan ju se problem med att folk lägger ut, alltså i cloudet…
57. I: Även om ni äger det menar du?
58. O: Nej! Jag menar att jag gjorde en sökning på en person som hade slutat på ett företag, jag ska inte nämna några namn. Jag gjorde sökningen på Google och fick upp namnet och då stod det ett annat namn i samband med det. Jag skulle ha kontaktuppgifterna på den första personen jag sökte så jag klickade på länken, personen jobbar i bankväsendet. Då öppnas en Googlekalender där det står vilka portkoder han har i Frankrike, vilka flighter som går till Frankrike, vem han spelar golf med. Helt öppet! Vilka bankkontakter han har och dylikt. Så det är en farlig trend, man ska vara väldigt medveten och vaksam över vad man gör. Det är ett hot och tyvärr flyttas ansvaret mer och mer över till den enskilda individen, det slutar ju med att man inte har något val man måste vara med.
59. I: Då menar du att du reglerar det för hårt så sänker du deras arbete eller man hindrar deras arbete genom att sätta för höga säkerhetsåtgärden?
60. O: Nej, jag tänker allmänt att användandet av molntjänsterna. Att kravställningen bör förändras, idag är det ju så att alla ska tillhöra molnet, lägg det där för det är lättillgängligt du kommer åt det överallt. Men vem kommer åt det, hur kommer de åt det? Var läggs det, vem kan se, vem får insyn? Man trycker godkänn på villkoren men vem äger data, vem äger bilderna? Om företaget som har molntjänsten säljs flyttas information med då, följer villkoren med?
61. I: Och tar du bort data, de har backup. Var ligger den?
62. O: Ja precis

Referenser

AlZain, M. A., Soh, B., & Pardede, E. (2013). A survey on data security issues in cloud computing: From single to multi-clouds. *Journal of Software, 8*(5), 1068-1078.

Angeles, S. (2013). 8 Reasons to Fear Cloud Computing. Retrieved 2015-04-20, 2015, from http://www.businessnewsdaily.com/5215-dangers-cloud-computing.html

Anonymous. (2012). BYOD Security Risks on the Rise. *Information Management, 46*(5).

Baldwin, R. (2014). How to protect yourself against hackers (or at least make it difficult for them). Retrieved 2015-04-20, 2015, from http://thenextweb.com/insider/2014/09/03/protect-hackers-least-make-difficult/

Berggren, L. (2008). Källkritik. Retrieved 2015-04-22, from http://www.lub.lu.se/skriva-referera/vaerdera/laes-mer-om-kaellkritik.html

Bourne, J. (2015). As cloud adoption continues to rise, fears over data breaches rise with it. Retrieved 2015-04-20, 2015, from http://www.cloudcomputing-news.net/news/2015/jan/09/cloud-adoption-continues-rise-fears-over-data-breaches-rise-it/

Caldwell, C., Zeltmann, S., Griffin, K. (2012). BYOD (Bring your own device). *American society for competitiveness. Indiana, United states*, 117-121.

Denscombe, M. (2009). *Forskningshandboken: för småskaliga forskningsprojekt inom samhällsvetenskaperna*: Studentlitteratur.

Gannett. (2012). Bring your own device. http://search.proquest.com.lib.costello.pub.hb.se/docview/1030105019

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications, 4*(1), 1-13.

Hensema, M. (2013). *Acceptance of BYOD among Employees at Small to Medium-sized Organizations.* Paper presented at the 19th Twente Student Conference on IT.

Jacobsen, D. I., Sandin, G., & Hellström, C. (2002). *Vad, hur och varför: om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen*: Studentlitteratur.

Kushida, K. E., Murray, J., & Zysman, J. (2011). Diffusing the cloud: Cloud computing and implications for public policy. *Journal of Industry, Competition and Trade, 11*(3), 209-237.

Lebek, B., Degirmenci, K., & Breitner, M. H. (2013). Investigating the Influence of Security, Privacy, and Legal Concerns on Employees' Intention to Use BYOD Mobile Devices.

Lennon, R. (2012). *Changing user attitudes to security in bring your own device (BYOD) & the cloud.* Paper presented at the Tier 2 Federation Grid, Cloud & High Performance Computing Science (RO-LCG), 2012 5th Romania.

Lindström, K. (2015). Skolorna struntar i problemen och satsar stenhårt på molnet. Retrieved 2015-03-26, 2015, from http://computersweden.idg.se/2.2683/1.609462/skolorna-satsar-stenhart-pa-molnet

Luis Diaz, A. (2011). Service Level Agreements in the Cloud: Who cares? Retrieved 2015-04-20, 2015, from http://www.wired.com/2011/12/service-level-agreements-in-the-cloud-who-cares/

Merrill, T. (2014). Cloud computing: Is your company weighing both benefits & risks?

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. *It Professional*(5), 53-55.

Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. *Network Security, 2012*(12), 5-8.

Niehaves, B., Köffer, S., & Ortbach, K. (2013). *The Effect of Private IT Use on Work Performance-Towards an IT Consumerization Theory.* Paper presented at the Wirtschaftsinformatik.

Patrizio, A. (2014). BYOC: Bring your own device is so 2012. Retrieved 2015-05-14, 2015, from https://powermore.dell.com/technology/byoc-bring-device-2012/

Putri, F. F., & Hovav, A. (2014). Employees´ compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory.

Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. *IEEE Internet Computing, 16*(1), 69-73.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology, 91*(1), 93-114.

Rong, C., Nguyen, S. T., & Jaatun, M. G. (2013). Beyond lightning: A survey on security challenges in cloud computing. *Computers & Electrical Engineering, 39*(1), 47-54.

Samson, T. (2012a). Dropbox fiasco serves as reminder of cloud-storage insecurity. Retrieved 2015-04-20, 2015, from http://www.infoworld.com/article/2617890/cloud-security/dropbox-fiasco-serves-as-reminder-of-cloud-storage-insecurity.html

Samson, T. (2012b). End-users admit ignorance of corporate cloud policies. Retrieved 2015-04-20, 2015, from http://www.infoworld.com/article/2616046/cloud-security/end-users-admit-ignorance-of-corporate-cloud-policies.html

Savvas, A. (2014, 2015-04-20). The benefits of public cloud computing. Retrieved 2014-04-20, 2015, from http://www.itproportal.com/2014/05/07/benefits-public-cloud-computing/

Scarfö, A. (2012). *New security perspectives around BYOD.* Paper presented at the Proceedings of the 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications.

Schalow, P. R., Winkler, T. J., Repschlaeger, J., & Zarnekow, R. (2013). *The Blurring Boundaries Of Work-Related And Personal Media Use: A Grounded Theory Study On The Employee's Perspective.* Paper presented at the ECIS.

Schmeiser, L. (2013). BYOD blues: What to do when employees leave. Retrieved 2015-04-20, 2015, from http://www.infoworld.com/article/2611171/byod/byod-blues--what-to-do-when-employees-leave.html

Searchcloudsstorage.techtarget. (2010). Cloud storage service-level agreements (SLAs) specify uptime guarantees but not data availability. Retrieved 2015-04-20, from http://searchcloudstorage.techtarget.com/feature/Cloud-storage-service-level-agreements-SLAs-specify-uptime-guarantees-but-not-data-availability

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications, 34*(1), 1-11.

Sullivan, S., Phifer, Lisa. (2013). Tablets and Smartphones in the Enterprise. Retrieved from TechTarget website: http://searchconsumerization.bitpipe.com/data/demandEngage.action?resId=1359128122_412

Symantec. (2012). The Myth of Keeping Critical Business Information Out of Clouds. Retrieved 2015-04-20, 2015, from http://www.symantec.com/content/en/us/about/presskits/b-myth-of-keeping-critical-business-information.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012_worldwide_CloudLaunch

Thurén, T. (2003). Sant eller falskt? Metoder i källkritik. *KBM:s utbildningsserie 2003:7*. https://www.msb.se/RibData/Filer/pdf/20180.pdf

Trustmarque. (2015). Research shows 40 cloud users using unsanctioned apps. Retrieved 2015-04-20, 2015, from http://www.trustmarque.com/research-shows-40-cloud-users-using-unsanctioned-apps/

Wagreich, S. (2013). Cloud Storage: 4 Legal Issues You Need to Know. Retrieved 2015-04-20, 2015, from http://www.inc.com/samuel-wagreich/the-4-things-you-must-have-in-your-contract-with-your-cloud-provider.html

Walker-Osborn, C., Mann, S., & Mann, V. (2013). to Byod or… not to Byod. *ITNow, 55*(1), 38-39.

Younis, M., & Kifayat, K. (2013). Secure cloud computing for critical infrastructure: A survey. *Liverpool John Moores University, United Kingdom, Tech. Rep*.