Uppsala universitet
Institutionen för informatik och media

# Framgång eller förfall?
## Utvecklingen, riskerna och potentialen av BYOD

*Alexander Facklam & Emil Berglund*

Kurs: Examensarbete
Nivå: C
Termin: VT-16
Datum: 25/5-16

## Sammanfattning:

Uppsatsen undersöker fenomenet Bring Your Own Device (BYOD), dess för- och nackdelar samt hur riskerna BYOD medför kan hanteras. För att uppnå detta har en litteraturstudie genomförts. Denna kompletteras av en enkätstudie på Stockholms Läns Landsting och tre intervjuer på Uppsala Kommun med målet att se hur dessa organisationer hanterar BYOD. Arbetet ger en djup insikt i BYOD olika aspekter och visar även på hur de risker som uppkommer kan hanteras.

## Nyckelord:

BYOD, Bring Your Own Device, Policy, IS-Säkerhet, Digitala hot, Riskhantering

# Innehållsförteckning

# 1. Inledning

I detta kapitel presenteras bakgrund, problembeskrivning, frågeställning, avgränsning och slutligen disposition.

## 1.1 Bakgrund

Dagens teknik går framåt med stormsteg och ständigt utvecklas ny hård- och mjukvara som används i nästan alla organisationer och företag dagligen. Utvecklingen av mobiltelefoner och surfplattor är inget undantag och ständigt kommer nya innovationer som gör dessa enheter kraftigare och mer flexibla. Bring Your Own Device (BYOD), som är den tekniska termen för användandet av privatägda enheter inom arbetet är ett relativt nytt fenomen som fått allt större fäste i och med att en majoritet av befolkningen har tillgång till någon form av mobil enhet. Den exakta utbredningen av mobila enheter är svår att kartlägga men har exploderat under de senaste årtiondet. Statistiska centralbyrån (SCB) visar i en rapport från första kvartalet 2014 att 70% av de tillfrågade i deras undersökning "*Privatpersoners användning av datorer och internet 2014*" svarade ja på frågan om de någon gång använt en mobiltelefon av något slag för att koppla upp sig mot internet. I åldersgruppen 16-44 år stiger denna siffra ytterligare till cirka 85%. Studien ställer inte frågan direkt om hur stor del som äger en smartphone men denna siffra visar på hur enormt uppkopplat samhället är. (SCB, 2014).

Det ökande användandet av mobila enheter leder till en ökad digital sårbarhet för både organisationer och privatpersoner. Det finns en utbredd mental bild av att mobiltelefoner och surfplattor inte kan utsättas för hackning eller få virus, detta är inte alls sant. Antivirusjätten Kaspersky uppgav i sin rapport för 2013 att de under året upptäckt 143 211 nya skadliga program som hade mobila enheter som mål. Under samma period upptäckts runt tio miljoner unika attacker mot dessa enheter i form av skadliga installationsprogram. (Securelist, 2014) Dessa hot kan i mångt och mycket bekämpas med hjälp av antivirusprogram och ett säkert förhållningssätt hos användaren. För organisationer som använder BYOD blir tydliga regler och policys för användandet av mobila enheter oerhört viktiga verktyg för skydd, då traditionella skydd så som brandväggar inte är anpassade för att upptäcka hot som sprids internt i ett IT-system, vilket kan ske om en virusdrabbad smartphone kopplas upp mot systemet. Utbildning av personal inom säkerhetsarbetet bör därför prioriteras högt men så är inte alltid fallet.

En undersökning 2014 gjord av Enterprise Management Association visade att upp till 56% av anställda inte hade genomgått en utbildning inom IT-säkerheten i deras respektive organisationer. Studien berörde 600 anställda inom olika organisationer och även om studien gjordes utanför Sverige så visar den på en global problematik. Vidare pekar studien även på att 58% av de tillfrågade lagrar känslig information på sina privata enheter och hela 59% svarade att de lagrat liknande information i någon form av molntjänst. (Softpedia News, 2014)

## 1.2 Problembeskrivning

I dagsläget pågår ständigt en debatt kring om BYOD bör sättas i system eller inte. Fördelarna är många med att låta anställda använda sina privata enheter inom jobbet. Inte bara finns det en uppsjö av exempel som visar att produktiviteten kan öka drastiskt och de anställdas flexibilitet och tillgänglighet skjuter också i höjden. Övriga fördelar med att använda sig av BYOD inom organisationen är kostnadsbesparingar men även en ökad tillfredsställelse hos de anställda i och med det personliga valet av enheter (Evans, 2013).

Dessa fördelar både för de anställda som individer och för organisationen, är av oerhört stort intresse. I dagens informationssamhälle rapporterar medier ständigt om dataintrång, virus, trojaner och kapade enheter. Globalt kostar säkerhetsrelaterade incidenter 100-tals miljarder dollar och av dessa kan upp emot 75% härledas till fel inom organisationen och mänskliga fel (D´Arcy m.fl. 2009). Trots alla dessa uppenbara risker med dåligt skyddade enheter finns det bevisligen fördelar med BYOD som är så pass givande för nutidens organisationer att de på många håll tar den risken.

Riskerna med att använda sig av BYOD inom en verksamhet är dock långt ifrån obefintliga. Digitala hot i form av bland annat skadlig kod, överbelastning- och hackerattacker är en realitet inom hela IT-sektorn. BYOD för med sig en helt annat typ av problematik. Brandväggar, VPN-tunnlar och dubbla nätverksuppkopplingar ger ett effektivt skydd mot så kallade externa och traditionella hot men hjälper väldigt lite i de fall då hotet finns internt. Att på närmast daglig basis kontrollera en hel arbetsstyrkas privata enheter efter intrång kräver enorma resurser och att låta den existerande IT-avdelningen sköta säkerheten på dessa enheter utöver organisationens egna, är helt enkelt orimligt. Då konventionella skyddsmetoder mot yttre hot inte hjälper, läggs istället ansvaret för säkerheten på den anställda vilket i sin tur ger nya problem att hantera, om än på ett mer administrativt sätt.

En stor del av de hot organisationer ställs inför går att undvika med hjälp av ett medvetet och aktivt säkerhetstänk. Organisationernas uppgift blir därmed att sätta upp en policy och därefter kommunicera vidare denna samt rådande säkerhetsrutiner till berörd personal. Detta arbete är på papperet enkelt, men i verkligheten är på många håll medvetenheten kring dessa policys och rutiner inte förankrade ordentligt i arbetsstyrkan, vilket kan få katastrofala följder för säkerhetsarbetet. Siffrorna varierar men upp emot 50-75% av alla incidenter inom IT-relaterade system anses kunna härledas till den “mänskliga faktorn”.(*D´*Arcy m.fl, 2009)
Det är därmed, utan motsvarighet, den enskilt största riskfaktorn för ett modernt IT-system.

Att användarbasen är den enskilt största riskfaktorn är i sig inte något nytt, och problematiken blir extra framträdande när det kommer till BYOD. Detta antagande grundar sig i den tidigare nämnda problematiken med att säkerhetsarbetet till stor del vilar på användarbasens förmåga att följa uppsatta regler och policys. Hanteringen av denna riskfaktor bygger i sin tur på ett gediget arbete när det kommer till utformningen av just dessa styrande dokument. Det stora hindret för införandet av en lyckad säkerhetspolicy ligger dock inte nödvändigtvis i själva utformningen utan i hur denna kommuniceras då en stor del av risken med just BYOD är att uppsatta regler

ignoreras. Ytterligare en förklaring till att BYOD trots riskerna blir allt vanligare kan vara den ökande utbredningen av handhållna enheter i samhället och den potential de har.

Digitaliseringen av gemene mans vardag sker i ett ständigt ökande tempo och smartphones och surfplattor är en självklarhet för många. Trots detta har det tekniska intresset och kunnandet inte hängt med i samma tempo och det anses vara en betydande säkerhetsrisk i "slutna" system och då ännu mer i de fall där BYOD tas med i beräkningen. (Pillay m.fl, 2013)

## 1.3 Frågeställning

Utifrån den ovanstående problembeskrivningen blev frågeställningen till denna uppsats: *Vilka är för-respektive nackdelarna med BYOD?* samt: *Hur kan riskerna med att implementera BYOD hanteras för att upprätthålla en god IT-säkerhet?*

## 1.4 Avgränsningar

Uppsatsen avgränsades till att behandla BYOD och vilken påverkan fenomenet kan ha på en organisation, främst ur ett säkerhetsperspektiv. Detta för att både informationssäkerhet och BYOD är två aktuella ämnen och starkt relaterade till varandra. De digitala hoten behandlades på så vis att de enskilda varianterna av skadlig kod (trojaner, virus, phishing med mera) inte inte behandlades som separata delar utan slogs ihop till samlingsnamnet skadlig kod. Avgränsningen i den empiriska studien gjordes på så sätt att endast två olika organisationer kontaktades. Värt att påpeka är att arbetet är avgränsat till att behandla den påverkan BYOD har för en organisation och inte för den enskilda individen, faktorer så som ökar eller minskat välmående är därmed inte medräknade.

## 1.5 Disposition

Kapitel 1 inleder uppsatsen med bakgrund, problembeskrivning och frågeställning, vidare förklarar och motiverar kapitel 2 vilken metodik som används i datainsamling och analys av denna. Kapitel 3 innefattar den teoretiska bakgrunden i form av en litteraturstudie kring BYOD medan kapitel 4 presenterar den enkät och de intervjuer som genomfördes i den empiriska studien. Uppsatsen avslutas med en analys där teori och empiri kopplades samman i kapitel 5 och den information som genererades sammanfattas och diskuteras i kapitel 6 följt av källförteckning och bilagor i kapitel 7 respektive 8.

# 2. Metod

I detta kapitel presenteras forskningsstrategi, forskningsparadigm, datainsamlingsmetodik, metod för dataanalys och generaliserbarhet.

## 2.1 Forskningsstrategi

Uppsatsen är en beskrivande fallstudie med en blandmetod där fallet var fenomenet BYOD. Då tanken med en fallstudie är att få en så djup kunskap som möjligt är det vanligt att man använder flera olika datainsamlingsmetoder, det har därför utförts tre kvalitativa intervjuer och en kvantitativ enkätstudie inom två stora offentliga organisationer. Datainsamlingen bygger på den teoretiska bakgrundsforskningen som har utförts.

Med fallstudie menas en djupgående studie inom ett specifikt ämne, i detta fall fenomenet BYOD. För att kunna anses vara en korrekt fallstudie får ingen påverkan på miljön där studien utförs i ske, ämnet ska kunna observeras i sitt naturliga tillstånd. Det är även viktigt att man fokuserar på komplexiteten av relationer och processer, och tittar på hur dessa är sammankopplade, istället för att fokusera på enskilda faktorer. (Oates, 2006, s.135-136)

Oates visar på tre olika tillvägagångssätt för hur en fallstudie kan utföras: undersökande studie, beskrivande studie samt förklarande studie. Denna uppsats är en beskrivande studie då syftet är att sammanställa en detaljerad analys av ett fenomen och dess sammanhang, och även hur olika individer uppfattar det som har utförts. (Oates, 2006, s.136-137)

## 2.2 Forskningsparadigm

Ett paradigm är en samling gemensamma antaganden, resonemang och funderingar kring en världsbild. Det finns huvudsakligen tre olika filosofiska paradigm som alla har ett eget sätt att behandla världsbilden. Dessa paradigm är Positivism, Interpretivism och Kritiskt paradigm. (Oates, 2006)

Då uppsatsen är en studie som ser närmare på vilken kunskap om informationssäkerhet individer har inom en organisation har både intervjuer och en enkätstudie utförts har det interpretivistiska paradigmet använts.
Här inriktar sig forskningen framförallt på sociala aspekter där fokus ligger på beteenden och hur människor ser på omvärlden och försöker dra slutsatser efter detta. Detta paradigm är mer öppet än positivism då resultaten av en interpretivistisk studie är osäkra och kan variera beroende på vilka parametrar studien grundar sig på, här får författarna även inkludera egna tankar och uppfattningar om forskningen. (Oates, 2006, s.261-263)

## 2.3 Datainsamlingsmetodik

Då syftet med denna uppsats var att få en så djup kunskap inom fenomenet BYOD som möjligt beslutades det att utföra både en kvalitativ och en kvantitativ datainsamling, dessa presenteras nedan.

### 2.3.1 Kvalitativ data

Målet var att besöka en större organisation, gärna offentlig då författarna via egna åsikter ansåg att en sådan typ av organisation bättre skulle stämma överens med det bristande säkerhetsarbete som delvis skapar problematiken bakom BYOD. Kontakt skapades därför med Uppsala Kommun vilket ledde till ett inbokat möte för att hålla intervjun. Uppsala Kommun styrs av politiker som kommunens medborgare tillsammans har röstat fram. Kommunen har hand om en stor del av den samhällsservice som finns i Uppsala, så som skolor, omsorg och sjukhus. Kommunfullmäktige är det högsta beslutande organet och hanterar de viktigaste frågorna i Uppsala. De beslutar bland annat om vilka policys som ska tillkomma och uppdateras, och även frågor som att välja ledamöter och ersättare till kommunens nämnder, styrelser och till kommunrevisionen. (Uppsala kommun, 2016)

Målet med dessa intervjuer var att få en inblick i hur det dagliga arbetet såg ut i samband med användandet av BYOD inom kommunen. Ett annat mål med intervjuerna var även att få svar på hur kommunens IT-policys såg ut, hur de arbetar för att utbilda och informera sina anställda om hur de använder egna privata enheter på ett säkert sätt inom arbetet, och vilka risker och hot som finns i samband med BYOD.

Den första intervjun som ägde rum på kommunen var av semistrukturerad karaktär då intervjufrågorna var öppna. Tanken var att intervjun skulle fortskrida av sig själv och på så vis fylla frågor som eventuellt kunde ha förbisetts vid utformandet av intervjufrågorna. När intervjun utfördes användes en diktafonapplikation i en av författarnas mobiltelefon för att spela in hela intervjun och intervjun dokumenterades även på en av författarnas datorer. För att följa upp dessa intervjuer utfördes även två intervjuer via telefon med slumpvisst utvalda medarbetare på kommunen. Dessa var fullt strukturerad där alla frågor i förväg var bestämda så att svaren blev klara och lätta att sammanställa. När intervjuerna utfördes sammanställdes dessa på en av författarnas datorer. (Oates, 2006, s.173-176)

### 2.3.2 Kvantitativ data

Tanken var att även utföra en enkätstudie inom Uppsala kommun, men det fanns inte möjlighet till det eftersom kommunen samtidigt utförde ett stort digitaliseringsarbete vilket gjorde det svårt att förmedla ut enkäten till en tillräckligt stor svarsgrupp. Kontakt skapades istället med Stockholms läns landsting (SLL) då dessa organisationer har en liknande uppbyggnad och organisering. Landstinget finns, precis som Uppsala kommun, till för länets invånare och är till för att erbjuda samhällsservice. De mest övergripande delarna de ansvarar för är hälso- och sjukvård, kollektivtrafik och regionplanering, och de bidrar även till kulturen i länet. Landstinget

är en organisation som styrs av utvalda politiker som byts ut vart fjärde år och röstas fram av länets invånare. Organisationen finansieras till största del via landstingsskatten, alltså skatteintäkter från medborgare, och det är landstingsfullmäktige som beslutar om hur stor skattesatsen ska vara. (Stockholms läns landsting, 2016)

Målet med att hålla denna enkätstudie var att utöver de utförda intervjuerna på Uppsala kommun få en ännu bredare bild över hur arbetet med BYOD ser ut på de större organisationerna i Sverige och för att lättare kunna se frågan ur ett större perspektiv. Kontaktperson på SLL var enhetschef May Blom som hjälpte till att förmedla ut enkäten inom landstinget. Inom Hälso -och sjukvårds förvaltning arbetar 650 personer, av dessa fick 125 ta del av enkäten, varav 75 anställda svarade på enkäten.

Enkäten skapades med hjälp av Googles Forms och bestod av 12 stycken frågor med fördefinierade svar där respondenterna fick välja mellan olika fördefinerade alternativ (Bilaga 8.3).
Enkäterna var helt anonym för att skydda deltagarnas identiteter, och för att få så sanningsenliga svar som möjligt.

## 2.4 Metodik för dataanalys

### 2.4.1 Kvalitativ dataanalys

Efter att intervjuerna genomförts transkriberades och sammanfattades dessa till empirin. Denna sammanställning låg sedermera till grund för utvecklingen av enkäten. Data från intervjuerna jämfördes med tidigare forskning om policys och utbildning inom säkerhet för att se hur väl de förhöll sig till varandra inom kommunen. Den semistrukturerade intervjun jämfördes också med de två telefonintervjuer som utförts för att se hur bra svaren stämde överens.

### 2.4.2 Kvantitativ dataanalys

För att analysera data som enkäten producerade sammanfattades och sedermera presenterades denna i form av tårtdiagram. I och med att enkäten bygger på en nominal datainsamlingsmetod fanns det bara ett sätt att utföra analysen på vilket var efter frekvens, alltså hur stor andel som svarade med ett visst alternativ (Oates, 2006, s.223). I analysen jämförs även datan med den forskning som sammanställts utifrån teorin. Tillägget awesometable i Googleforms användes för att kunna göra urval efter svarsalternativ.

## 2.5 Generaliserbarhet

Den teoretiska bakgrunden är i hög grad generaliserbar då för- och nackdelarna samt hur risker med BYOD kan hanteras är aktuella för en allt större grupp organisationer ju mer fenomenet sprids.

Den empiriska forskningen som gjorts behandlar två specifika instanser och dess generaliserbarhet är därmed inte lika hög. Liknande organisationer bör kunna använda sig av materialet då frågeställningen och problematiken som tas upp inte är unik för de två organisationer som undersökts.

# 3. Teoretisk bakgrund

Detta kapitel ger inledningsvis en introduktion kring hur begreppet BYOD hanteras i litteraturen för att sedan redogöra för de positiva och negativa aspekterna av att införa BYOD. Efter att detta hanterats fortsätter kapitlet med en beskrivning av hur arbetet med att upprätthålla en god informationssäkerhet bör utföras i kontext med BYOD.

## 3.1 Definition av BYOD

Tidigare forskning som behandlar BYOD har visat sig ha olika bild av vad begreppet faktiskt innefattar. Pillay m.fl. (2013) ger förklaringen: "BYOD är en strategi som tillåter anställda, handelspartners och övriga användare att använda sig av personligt utvalda och införskaffade klient-enheter för att utnyttja organisationens applikationer samt komma åt data".

Detta synsätt återfinns i flertalet av de källor som använts och ger en mycket övergripande, om än förenklad bild, av vad begreppet BYOD innefattar. Enhetligt för alla författare är att smartphones, surfplattor och laptops anses tillhöra BYOD-begreppet. Gällande fjärråtkomst från stationära enheter finns det även där en konsensus i den litteratur som står till grund för detta arbete att det räknas in i begreppet BYOD trots, att data inte hanteras av de enheterna i sig själva. Hur långt utifrån de mer givna privatägda enheterna BYOD sträcker sig varierar däremot mellan olika experter inom området och antalet gråzoner är många. Morrow (2012) resonerar exempelvis att en av riskerna med att använda sig av BYOD inom en organisation är den bristande kontrollen över mail-konton, att en mängd olika enheter har tillgång till känslig data. Utifrån detta synsätt inkluderas även fjärråtkomst till mailapplikationer så som Outlook till BYOD.

I motsats till vad begreppet anger så behöver BYOD-enheter inte vara inköpta av en privatperson utan dessa kan även vara enheter som en organisation köper in till sina anställda med tanken att de ska kunna användas utanför arbetsplatsen (Romer, 2014).

BYOD som begrepp inom IT har därmed visat sig vara mer mångfacetterat än vad en första anblick kan ge sken av. Gråzonerna är många och ökar komplexitetsgraden av att använda sig av BYOD inom en organisation. Gemensamt är dock att alla innefattar enheter där organisationen i sig självt inte har förstahandskontrollen över de enheter som används för att komma åt dess interna system och den data de innehåller.

## 3.2 Utbredning av mobila enheter

Antalet mobila enheter i omlopp växer ständigt. Gartner (2016) anger att runt 2,4 miljarder datorer och mobila enheter levererades globalt under 2015 och uppskattar att den årliga siffran kommer att stiga med cirka 150 miljoner enheter fram till 2018. Av de som levererades under 2015 var 1,9 miljarder mobiltelefoner av olika slag, en klar majoritet av dessa smartphones. Enligt tidigare forskning av Becket (2014) beräknas närmare 65% av dessa användas inom BYOD i någon utsträckning.

Dessa siffror i sig visar på ett tydligt fenomen:

Samhället blir allt mer digitaliserat, och det blir allt mer mobilt. Detta lägger i sin tur press på arbetsgivare som tvingas anpassa sig för att kunna attrahera och behålla kompetent personal, som annars riskerar att välja andra företag ifall de anser att de inte har den frihet de är vana vid när det kommer till valet av arbetsverktyg (Thomson, 2012).

Statistiska Centralbyrån (SCB) utförde i slutet av 2014 en undersökning som visar att 99% av svenska invånare i åldrarna 16-54 år har tillgång till internet på daglig basis. Av dessa har 77% tillgång via bärbara datorer och 74% via smartphones. Vidare uppgav 50% av de tillfrågade att de använt sig av någon form av molntjänst för lagring av data. Dessa siffror ger en tyngd till Thomsons teorier och dess bakomliggande forskning. I en värld där främst de yngre generationerna ständigt har tillgång till all data de kan vilja ha så blir det svårt för organisationer att låsa ner sina system utan att mötas av opposition från sina anställda. När det gäller antalet enheter per anställd blir faktumet ännu tydligare. Studier bland företag i USA som anammat BYOD som arbetssätt visar att varje enskild anställd i snitt har 3,5 mobila enheter, privat köpta eller tillhandahållna av organisationen de arbetar för. Hur denna mängd bör hanteras råder det även delade meningar om, vilket kommer behandlas i senare avsnitt.

## 3.3 Fördelar med BYOD

### 3.3.1 Produktivitet och flexibilitet

Implementering av BYOD som arbetssätt inom en organisation har visat sig ha positiva följder på produktiviteten hos de anställda. Detta är främst en följd av en ökad flexibilitet när det kommer till möjligheten att komma åt den data som krävs för att kunna utföra arbete utan att fysiskt behöva befinna sig inom organisationens lokaler. Denna förhöjda grad av flexibilitet möjliggör även för de anställda att arbeta utanför arbetstid, något som effektiviserar främst administrativa uppgifter (Pillay m.fl, 2013).

IT-jätten Cisco visar i en undersökning innefattande över 2400 användare i sex olika länder att produktiviteten i många fall ökar dramatiskt när personalen har tillgång till användningen av privata enheter. I snitt sparade varje anställd in mellan 37 och 81 minuters arbetstid per vecka men undersökningen visade även att 36% av de tillfrågade BYOD-användarna var "hyperproduktiva" och sparade upp till fyra timmar i veckan genom att kunna effektivisera sitt arbete. Dessa siffror visar på den potential som BYOD har när det kommer till produktivitet och även innovation. Av de tillfrågade upplevde 53% att deras effektivitet hade ökat tack vare nya arbetssätt utan inblandning av den centrala ledningen. En studie från 2013 av Dell visar på att organisationer som anamat BYOD upplever upp emot 74% ökning i produktiviet (TIMR, 2016). Vidare anser Cisco (2013) att en stor majoritet av organisationerna som tog del i undersökningen inte utnyttjade den fulla potentialen av BYOD, detta kommer tas upp mer ingående under avsnittet rörande implementering av BYOD.

Att själv kunna anpassa verktygen som används efter arbetsuppgiften är också en stor fördel när det kommer till användningen av BYOD. Där exempelvis bärbara datorer använts tidigare för att få med nödvändig data, har tillgången till surfplattor visa sig vara ett smidigare verktyg som

underlättar (Pillay m.fl, 2013 ). Uppemot 80% av anställda uppgav redan 2012 att de på ett eller annat vis använde sina privata enheter i jobbsammanhang, av dessa lagrade 47% jobbrelaterad information på sina privata stationära datorer (Morrow 2012). Användandet av stationära datorer har förvisso sjunkit de senaste åren i och med utbredningen av allt snabbare och överkomligt prissatta bärbara datorer men siffrorna ger trots det en fingervisning om att en stor del inte bara har, utan även efterfrågar möjligheten att kunna arbeta på distans med åtkomst till sin arbetsdata. Dessa siffror bekräftas av den ovanstående studien Cisco genomförde. De fann att 49% föredrog att arbeta från sina egna enheter, 30%, föredrog företagets tillhandahållna och 20% hade ingen föredragen plattform. Indien och Kina toppar statistiken med 63% respektive 66% i fördel för privata enheter (Cisco 2013). Just denna efterfrågan är något som bland andra Thomson (2012) fäster stor vikt vid när det gäller BYOD och varför han menar att ansvaret att anpassa sig ligger på arbetsgivaren och inte i första hand på de anställda.

Detta synsätt utgår ifrån att det moderna samhället har blivit uppkopplat till den grad att åtkomst till all information gemene man kan tänkas vilja ta del av, har blivit en naturlig del av vardagen, en resurs vars bortfall inte accepteras. Med ett sådant perspektiv breddas flexibilitetsaspekten, det handlar inte längre om att kunna utföra arbete på ett flexibelt sätt under flexibelt satta arbetstider, utan den teknologiska revolution mobila enheter och framförallt smartphones medfört. Thomson (2012) menar att denna revolution inte är något företag och organisationer kan bortse ifrån eller för den delen förhindra.

### 3.3.2 Ekonomi

Effektivare arbetssätt och i fortsättningen en ökad produktivitet leder i många fall till ökade inkomster för organisationer som anammar BYOD. Den stora ekonomiska aspekten för många är dock besparingar. I de fall där organisationen själv tillhandahåller enheter för de anställda försvinner besparingarna som kan göras genom att personalen står för inköpskostnaden. Att stå för en sådan investering kan vid första anblick avskräcka, men de ekonomiska besparingarna går utanför de rena inköpen av enheter. Underhåll, uppgraderingar och support av enheter är alla aspekter som, beroende på implementering, avtal med mera, kan leda till betydande besparingar (Pillay m.fl, 2013). Viktigt att ta med här är att Pillay med kollegor även menar att de ekonomiska fördelarna rent materialmässigt inte alltid slutar i en enorm vinst då ny infrastruktur och säkerhet kring denna i många fall behöver installeras för att kunna hantera det förändrade informationsflödet. De initiala ekonomiska fördelarna vid implementering av BYOD är således oerhört svåra att beräkna och varierar kraftigt mellan olika organisationer. För att se de ekonomiska fördelarna av BYOD behöver främst den ökade produktivitetens potential undersökas (Cisco 2013).

### 3.3.3 Ökad motivation inom personalstyrkan

Redan i det tidigare avsnittet gällande utbredningen av mobila enheter fastställdes att smartphones, surfplattor och andra typer av mobila enheter i alla dess former har kommit att bli en naturlig del av vardagen. Att använda sig av sina egna verktyg och applikationer spelar roll även inom arbetslivet, som går allt mer ihop med det privata för många. Att kunna välja sina

verktyg ser många som en stor fördel när det kommer till arbete. Vana, smak och ett visst mått av känsla av individuell påverkan är alla aspekter som kan tillfredsställas genom att använda BYOD och leder i sin tur till en mer motiverad arbetsstyrka (Thomson, 2012; Pillay m.fl, 2012).

## 3.4 Risker och nackdelar med BYOD

### 3.4.1 Komplexitet

Att gå ifrån ett stängt system endast innehållande företagsägda och kontrollerade enheter till att öppna för enheter som ägs privat av de anställda, eller i vart fall får användas för privat bruk, ställer helt andra krav på hur en organisation måste hantera sina digitala system. I dagsläget är många system utvecklade för att användas på en viss typ av hård- och mjukvara och risken finns att flertalet applikationer inte fungerar korrekt, om alls, i de fall där en ny plattform introduceras. En grundläggande satsning för att lyckas med införandet av BYOD är att se över säkerheten i de applikationer som används, se till att dessa går att komma åt oavsett vilka enheter som används samt bygga upp den bakomliggande infrastrukturen i systemen för att kunna hantera den ökade trafiken utifrån (Pillay m.fl, 2013).

Denna ökning lägger ett ökat ansvar på organisationens IT-avdelning. Även om vissa ansvarsområden, såsom införskaffande av enheter och support av dessa försvinner, så kommer avdelningen kräva ökade resurser för att se till att systemet är och förblir anpassat till den nytillkomna vågen av enheter. Användningen av BYOD leder även till att arbete inte nödvändigtvis sker under traditionell arbetstid vilket ställer ytterligare krav på systemet. Uptime och redundans i systemet blir viktigare då avbrott i informationsflödet mellan systemets användare och den data det lagrar kan få betydligt mer omfattande konsekvenser för den dagliga verksamheten (Thomson, 2012). Även juridiskt och etiskt kan användningen av BYOD bli problematisk. Misstankar om brott eller försummelse av en anställd kräver en bred kartläggning av användarmönster för att se vart datan användaren hanterat kan ha tagit vägen. I en stängd miljö där enheterna som används är organisationens egna tillgångar är detta sällan ett problem men när enheterna som använts är privat egendom riskerar en intern undersökning att hamna i legala gråzoner. Utan påskrivna avtal som ger arbetsgivaren rätt att gå igenom dessa enheter kan dessa förbli oåtkomliga utan hjälp av myndigheter i de fall då endast misstanke om brott finns. Dessa fallgropar går att komma runt med tydliga anställningsavtal men beslagtagning av enheter kan upplevas som väldigt påträngande och kränkande för den enskilda individen trots att det är legalt och kontraktsmässigt godtagbart (Beckett 2014).

### 3.4.2 Förlust av kontroll

En av de stora farorna med att använda sig av BYOD är den förlust av kontroll det för med sig. Traditionellt sett har en organisation haft full kontroll över enheterna i de system som används, vilka applikationer som installeras och vilka externa källor som går att komma åt. I och med att stationära datorer allt mer ersatts av bärbara försvinner redan här en del av kontrollen över vilken digital nätverkstrafik som tillåts då dessa enheter ofta används utanför organisationens brandväggar. Däremot bibehåller organisationen fortfarande kontrollen över vilken hårdvara som används, vilken mjukvara som får installeras och i många fall installeras även mjukvara för att

genom fjärrstyrning kunna hantera enheten, uppdatera programvara och radera data i fall av förlust. När kontrollen över enheten övergår till användaren själv förflyttas även ansvaret för säkerheten. (Pillay m.fl. 2013; Tokuyoshi, 2013)

Förlusten av kontroll är ett problem som måste hanteras via nya arbetssätt. Utan att säkerhetsställa att känslig data och enheterna de lagras på är skyddade blir hotbilden snabbt ohållbar. Tokuyoshi menar på att *"Utan skydd på plats för att skydda nätverkstrafiken är informationen lika säker som ett vykort, öppen att läsa för alla som tar sig tid att ta en titt"*(Tokuyoshi, 2013, s.12). Citatet visar på hur oerhört viktigt det är för en organisation som behandlar känsliga uppgifter att de trots användning av BYOD håller kvar kontrollen över sin data och även de enheter som har åtkomst till denna.

En lätt översedd aspekt av kontrollen över data gäller molntjänster. Som tidigare nämnts använder sig en stor del av anställda av olika typer av molnbaserade filtjänster för att lagra jobbrelaterat material. Förutom den direkta spridningen av data till lagringsplatser utanför organisationens egna system så kan användningen av sådana tjänster riskera att organisationen förlorar rättigheterna till sin egna information då det i många fall anges i användarvillkoren att allt som lagras i en molntjänst får användas av tjänsteleverantören. Det är därför oerhört viktigt att grundligt gå igenom användarvillkoren och därefter se över vilken typ av information som bör och tillåts att lagras i molnet. (Romer, 2014) Romer menar även att de flesta molntjänster är utvecklade för privat bruk snarare än för företag, vilket kan leda till att säkerheten (på samma sätt som med mobila enheter) inte är den största fokuspunkten utan användbarhet och flexibilitet kommer före. Ett exempel som Romer tar upp för att visa detta är att molntjänsten Dropbox under fyra timmar 2012 lyckades stänga av lösenordskravet för sina användare, ett scenario som riskerade att låta mängder av känslig information bli åtkomlig för obehöriga.

### 3.4.3 Intrång och skadlig kod

Intrång och spridning av skadlig kod har traditionellt bekämpats med hjälp av brandväggar och andra typer av yttre "skal" som skydd. Dessa är väldigt effektiva när det kommer till att kontrollera in- och utgående trafik för ett system men ger inte alls samma grad av skydd mot skadlig kod som tagit sig in i systemet. När koden väl tagit sig in i systemet kan dessa skal i viss mån analysera utgående trafik och identifiera misstänksam kommunikation men besitter inte förmågan att oskadliggöra hotet.

I och med införandet av BYOD riskerar detta skal att bli i stort sätt verkningslöst. Företagsenheter som används utanför organisationens slutna system och i ännu högre utsträckning privatägda enheter, löper en större risk att infekteras av skadlig kod. När dessa sedan används innanför organisationens yttre skal kan i värsta fall denna kod spridas närmast obehindrat. Även om den initiala koden som slinker igenom på det här viset i många fall är i det närmast harmlös så kan den öppna för attacker utifrån i form av bland annat trojaner för stöld av data och keyloggers. Användning av företagsservrar för lagring av privat material, avsiktlig eller ej, kan på samma sätt innebära en kontaminering genom att filer infekterade med skadlig kod direkt hamnar i organisationens servrar (Romer, 2014). Problemet med risken för ökad spridning

av skadlig kod, enligt en undersökning gjord av Cisco (2012), anses tillsammans med ökade hot för dataintrång vara de enskilt största anledningarna till att många organisationer känner osäkerhet kring att implementera BYOD som arbetsverktyg.

### 3.4.4 Förlust och läckage av data

Bortsett från intrång och till följd av skadlig kod är förlust av data till följd av mänskliga faktorer, såsom bristande kunskap eller ren försummelse, ännu en aspekt som bör tas med i beräkningarna när det kommer till att besluta om införandet av BYOD.

Infonetics (2012) visar i en studie att involverade IT-jättar såsom F-Secure, Apple och IBM att 65% av de tillfrågade hos företagen anger att de hade varit med om att enheter innehållande känslig information antingen tappats bort eller stulits. Trots att flera av dessa bedriver stora mängder forskning inom områden där läckage kan få stora ekonomiska konsekvenser var det få som hade specifika lösningar för att kunna hantera sådana situationer.

I sin forskning rörande förlust av data refererar Morrow (2012) till en undersökning av Ponemon Institute som anger att uppemot 90% av anställda med ansvar för IT-säkerhet var säkra eller ansåg det högst troligt att organisationen de arbetade hos varit med om förlust eller läckage av känslig data de senaste tolv månaderna. Problemet med dessa siffror är att många organisationer inte vill uppge i vilken mån de är med om förlust av data av PR-mässiga skäl eller på grund av att de helt enkelt inte vet. Oavsett anledning så menar D´Arcy m.fl (2009) att det finns ett stort mörkertal när det gäller denna typ av incidenter. Både Morrow och D´Arcy anser att den uttalade osäkerheten och bristen på insyn i skyddet kring BYOD-enheter är ett kritiskt och även skrämmande problem.

Poängen i de bådas snarlika observationer blir ännu mer påtagliga och tänkvärda när de sätts tillsammans med Romers (2014) uppgifter att bara i USA förloras 3,5 telefoner per sekund. Av dessa används, som tidigare nämnts, enligt Beckett (2014) uppskattningsvis en klar majoritet för BYOD-relaterade ändamål. Vidare framhåller Romer (2014) att förlusten eller läckaget av data inte nödvändigtvis behöver ske genom den förlorade enheten i första hand utan lagrade inloggningsuppgifter eller lösenord kan möjliggöra och underlätta framtida intrång i organisationens system. Det är på så vis inte en garanti för säkerheten att endast se till att inte lagra känslig data i sig på BYOD-enheter utan även åtkomstmetoder behöver hanteras på ett korrekt sätt.

## 3.5 Åtgärder för att minimera risker

### 3.5.1 Policys

En undersökning utförd av Ian Cook åt CXO visar på att BYOD-trenden ökar ständigt och trots detta så är det väldigt få företag och organisationer som har utvecklat en BYOD-policy. Undersökningen visade att det globalt sett är cirka 60 % av alla fulltidsarbetare som använder någon form av egen enhet på arbetet, men trots detta är det bara ungefär 20% som har skrivit under på att de tagit del av en BYOD policy. En annan undersökning visade att hela 78 % av företag som använder någon form av BYOD inte ens har en policy för det (Gabriel, 2013). Gabriel menar att en organisation som använder BYOD lösningar utan att ha implementerat en ordentlig BYOD-policy omöjligt kan ha en bra kontroll av dataflödet, och det blir svårt att skydda både medarbetare och ledningsgruppen mot de väldokumenterade hot som finns. Han tror dock att en stor anledning till att så få organisationer har etablerat en BYOD policy är att det inte alltid är så lätt. Att implementera en policy kräver nästan alltid ett bra samarbete mellan ledningsgrupp och HR-grupp, att man har god insikt i hur lagarna ser ut så att inte policyn blir lagstridig och att man har bra IT-lösningar som möjliggör arbete på ett arbetssätt som policyn förespråkar.

### 3.5.2 Utformning av policy

Hur en BYOD policy ska se ut och hur man går tillväga för att implementera den är inte alltid självklart, företag och organisationer kan se väldigt olika ut, och detta betyder också att det ställs varierande krav på uppbyggnaden av policyn och framförallt hur man implementerar den. Det är med andra ord svårt att beskriva exakt hur man gör för att skapa en BYOD policy. Jonathan Hassell (2012) skrev en artikel åt tidningen CIO Sweden där han beskriver generellt hur man genom sju steg kan etablera en BYOD policy på sitt företag.

- Specificera vilka enheter som är tillåtna att använda.
- Etablera en bindande säkerhetspolicy för alla enheter.
- Definiera en klar servicepolicy för enheter under BYOD kriterier.
- Klargör vem som äger vilka applikationer och data.
- Bestäm vilka applikationer som kommer vara tillåtna och vilka som blir förbjudna.
- Integrera BYOD planen med policyn för accepterat användande.
- Upprätta en strategi för uppsägning av anställda.

Förr i tiden när BlackBerry var den ledande enheten att använda på jobbet var det vanligast att man använde sin BlackBerry när man arbetade, men inte hemma. Idag finns det en rad olika fabrikat, de vanligaste är iPhone och iPad, androidenheter och HTC. Detta gör att det blir allt vanligare att anställda vill ha möjlighet att använda dessa enheter i arbetssituationer. När man skapar BYOD policyn är det därför viktigt att bestämma exakt vilka enheter som de anställda får använda, och vilka enheter som inte kommer fungera.

Hassel (2012) menar att användare tenderar att vägra ha lösenordskydd eller skärmlås på sina privata enheter, eftersom det ibland anses jobbigt med åtkomst till data eller applikationer. Dock

är detta inte en godtagbar ursäkt då man ofta inom arbetet behandlar känslig information. Om anställda vill använda sina egna enheter på arbetsplatsen så måste de acceptera att ha lösenordsskydd och skärmlås på dessa. Lösenorden måste dessutom vara starka med många tecken och bokstäver inblandat, en vanlig pinkod på fyra siffror är inte accepterat då de är något lättare att knäcka. Lösenord bör även bytas ut frekvent.

Precis som Hassel (2012) säger, är det viktigt att anställda förstår vem de ska vända sig till när frågor och problem uppstår med deras egna enheter, och det är därför viktigt att besluta om följande frågor som rör service.

- Vilken grad av service ska finnas för åtkomst till nätverket från personägda enheter?
- Vilken typ av support ska IT-representanterna ge för enheter som slutar fungera?
- Kommer support ges för installerade applikationer på privatägda enheter?
- Ska man begränsa supporten till att lösa problem med mail, kalender och andra applikationer som hanterar personuppgifter?
- Vad händer om en applikation i en enhet blockerar åtkomst till en av de applikationer som man behöver inom arbetet?
- Ska supporten bestå av en simpel "Wipe and reconfigure" procedur?
- Ska man erbjuda låneenheter till anställda när deras privata enheter blir servade?

I och med att organisationen äger all personlig information som är lagrad på företagets servrar som personal har tillgång till via privata enheter, menar Hassel (2012) att det blir problematiskt när en enhet tappas bort eller blir stulen. Detta betyder att man oftast behöver radera all data som finns på enheten för att förhindra dataintrång. När man återställer en enhet så betyder det i de flesta fall att allt på enheten raderas, inklusive musik, bilder och applikationer som privatpersonen ofta själv betalat för. Hassel tycker därför att man måste göra det klart via policyn att man har rätt att återställa borttappade enheter och därmed är det en god idé att erbjuda utbildningar om hur personal säkerställer sin data, och hur man säkerhetskopierar sina enheter så att det blir lätt att återställa alla data när ny enhet erhålls.

En viktig fråga som Hassel (2012) tar upp är om användare kan ladda ner, installera och använda applikationer som kan innebära säkerhetsrisker på enheter som har tillgång till företagets system. Nya uppdateringar på applikationer kan betyda att dessa har säkerhetsproblem, vilket gör att information kan bli stulen eller kopierad, därför är det viktigt att i policyn klargöra vikten av att kontrollera vilka applikationer man laddar ner och använder sig av. Detta ska gälla för alla enheter som är kopplade till organisationens system.

Det är viktigt att få anställda att förstå att viss aktivitet inte är accepterad när det gäller privat användande på arbetsplatsen. När de ansluter sina enheter till företagets VPN betyder detta att enheter ska användas för jobbrelaterade uppgifter, och Hassel (2012) menar därför att det är viktigt att ta ställning till följande frågor när man skapar BYOD policyn:

- Om man sätter upp en VPN tunnel på en iPhone, är det då tillåtet att anställda går in på Facebook eller andra sociala tjänster?
- Vad händer om en anställd går in på stötande webbsidor när de har VPN anslutning på deras privata enheter?

- Om de sprider material som strider mot företagets värdegrund, oavsiktligt eller ej, över nätverket med sina egna enheter? Vilken straffpåföljd ska detta medföra?
- Vilka övervakningsstrategier och verktyg ska finnas tillgängliga för att upprätthålla dessa policys?
- Vilka rättigheter har organisationen att sätta upp dessa krav?

Vad som händer när anställda säger upp sig som har använt egna privata enheter inom arbetet, och hur man ser till så att arbetsrelaterat material hämtas tillbaka och tas bort från enheten kan vara problematiskt. Det är inte lika lätt som att användare lämnar tillbaka enheten de fått från företaget, utan man bör istället stänga av tillgången till jobbmailen eller den synkroniserade åtkomsten. Vissa mer säkerhetsinriktade företag väljer att radera allt och återställer de personliga enheterna helt när personal avslutar sin anställning. Hassel (2012) anser att man bör ha en tydlig metodik för hur säkerhetskopiering av personliga bilder och applikationer ska gå till innan man återställer en enhet. Det är därför viktigt att ha med dessa delar i BYOD policyn, och uppmärksamma de anställda på vilka rättigheter organisationen har när det gäller att radera data på privata enheter.

### 3.5.3 Skydd av data

Att från början ha ett tydligt säkerhetstänk anses vara en självklarhet enligt de verk som denna teoretiska bakgrund bygger på. Hur detta säkerhetstänk bör implementeras i praktiken skiljer sig dock nämnvärt mellan olika författare. Beckett (2014) menar på att tydliga och klara direktiv över vilka applikationer och enheter som får användas är lösningen på problemet tillsammans med att se till att alla enheter som har tillgång till systemet är utrustade med skyddande mjukvara.

Eschelbeck och Schwartzberg (2012) utgår från samma grundtankar som Beckett men ger en mer ingående förklaring av hur de anser att BYOD-enheter bör hanteras. Krav på lösenord eller andra typer av kodlås för samtliga enheter, krav på att någon form av antivirusprogram installeras och kontroll över vilka applikationer som får installeras är delar de ser som kritiska, men nämner även full kryptering av enheter och Mobile Device Management (MDM) som nödvändiga åtgärder för att säkerställa data och systemåtkomst. Användningen av MDM som ett verktyg för att låsa ner eller radera all data på en enhet är en lösning som återkommer hos flera författare med motiveringen, att det är ett effektivt och förhållandevis enkelt sätt att återta kontrollen över de enheter som används. Tokuyoshi (2013) är en av de författare som i sitt arbete lyfter fram MDM för dess roll i att ge tillbaka kontroll över data till organisationen men menar samtidigt att all form av *"endpoint security"* där skyddet ligger på användarens enhet bör vara en sista utväg, även om det inom BYOD i vissa fall kan vara det enda alternativet. Problematiken med MDM anser Tokuyoshi vara att ansvaret för säkerheten fortfarande ligger på användarna och nämner tre grundpelare som är viktiga inom implementering av BYOD: Tillit, skydd och kontroll. Även om MDM ser till att organisationen har tillräcklig kontroll för att exempelvis kunna radera all data på en enhet i händelse av förlust, så är det svårt att kontrollera att ordentliga skydd så som antivirusprogram eller lösenord används på enheten. Därmed blir tilliten från organisationen gentemot de anställda kritisk.

Thomson (2012) och Romer (2014) stämmer även de in i kritiken mot att se MDM som en universell lösning. Thomson anser att Data Loss Prevention (DLP) bör ha högre prioritet och att företag bör ställa sig frågan: *"Skyddar vi rätt data, och skyddar vi den på rätt sätt?",* och följer upp med uttalandet *"Du kan inte bygga murar av säkerhet runt det du behöver skydda om du inte vet vad det är."* Med det menar Thomson att många organisationer saknar en ordentlig kategorisering av data och för att kunna förhindra läckage och förlust måste all data först kategoriseras för att kunna skyddas på rätt sätt. Att inte kunna komma åt känsliga filer från en mobiltelefon ökar inte säkerheten nämnvärt ifall dessa går att kopiera över till ett USB-minne.

Romer för liknande resonemang som Thomson och anser att ett fokus på vad som skyddas är viktigare än vilka enheter som har tillgång till datan. Romer menar även att användning av MDM riskerar att resultera i en oändlig att-göra-lista då det ständigt lanseras nya enheter. Två alternativa lösningar som presenteras är först metoden Access Control Lists (ACL), där åtkomst till olika nivåer av systemets data regleras efter enhetstyp. ACL förenklar det administrativa arbetet men likväl som med renodlad MDM så brister denna i kontroll över enskilda filer och ger ingen garanti att enheten är korrekt skyddad på klientsidan. Den andra metoden är att istället använda Mobile Content Management (MCM) som fokuserar på att skydda data på samma vis, oberoende av vilken typ av enhet som begär åtkomst till denna. Detta sker i form av att all skyddad data på klientsidan innesluts i mjukvarucontainrar. På så vis kan datan inte bli kontaminerad även om andra filer på enheten är det. I kombination med en centralisering av åtkomstkontroll, val av betrodda säkerhetslösningar och användningen av privata molntjänster, istället för kommersiella, kan en god säkerhet upprätthållas samtidigt som riskerna BYOD medför minimeras.

## 3.6 Sammanfattning av teori

BYOD är ett fenomen som stadigt sprider sig inom både företagsvärlden och offentliga organisationer. En ny, ständigt uppkopplad livsstil, främst hos de yngre generationerna tillsammans med smidigare, säkrare och effektivare lösningar för att kunna arbeta via distans lockar, och enligt vissa även tvingar, organisationer att implementera BYOD som arbetssätt. Vinsterna ett enskilt företag kan ta del av är anmärkningsvärda, men riskerna för läckage och förlust av data kan samtidigt vara förödande. Förlusten av kontroll tillsammans med en ökad risk för förlust och oönskad spridning av immateriella tillgångar är avskräckande biverkningar som måste hanteras.

Till dessa tillkommer det faktum att ett stort antal organisationer ännu inte har tydliga policys uppsatta för hur det dagliga arbetet ska genomföras på ett säkert sätt, alternativt är dessa undermåligt cementerade i arbetsstyrkan. Även utan den ökade säkerhetsmässiga komplexitet som BYOD medför är den mänskliga faktorn det största hotet mot en god IT-säkerhet och i och med dess införande blir denna faktor ännu mer påtaglig. I slutändan måste ett stort antal parametrar begrundas för att kunna göra en bra övervägning huruvida BYOD ska användas inom organisationen och även i vilken utsträckning.

En robust och pålitlig systeminfrastruktur tillsammans med noggrann kategorisering av data och bestämmelser kring åtkomstnivåer sammanfattar grundkraven för att kunna implementera BYOD på ett säkert sätt, utan att varken användare eller organisationen blir lidande. För att lyckas med detta krävs en omfattande intern forskning kring vilken funktionalitet som behövs, vilka resurser som finns tillgängliga och i vilken grad systemet kommer att användas.
Väl på plats riskerar dessa system att få ett försvagat skydd ifall inga tydliga riktlinjer och regler finns för hur de får och bör användas. Utbildning är av yttersta vikt för att minimera risken för förlust av data. I fall av förlust av enhet innehållande känslig data bör åtgärdsplaner för att hantera dessa finnas och gås igenom rutinmässigt.

| Faktor | Beskrivning | Källa |
|---|---|---|
| Definition | Definition av BYOD | (Pillay m.fl, 2013)<br>(Romer, 2014) |
| Spridning | Utbredning av mobila enheter | (Gartner, 2006)<br>(Becket, 2014)<br>(Thomson, 2012)<br>(SCB, 2014) |
| Fördelar med BYOD | Produktivitet och flexibilitet, ekonomi, enskild tillfredsställe | (Pillay m.fl, 2013)<br>(Cisco, 2013)<br>(Morrow, 2012)<br>(Thomson, 2012) |
| Nackdelar med BYOD | Komplexitet, förlust av kontroll, intrång och skadlig kod, förlust och läckage av data | (Pillay m.fl, 2013)<br>(Thomson, 2012)<br>(Beckett, 2014)<br>(Tokuyoshi, 2013)<br>(Romer, 2014)<br>(Cisco, 2012)<br>(Infonetics, 2012)<br>(D'Arcy m.fl, 2009) |
| Åtgärder och riktlinjer | Policys, utformande av policy och skydd av data | (Personalkonsulten, 2012)<br>(Gabriel, 2013)<br>(Hassell, 2012)<br>(Beckett, 2014)<br>(Eschelbeck & Schwartzberg, 2012)<br>(Thomson, 2012)<br>(Romer, 2014) |

Tabell 1. Teoretiskt ramverk

# 4. Empirisk forskning

I detta kapitel redogörs först för den kvantitativa enkätstudien och sedan de tre intervjuerna på kommunen i den ordning som de utfördes. Frågorna som ställdes i enkäterna samt svarsalternativ presenteras i bilaga 8.3 i uppsatsen. Den längre intervjun med Baggesen och Bergdahls frågeställning återfinns i bilaga 8.1 och frågorna till telefonintervjuerna i bilaga 8.2.

## 4.1 Sammanställning av enkätstudie

Enkäten gick som tidigare nämnt ut till 125 anställda på Stockholms Läns Landsting och av dessa svarade 75 personer. Då inte alla anställda på landstinget av praktiska skäl kunde tillfrågas om att besvara enkäten är resultaten inte nödvändigtvis representativa för arbetsstyrkan över lag, men kan ändå anses ge en värdefull insikt i hur informerade de anställda är.

De första två frågorna av enkäten gällde kön och åldern på de 75 svarande, resultatet blev att 78,7% av de tillfrågade var kvinnor vilket var en något större majoritet än förväntat. Åldersmässigt uppgav 37,3% att de var mellan 30 och 49 år medan 60% var över 50 år. Enkäten fortsatte med att fråga ifall de svarande hade möjlighet till användning av privata enheter inom arbetet, inklusive tillgång till jobbmail via dessa, och om arbetsplatsen tillhandahåller mobila enheter till de anställda.

På frågan rörande privata enheter svarade 84% att de hade möjlighet att använda sig av privata enheter inom arbetet, 12% av de inte hade det och 4% visste inte om möjligheten fanns. Hela 94,7% svarade att landstinget tillhandahåller nån form av mobil enhet för arbetsändamål, resterande svarade nej. Dessa svar visar tydligt på att landstinget jobbar med BYOD, om än inte i vilken utsträckning. Svaren visar även på en potentiell brist i kommunikationen, då en del av personalen inte vet om de har möjligheten att arbeta via sina privata enheter.

Enkäten fortsatte med frågan om de svarande någon gång lagrat arbetsrelaterad information på privata enheter, här medräknat externa lagringsmedium så som portabla hårddiskar och USB-minnen. 70,7% uppgav att de någon gång lagrat information på det sättet vilket leder till en ökad risk för att informationen hamnar i obehöriga händer. Det bör tas i beaktande att det inte framgick ifall dessa enheter var skyddade via lösenord eller kryptering vilket skulle minska risken för skada vid förlust av enhet.

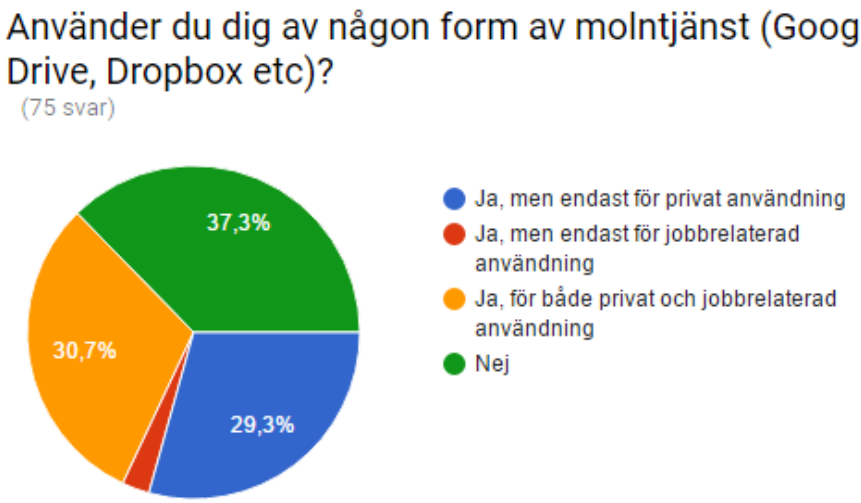


Fig 1.

Resultatet (Figur 1.) på frågan gällande användning av molntjänster ligger i linje med teorin som visade på en snarlik utbredning av molntjänstanvändning. En relativt stor del använder sig av molntjänster inom arbetet vilket kan vara alarmerande, beroende på vilken data som lagras och vilken tjänst, men överstiger inte förväntningarna nämnvärt.

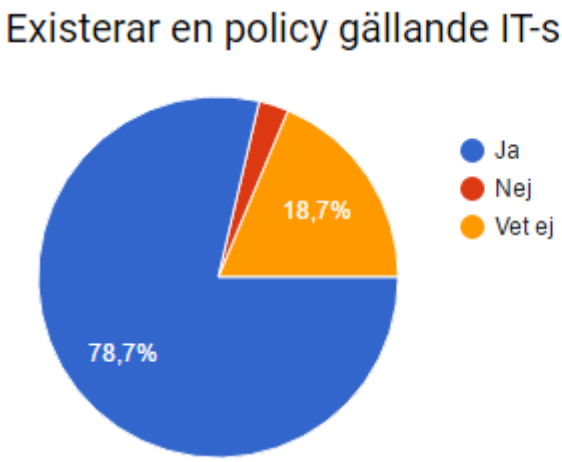


Fig 2.

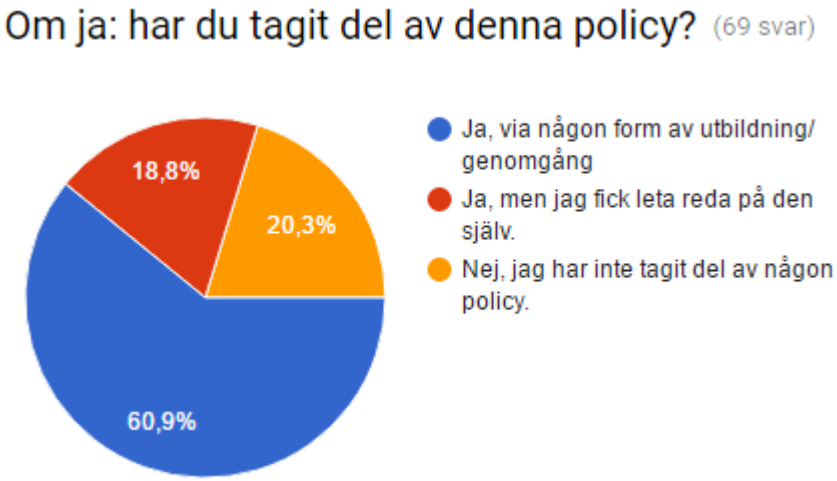


Fig 3.

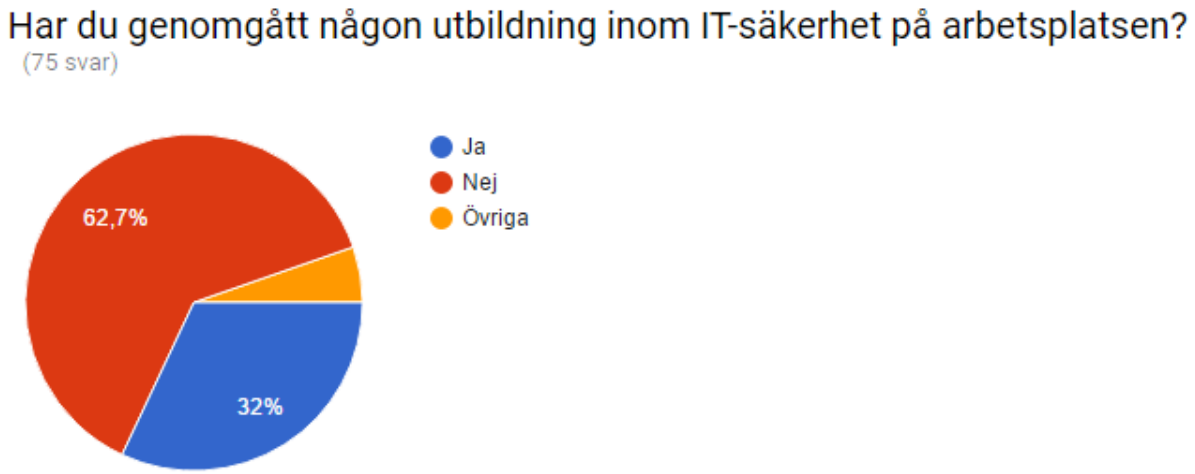


Fig 4.

De tre ovanstående svarsdiagramen gav ett förväntat resultat när det gäller den andel som inte hade genomgått en utbildning inom IT-säkerhet och ligger i linje med den bild som målades upp efter intervjun på Uppsala Kommun att säkerhetsutbildningar är ett område i behov av förbättring.

De "Övriga" svaren var: *"Minns ingen, men möjligtvis"*, *"Ja, en datorbaserad utbildning som var tillgänglig på intranätet"*, *"Ej utbildning, endast kortare info"* samt *"Mer information än utbildning"*. Gällande existensen av en säkerhetspolicy svarade en överraskande stor det att de inte visste ifall ett sådant dokument existerade. Av de som visste att en policy fanns så verkar svaren tyda på att alla på något sätt har tagit del av dokumentet antingen via en genomgång eller själva sökt upp det. Den stora andelen som inte var medvetna om dess existens utgör ett potentiellt riskelement när det kommer till att upprätthålla en god IT-säkerhet då det tyder på bristande rutiner när det gäller att se till så all personal tagit del av den rådande policyn.


Fig 5.


Fig 6.

En klar majoritet av de tillfrågade angav att de hade god kunskap om vilka regler som gäller på arbetsplatsen men strax över hälften menade ändå på att de var osäkra gällande vissa delar.
Svarsandelen som uppgav att de hade dålig kunskap gällande vilka regler som fanns uppsatta stämmer in på andelen som tidigare i enkäten angav att de inte visste om någon säkerhetspolicy existerade. Det kan därmed anses rimligt att dra slutsatsen att kommunikationen av rådande säkerhetspolicy har en positiv inverkan på huruvida de anställda är medvetna om vad som är tillåtet på arbetsplatsen, vilket var det förväntade resultatet.
Trots att majoriteten uppgav att de följer de regler som finns uppsatta på arbetsplatsen har en förhållandevis stor del någon gång brutit mot de regler som gäller. Här uppdagas också en riskfaktor även om anledningen till detta fenomen inte framgår.

Antagandet här är tvådelat: antingen har vikten av att följa de regler som finns uppsatta inte cementerats ordentligt inom arbetsstyrkan alternativt är reglerna inte verklighetsförankrade när det gäller det praktiska arbetet vilket i sin tur kan resultera i att de förbises till fördel av ett smidigare arbetssätt. Den sista delen som valde *"Vill inte svara/Vet ej"* som svarsalternativ kan även den vara ett möjligt hot. Då enkäten var helt anonym och svaren inte kan kopplas till en

enskild person och då svaret sammanfaller bra med procentandelen som angav att de hade dålig kännedom om vilka regler som finns, 14,7% respektive 18,7%, så är det befogat att se svaren som *"Vet ej"* även om det inte är styrkt bortom allt tvivel.

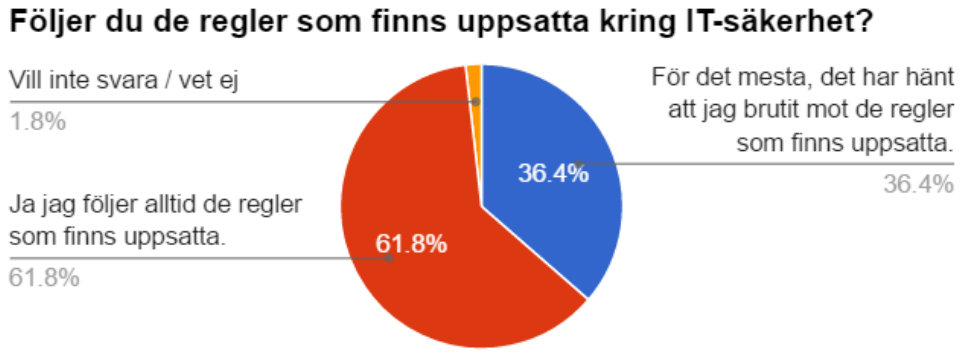


Fig 7. Resultat från de svarande som uppgav att de tagit del av rådande policy.

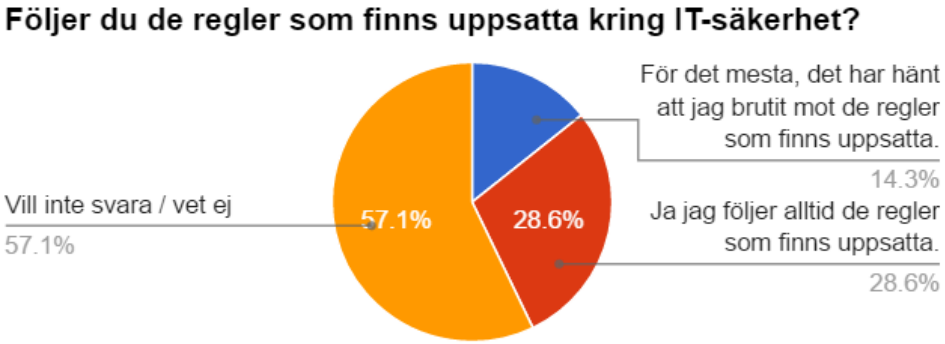


Fig 8. Resultat från de svarande som uppgav att de inte tagit del av rådande policy

När svaren sorterades utifrån huruvida de svarande hade tagit del av policyn eller inte, framkom stora skillnader. De som tagit del av policyn var överlag markant bättre på att följa de regler som finns uppsatta även om en oroväckande stor del trots det angav att de någon gång brutit mot dessa. Figur 8:s andel som angav *"Vill inte svara/Vet ej"* tolkades som "*Vet ej"* då svaren var helt anonyma och därmed ansågs det inte finnas någon motivering bakom alternativet *"Vill inte svara",* här brister dock frågeställningen något då svaret blir mångtydigt. Författarna av uppsatsens tolkning menar på att det finns en bristande kunskap kring vilka regler som finns och därmed även en hotbild mot informationssäkerheten.

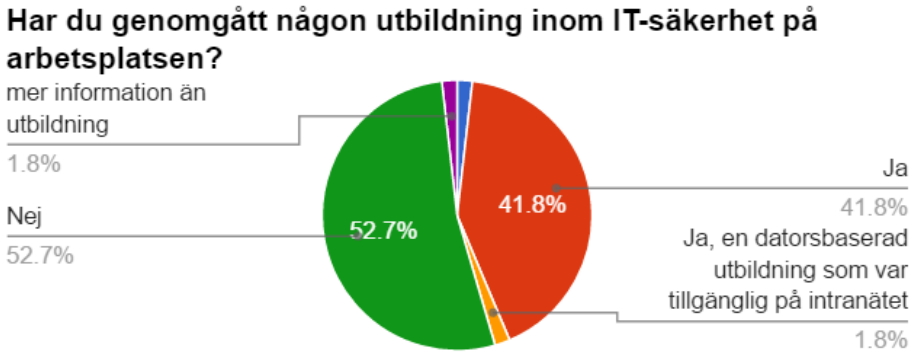


Fig 9. Resultat från de svarande som uppgav att de tagit del av rådande policy.

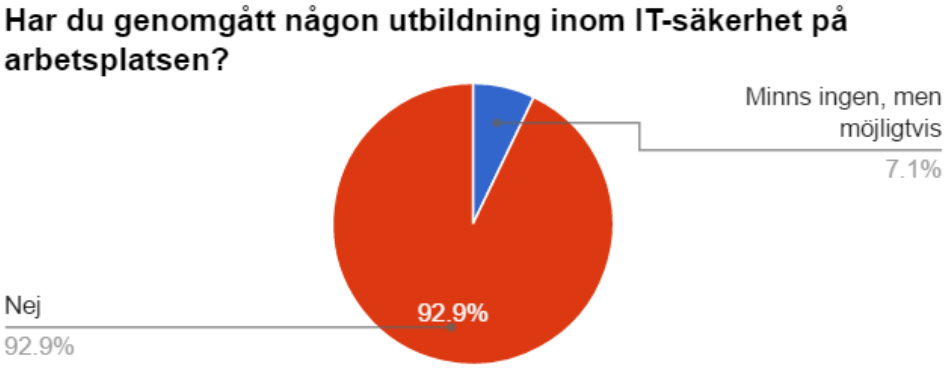


Fig 10. Resultat från de svarande som uppgav att de inte tagit del av rådande policy. Skillnaden i färg på bitarna beror på att verktyget Awesometable inte tillät ändring av färger och inte tilldelade färgerna konsekvent.

När de olika urvalsgrupperna jämfördes rörande vilken utbildning de tagit del av blev skillnaderna åter tydliga. Av de som inte tagit del av policyn kunde ingen ange att de säkert genomgått någon form av utbildning inom IT-säkerhet, då dessa varken tagit del av policyn eller någon utbildning är det en betydande säkerhetsrisk då det är rimligt att anta att de inte har tillräcklig insikt i vilka regler som gäller.

Sammanfattat visar enkätstudien på att Stockholms Läns Landsting behöver utveckla arbete gällande policys och initiera utbildning av anställda rörande IT-säkerhet.

## 4.2 Sammanställning av intervjuer

### 4.2.1 Intervju med Olle Bergdahl och Peter Baggesen

När kontakt togs med Uppsala kommun så blev vi hänvisade till två personer: Olle Bergdahl och Peter Baggesen. Bergdahl arbetar som IT-strateg och har som huvudsaklig uppgift att styra projekt även om han beskriver sitt arbete som mångsidigt. Han har jobbat inom kommunen tidigare 2011 till 2012 för att sedan byta bana och istället arbeta som konsult i två år. Han fick därefter "hemlängtan" och kom tillbaka till kommunen 2014.
Baggesen är IT-säkerhetsspecialist på kommunen och arbetar med informationssäkerhet på säkerhetsenheten i Uppsala. Han kommer tidigare ifrån Skatteverket och anställdes av kommunen för cirka ett år sedan. Han har dock varit föräldraledig i ungefär sex månader, och är därmed enligt egen utsaga inte lika rutinerad som vissa av hans kollegor.

**Säkerhetsarbete**

Intervjun började med att en fråga ställdes om hur kommunens säkerhetsarbete ser ut på en daglig basis på vilken svaret blev att det är väldigt varierande från dag till dag. Detta följdes upp med en frågeställning rörande hur organisationens säkerhetspolicy ser ut och hur arbetet kring denna såg ut. Baggesen beskrev här den säkerhetspolicy som finns etablerad inom kommunen men påpekade samtidigt att denna inte uppdaterats sedan 2009 och därav hade ett behov av förbättring. Baggesen är den av de båda vars arbetsuppgifter är tydligt kopplad till förmedling av kommunens policy, detta för att upprätthålla en god säkerhet och se till att hela personalstyrkan har samma utgångspunkt och förutsättningar. Vissa roller inom organisationen har även krav på genomgång av rådande policy inbäddade i rollbeskrivningen. De olika verksamheterna som arbetar med kommunen eller har någon form av tillgång till dess system bör även de ta del av policyn för att se vilka riktlinjer och regler som finns uppsatta.

Även om Bergdahls preliminära arbetsuppgifter inte alltid är direkt relaterade till policyarbetet så gav han sin syn på hur detta fungerade och inflikade även, med medhåll från Baggesen, att han ansåg att det finns ett mörkertal och en upplevd brist när det gäller hur stor andel som tagit del av policydokumentet.

**BYOD**

Gällande vilka fördelar de anser att det finns med att implementera BYOD anger Baggesen att han tror att inom just kommunen kan BYOD underlätta arbetet med att locka yngre att börja arbeta inom kommunen och även visa på att kommunen inte är lika "stabbig" som den har en tendens att upplevas. Han nämnde även att vissa kostnader skulle kunna elimineras när det gäller inköp av enheter för de anställda. Bergdahl inflikar att det är väldigt positivt att användandet av egna enheter öppnar för ett allt mer flexibelt arbetssätt där exempelvis fysiska begränsningar av arbetsplatsen elimineras vilket underlättar samarbetet mellan avdelningar då dessa kan arbeta tillsammans på valfri plats. Flexibiliteten mobila enheter ger medför även att uppgifter som kräver en ostörd miljö kan utföras trots att merparten av arbetet kanske sker i en öppen kontorsmiljö.

Han fortsätter med att nämna att olika roller inom organisationen har skilda krav på vilka enheter som kan och får användas för att sedan poängtera att BYOD och dess syskon BYOC (Bring Your Own Cloud) kommer växa stadigt inom diverse IT-lösningar och därmed bör organisationen se över dessa krav.

När det kommer till nackdelarna de ser med BYOD svarade Baggesen att han anser att det största problemet är kontrollen av informationsflödet, det finns en osäkerhet kring vart informationen tar vägen och det är svårt att kontrollera vad för information som anställda tar med sig hem. Det leder i sin tur till frågetecken kring vilken information som går förlorad om det sker en incident. Det kan även vara svårt att på ett bra sätt återfå all viktig information vid en anställnings avslutning. Bergdahl hoppar här in i diskussionen och menar på att det i dagsläget är lätt för kommunen att kontrollera att de enheter som används är ordentligt skyddade och uppdaterade. Denna aspekt försvåras avsevärt vid en övergång till användandet av privatägda enheter där IT-avdelningen inte nödvändigtvis har befogenhet att genomföra alla nödvändiga inställningar utan detta ansvar läggs på de anställda.

Intervjun fortsatte med frågan om det fanns några specifika nackdelar eller svårigheter som är unika för kommunen, då integritetsskydd ansågs självklart ställdes frågan med fokus på aspekter som lätt kan ha missats under utformningen av intervjun. Bergdahl svarade med ett exempel på att vissa mjukvaror och system bara stöds av specifika webbläsarversioner, i de flesta fall Internet Explorer. Detta medför att det kan förekomma komplikationer vid användningen av dessa tjänster på privata enheter. Även om rätt webbläsare är installerad kan fel version resultera i att programmen fungerar dåligt eller inte alls. Använder man däremot kommunens tillhandahållna enheter kan man vara ganska säker på att tjänsterna i de flesta fall ska fungera bra. Anledningen till att det i de flesta fall bara fungerar med en specifik version av Internet Explorer är enligt de svarande att upphandlingarna av systemen i många fall är så pass gamla att kravspecifikationerna endast innefattade en enda webbläsare då de två huvudsakliga rivalerna Firefox och Google Chrome inte var aktuella. Till skillnad mot dagens upphandlingar innehöll dessa inte heller några krav på att senare uppdateringar av webbläsare behövde stödjas vilket har blivit ett allt större problem.

På frågan om hur BYOD används och i vilken utsträckning det används inom kommunen, inte bara datorer, mobiler och surfplattor, utan även portabla lagringsmedia såsom externa hårddiskar och USB-minnen, svarar Baggesen med ett skratt att hur det ser ut och hur det borde se ut tyvärr inte riktigt är samma sak. Han kände sig lite osäker på frågan, så han bollar över till Bergdahl som svarar att ur hans synvinkel är inte BYOD användandet speciellt utbrett bland deras egna anställda, det vanliga är att de anställda använder de enheter som de fått ifrån kommunen. Med det sagt poängterar han att det finns yrkesgrupper, framförallt externa konsulter som kommer in till dem och behöver använda sina egna enheter för att ha tillgång till viss programvara eller specifik information som de inte har åtkomst till via kommunens enheter. I dessa fall kan undantag ske och enheterna få tillgång till systemen på samma sätt som kommunens egna.

**Tillgång till system**
På frågan hur just tillgången till de kommunala systemen ser ut, svarade Bergdahl att de använder sig av fjärråtkomst via VPN-tunnlar med hjälp av Citrix. Det går därmed att komma åt de flesta tjänster hemifrån, främst webbaserade tjänster då de lätt kan exponeras via ett säkerhetsskal med krav på inloggning. Vid frågan om information sparas lokalt på användarnas datorer, eller om kommunen har en central lagringsplats där allt sparas, svarar Bergdahl att information inte sparas på användarnas datorer utan på centrala servrar. Bilagor och liknande på exempelvis arbetsmailen går dock att ladda hem på en privat enhet.

**Påverkan**
Intervjun gick sen vidare till att fråga hur de ansåg att den växande BYOD-vågen har påverkat dels dem själva som individer men även de anställda på kommunen överlag. Baggesen svarar att han har varit på kommunen så pass kort tid att han inte har haft möjlighet att observera någon uppenbar påverkan. Bergdahl uppgav att han under åren 2010-2012 jobbade intensivt med att undersöka och fastställa en funktionalitet rent tekniskt för att möjliggöra BYOD. Då undersöktes olika tekniska lösningar, bland andra Citrix, för att kunna virtualisera applikationer och tjänster så att de blir plattformsoberoende. Satsningen svalnade av i och med utvecklingen av Microsofts kontorsplattform, Office 365. De ansåg då att det var viktigare att satsa på molntjänster då det blev mer aktuellt i samband med Office 365.

**Policy och utbildning**
Efter att påverkan av BYOD gåtts igenom fördes diskussionen vidare med frågan om hur kommunens policy och regelverk ser ut och hur dessa kommuniceras ut till de anställda.
Baggesen svarade att det finns potential för ett relativt stort förbättringsarbete inom området, främst när det gäller att se till att de anställda tar del av den policy som finns. När han själv blev anställd fick han ingen information över huvud taget angående policys. Han misstänker att arbetsgivarna förväntade sig att han själv skulle ta initiativet att läsa igenom policyn på egen hand, han angav däremot att det kan skilja ordentligt mellan olika chefer, vilken avdelningen och vilka arbetsuppgifter som anställningen berör. Oavsett dessa aspekter anser han att alla nyanställda borde informeras om gällande regler och riktlinjer då de har vissa rutiner som ska följas vid anställning. När det gäller BYOD policy så finns det i dagsläget ingen, utan det finns bara en generell IT-policy som berör alla delar av IT-verksamheten.

Efter detta ställs en följdfråga om kommunen har någon relaterad IT-utbildning för personalen. Bergdahl svarar att de har två utbildade IT-pedagoger som går igenom de programvaror som de anställda använder och vid behov håller utbildningar om dessa.
De existerar även ett kurspaket som de anställda kan anmäla sig till om de vill utveckla sina kunskaper, detta paket är dock frivilligt att genomföra. För att få vissa behörigheter, till främst system och mjukvara som hanterar känsliga personuppgifter, krävs dock att obligatoriska utbildningar genomförs. Baggesen fyller i att de även har en e-utbildning, som är utdaterad på många håll, och att de arbetar på att utveckla den så att den återigen blir aktuell. När denna e-utbildning är färdigutvecklad kommer det vara ett krav på att alla som arbetar med någon form av IT genomför den. Detta upplägg kommer underlätta uppföljningsarbetet då det kommer synas vilka som genomfört utbildningen och vilket resultat de fick.

På frågan om hur välinformerade de upplever att personalen är när det kommer till regler och policys svarade Baggesen och refererade till det Bergdahl sagt tidigare att det i stor mån är beroende på var i organisationen man arbetar. De personer som arbetar med känslig information, så som personuppgifter och liknande ansåg båda hade överlag väldigt bra insikt i vilka regler och rutiner som ska följas medan de upplevde att den övriga personalstyrkan inte alltid var lika insatt. Följdfrågan till detta blev vilka de största svårigheterna är när det kommer till att utbilda och informera de anställda. Baggesen svarade att de största hindren är tid och prioritering, det är stundtals problematiskt för beslutsfattarna att vara realistiska med hur mycket tid som bör avsättas för utbildning av personal vilket medför att det ibland genomförs halvdant.

**Respons på utbildning**

På frågan om hur responsen från de anställda ser ut, och om de tar utbildningarna på allvar eller om det existerar en utbred mentalitet av "*Det händer väl inte mig?"* svarade Baggesen att det är svårt att avgöra. Han menar dock att om man kan visa upp skarpa exempel på incidenter som har inträffat inom den egna verksamheten är det lättare att få individer att förstå riskerna som finns och att det lätt kan hända även den bäste.

Bergdahl svarade att han ser utbildningarna som två delar. Den första delen handlar om att informera om vad som faktiskt gäller, och den andra delen är att fostra ett beteende hos de anställda där säkerhetsarbetet är en del av den dagliga rutinen. Exempelvis är en del att försöka få de anställda att förstå att det är bättre att anmäla en potentiell säkerhetsrisk två gånger än att inte anmäla alls.

**Framtida säkerhetsarbete**

Intervjuns sista område började med en fråga om hur de skulle vilja lägga upp och ändra på arbetet kring utbildning och policy om de skulle leva i en drömvärld där ledningen förstod vikten av att avvara tid för utbildning och att de fick tillgång till den tid och de resurser som de behövde.

Baggesen svarade att baserat på hur utbildningarna ser ut i dagsläget så är de väldigt generella och fungerar mer som en introduktion än en ordentlig utbildning. Han tycker att de frågor som tas upp under utbildningarna i högre grad borde integreras i det dagliga arbetet och att:*"Säkerheten i sig ska inte vara en separat del utan den ska vara integrerad i resten, det är en del av det dagliga arbetet".* Han menade att de är där för att utföra ett bra arbete, och att det till stor del görs genom att arbeta på ett säkert sätt.

De intervjuade tillfrågades om vart de anser att utbredningen och utvecklingen av BYOD är på väg, om fenomenet kommer att fortsätta växa eller om det kommer att svalna av. Bergdahl uppgav att han tror att BYOD kommer fortsätta att växa, men att fokus kommer ligga mer på vikten av åtkomst till rätt data. Här menar han på att BYO Cloud, BYO application och BYO Data kommer se stora uppgångar.

Han tror också att det kommer uppstå ett ökat behov av att kunna ta emot data utifrån som genereras utanför organisationen så som smarta uppkopplade armband som kan användas inom äldreomsorgen för att strömma data till kommunen för att underlätta besluten om vart organisationen bör lägga resurser innan skadan är skedd.
Han pratar också om att de inom tjänsteutvecklingsområdet har arbetat traditionellt i ett så kallade *triple helix-projekt* där akademin, företag och staden alla varit delaktiga inom olika testbäddsprojekt. En förändring av utvecklingen är på väg där man ska gå över från *triple-helix* till *quad-helix-projekt* där även medborgare involveras i testningen.
Tanken är att man ska låta medborgare testa betaversioner av olika system så att man tidigt kan ta reda på om det är värda att satsa på eller inte.

Detta medför att det ställs ännu högre krav på informationssäkerheten, det är inte bara den data som kommunen genererar själva, utan även data som kommer utifrån från allaolika enheter som måste lagras, bearbetas och skyddas. Bergdahl tror också att samhället kommer att se en explosion av BYOD i samband med IoT (Internet of Things) där varje sensor i sig är en enhet som strömmar in data. Baggesen gav här medhåll och inflikade att han tror att det kommer behöva arbetas mer med att upplysa och informera om vilka regler som gäller för att få en bättre struktur på informationen, framförallt med tanke på det nya datalagringsdirektivet som snart börjar gälla och som ställer högre krav. Bergdahl infogade skämtsamt att *"datalagringsdirektivet är det största som har hänt inom PUL (Personuppgiftslagen red. anm) sedan PUL".*

På detta ställs en följdfråga om vilka de största skillnaderna kommer bli för de som arbetar inom kommunen efter dess införande. Baggesen svarade att det är två år kvar tills dess att det nya direktivet börjar gälla som svensk lag och att de då måste vara förberedda. Han lyfte även fram att det finns en utbredd rädsla kring det faktum att den nya lagstiftningen öppnar för att organisationer kan bli tvingade att betala vite om lagstiftningen inte följs korrekt. Avslutningsvis beskriver Baggesen att direktivets syfte är att se till att organisationer är medvetna om vem som har tillgång till dess data och vart den tar vägen utanför systemet. Direktivet ger också varje enskild individ rätten att begära tillbaka information om sig själva från organisationer som då måste radera all individuell data. För att detta ska vara möjligt krävs just den tidigare nämnda medvetenheten kring vart informationen sprids och lagras.

Intervjun med Bergdahl och Baggesen gav en tydlig och ingående bild av hur Uppsala Kommun arbetar för att upprätthålla en god IT-säkerhet, de svar vi fick överensstämde i hög grad med den teoretiska forskning som låg till grund för uppsatsens frågeställning. Utöver det förebyggande och utvecklingsrelaterade arbete de utförde framkom även ett antal förbättringsområden organisationen har i sitt säkerhetsarbete. Intervjun uppfattades därmed som väldigt öppen och ärlig från informanternas sida och svaren verklighetsförankrade.

Trots den upplevda pålitligheten i informationen intervjun genererade utfördes även två ytterligare intervjuer via telefon med slumpmässigt utvalda anställda utanför IT-avdelningen för att undersöka huruvida det fanns meningsskiljaktigheter kring hur väl säkerhetsarbetet fungerade. Grundtanken var att tre telefonintervjuer skulle genomföras för att få ett bra underlag, till följd av att en av de tillfrågade inte kunde medverka med tillräckliga marginaler innan

deadline hann bara två telefonintervju utföras. Svaren vi fick bör betraktas med ett visst mått av försiktighet då de kommer från ett fåtal enskilda anställda vars svar inte nödvändigtvis är representativa för arbetsstyrkan i sin helhet.

### 4.2.2 Intervju med anställd nummer 1

Intervjun bestod av ett antal frågor rörande säkerhetspolicys och utbildning samt den tillfrågades kännedom om dessa tillsammans med ett par frågor relaterade till dennes användning av BYOD på arbetsplatsen. Den intervjuade uppgav att hen inte hade tillgång till privata enheter inom arbetet, vilket överensstämmer med den primära intervjun, men däremot till jobb-mail via VPN-koppling. Denna tillgång är dock endast tillgänglig via kommunens tillhandahållna datorer, ej via privata. Molntjänster användes inte heller av den anställde då hen fick information om att dessa ej var tillåtna att använda via anställningens start, däremot privata USB-minnen för att överföra data mellan olika datorer.

Efter en start som överensstämde och passade väl ihop med de första intervjuerna fick svaren en annan karaktär när frågorna övergick till att handla om utbildning och policys. Den anställde var osäker på om en policy rörande IT-säkerhet existerade och hade oavsett det inte tagit del av denna, inte heller någon utbildning inom IT-säkerhet hade genomgåtts av personen. Här lades en kommentar gällande de obligatoriska utbildningarna som nämndes av Bergdahl och Baggesen för vissa system men att dessa fanns var helt ny information för den anställde. I samband med detta fyllde den tillfrågade i med att berätta om att en kollega till denne som runt 2013-2014 arbetat på att ta fram en ny IT-utbildning, men planerna att implementera denna lades på is och materialet raderades, enligt utsago utan att någon tillfredställande förklaring gavs.

På frågan om känslan av delaktighet i säkerhetsarbetet blev svaret 1 på en femgradig skala vilket var lägsta möjliga svar. Detta motiverades till stor del av att det utbildningsmaterial, vilket finns utlagt på kommunens intranät, inte sett någon aktivitet sedan den förrförra säkerhetschefen gjorde ett inlägg i februari 2014. Dessa uppgifter har inte kunnat bekräftas av någon på IT-avdelningen och bör därför inte ses som bevisande fakta även om källan får anses vara trovärdig. I det fall att uppgifterna stämmer kan det tyda på klara brister i uppföljning, rutinmässig genomgång av säkerheten och inom utbildning av personalstyrkan.
Nämnvärt här är att den tillfrågade höll med Bergdahl och Baggesen i observationen att de avdelningar av organisationen som hanterade mängder av känsliga uppgifter, så som sjukvård och socialnämnd, överlag var oerhört insatta i vilka regler som fanns uppsatta och följde dessa bättre än de avdelningar som inte hanterade den typen av information. Slutligen ansåg den intervjuade att systemet med olika åtkomstnivåer baserat på enhet och åtkomsttyp inte var tydligt nog och uppfattas som rörigt vilket lätt leder till missförstånd i kommunikationen mellan IT-avdelningen och de anställda.

Sammanfattningsvis levererade denna intervju ett mestadels förväntat resultat där de brister som uppdagades i det stora hela överensstämde med vad som sagts i tidigare intervju även om omfattningen gällande vissa problem skilde sig. Exempelvis fanns redan bilden av att

utbildningsmaterialet inte var uppdaterat ordentligt men att forumet hade varit inaktivt under drygt två års tid var inte förväntat och var ingenting som framkommit under den tidigare intervjun.

### 4.2.3 Intervju med anställd nummer 2

Den andra intervjun som genomfördes började med att den tillfrågade fick en fråga rörande hens möjligheter att använda sig av privata enheter inom arbetet eller hade tillgång till jobbrelaterade resurser via dessa. Svaret blev att den tillfrågade hade tillgång till mailkonto samt kommunens intranät via vilken dator som helst via VPN-tunnel, svaret skiljer sig därmed mot den första intervjun där det framgick att endast kommunens tillhandahållna enheter hade tillgång till intranätet. På frågan om den intervjuade hade lagrat jobbrelaterat material på privata enheter blev svaret nej. Hen upplevde att kommunens tillhandahållning av bärbara datorer, surfplattor och smartphones gav en tillräckligt hög flexibilitet för att privata lagringsenheter inte tillförde något till det dagliga arbetet. Hen såg överlag positivt på systemet och menade på att den största svårigheten var avvägningen mellan vilken typ av enhet som skulle användas för varje arbetsuppgift. I dagsläget använde hen sig mycket av suftplattor men anade att användningen av bärbara datorer skulle öka i och med att de blir allt smidigare, den stora motiveringen till detta var den delvis bristande kompabiliteten mellan systemen och surfplattor. Slutligen var den intervjuade positivt inställd till kommunens satsning på mer flexibla arbetssätt och möjligheten att fritt kunna välja arbetsplats.

Gällande användningen av molntjänster gav den tillfrågade samma svar som den första telefonintervjun att inga molntjänster användes inom arbetet då inget klartecken getts för detta ännu. Hen fortsatte med att uppge att Microsofts OneNote används under möten för anteckningar, men att dessa endast gick att komma åt via VPN för andra inställda. Hen menade att möjligheten att enkelt kunna synkronisera dokumenten skulle underlätta då det aktuella åtkomstsättet via VPN-tunnlar känns onödigt krångligt.

Intervjun fortsatte sedan med frågor gällande ifall den intervjuade tagit del av kommunens IT-policy eller genomgått någon form av IT-utbildning på arbetsplatsen. Även här överensstämde svaren i hög grad med den första intervjun som gjordes då den tillfrågade inte hade tagit del av någon policy och endast genomgått en övergripande utbildning för många år sedan. Hen trodde och antog att det fanns riktlinjer eller policys uppsatta men kunde inte med säkerhet säga att så var fallet. Trots detta ansåg sig den svarande ha god kontroll på vad som gällde och upplevde att hen följde de regler som finns. Detta antagande baserades i stor del på att den intervjuade inte arbetade med hantering av känsliga uppgifter och arbetade på ett sådant sätt att spridning av information var osannolik. Hen fortsatte med att förklara att den tidigare ståndpunkten grundades i en stark tillit till de etablerade kanalerna och systemen som används och uppgav att det var en mentalitet som många delade, ett antagande att systemen i sig är så pass säkra att så länge dessa används kan väldigt lite gå fel. I samband med detta ställdes frågan om i vilken grad mellan 1 och 5 den intervjuade kände sig delaktig i säkerhetsarbetet, där 1 representerade *inte alls delaktig* och 5 *väldigt delaktig*, och svaret blev då 2.

Sammanfattningsvis var den andra telefonintervjun kortare än den första då den inte kom in på samma sidospår. Trots detta överensstämde svaren till stor del gällande i vilken grad de båda tillfrågade hade tagit del av policydokument och utbildningar. Vissa skillnader uppkom dock kring i vilken grad de uppgav att de hade tillgång till intranätet från privata enheter, även om båda uppgav VPN-anslutning som krav. Överlag överensstämde intervjun med den som utfördes med Baggesen och Bergdahl gällande tillgång till kommunens system och utbredning av mobila enheter, däremot visade den på samma sätt som den första telefonintervjun på betydande brister i arbetet med att kommunicera ut organisationens policy till de anställda.

# 5. Analys

I denna del av uppsatsen presenteras de resultat som vår teoretiska bakgrund och empiriska forskning har sammanställt, samt hur de relaterar till varandra.

## 5.1 BYOD

### 5.1.1 Fördelar med BYOD

Utbredningen av BYOD är ett symptom på ett samhälle som blir att mer digitaliserat och allt mer mobilt. En enskild faktor bakom denna utveckling är svår att finna, de olika författarnas verk som använts i teorin visar på att kombinationen av ett allt mer digitaliserat samhälle och långsiktiga ekonomiska vinster för organisationer som tar till sig arbetssättet ligger till grund (Tabell 1, spridning).

Majoriteten av den tidigare forskningen lyfter fram ökad produktivitet, flexibilitet och genom dessa ökade vinster som motivering för att införa BYOD. Dessa punkter återkom även i den empiriska studien som förväntat. BYOD:s odiskutabla framgångar som arbetssätt och den överlag positiva attityd som den teoretiska studien resulterade i, visade sig dock brista när det kom till konkreta siffror. Av allt material som genomarbetades vad det endast Cisco (2013) som uppgav faktiska data på hur stor ökning av produktivitet eller vinst per anställd som BYOD har potential att medföra.

Den andra sidan av fenomenet, en förändring av samhället i stort, vilken förespråkades främst av Thomson (2012) är av en helt annan karaktär då den kräver en genomgående sociologisk studie för att kunna styrkas vetenskapligt. Thomsons studie baseras i hög grad på statistik kring hur amerikanska collegestudenter ser på användningen av BYOD. Studien visar på en betydligt mer komplex anledning till fenomenets popularitet, att användningen av mobila enheter blivit en så pass etablerad del i vardagen att förbud mot att utnyttja deras potential i arbetet inte accepteras. Denna förändring i hur gemene man använder sig av digitala enheter sätter enligt denna infallsvinkel press på arbetsgivare att skapa de förutsättningarna som krävs för att attrahera personal. Av intervjun hos Uppsala Kommun framgick att även om organisationen inte tillåter användningen av privatägda enheter så använder de sig av en stor variation av olika enheter för att kunna optimera arbetet för olika behov.

Även om dessa skilda teorier var för sig inte förklarar BYOD framgångar så ger de kombinerade en stark motivering till varför BYOD kan vara till fördel för en organisation. Resultaten av uppsatsen visar på en betydligt mer mångfasetterad bild av fenomenet både på gott och ont men saknar hårda fakta över hur stora vinsterna kan bli, ett resultat som inte förväntades vid skrivandes start.

### 5.1.2 Risker och nackdelar med BYOD

På samma vis som med fördelarna av att implementera BYOD så är problematiken bred och varierande beroende på vilken utsträckning systemet införs och inom vilken organisation.
Sammanfattningsvis visar den forskning uppsatsen bygger på att de tre stora riskgrupperna är förlust av kontroll, kontaminering av data och risk för läckage eller förlust av data.

Traditionell IT-baserad verksamhet där organisationen bestämmer vilka enheter som används och på vilket sätt det underlättar både till utveckling av system och skydd av dessa. I och med införandet av BYOD förlorar organisationen i mångt och mycket kontroll över åtkomsten till sina system och den data det hanterar. I de fall där organisationen själva tillhandahåller enheter för de anställda, exempelvis Uppsala Kommun, behålls kontrollen över *vilka* enheter som används men *hur,* och *vart* dessa används står allt som oftast fortfarande utanför organisationens kontroll.

Även om osäkerhet kring vem som har åtkomst till systemen är det mest påtagliga hotet så finns en konsensus i den litteratur som studerats att den bristande medvetenheten kring vart informationen som används på BYOD-enheter hamnar. Det kan få stora konsekvenser för en organisation och även leda till att de förlorar äganderätten till informationen ifall den exempelvis lagras på någon form av molntjänst. (Tabell 1, Risker och nackdelar)
Denna problematik återfinns både i intervjuerna med Uppsala Kommun och i enkätstudien från SLL där båda instanserna visar på brister i medvetenhet gällande spridning av information. SLL ser ett utbrett användande av privata lagringsenheter och publika molntjänser medan Uppsala Kommun ger en bild av att ha striktare förhållningsregler gällande dessa. De anonyma intervjuerna på kommunen visar dock på att det finns ett oaktoriserat användande av privata enheter även här.

Kontaminering av den data som lagras på en organisations servrar är ytterligare en fara som utvecklas i och med introduktionen av BYOD. På samma sätt som med kontroll av informationsflöde så ger en traditionell uppbyggnad av IT-system ett enkelt och effektivt skydd, här med hjälp av ett yttre skyddande skal så som brandväggar för att förhindra att skadlig kod tar sig in i systemen. Oavsett implementeringssätt av BYOD, och om organisationen eller individen själv tillhandahåller enheterna som används, ökar risken att skadlig kod kommer in innanför detta skal och sprids. Här ställs åter båda organisationerna vi undersökte inför en ökad hotbild. Uppsala Kommun ger visserligen inte åtkomst till systemen från privata enheter men då dessa används utanför organisationens nätverk löper de en risk att infekteras av skadlig kod som vid uppkoppling kan spridas vidare internt. Användandet av privata lagringsenheter på SLL ger ett ännu mer konkret exempel på denna risk då dessa enheter helt står utanför organisationens kontroll. Nämnvärt är att frågeställningen hos vardera organisation inte undersökte vilka åtgärder som finns för att hantera skadlig kod och suspekt trafik inom själva systemen, allvaret i dessa riskmoment kan därmed inte säkerställas.

Förlust och spridning av data är starkt kopplat till den första punkten gällande kontroll. Med förlust menas främst fysisk förlust av enheter innehållande känslig data till följd av stöld eller borttappande. Både den tidigare forskning som bearbetats och intervjun på Uppsala Kommun visar på att det finns ett stort mörkertal kring i vilken utsträckning förlust av enheter sker. Även i det fall där förlust rapporteras menar Bergdahl och Baggesen att det i många fall är omöjligt att säkerställa vilken data som gått förlorad och därmed riskerar att hamna i obehöriga händer, ett problem som kommer behöva hanteras i och med det nya datalagringsdirektivet.

## 5.2 Säkerhetsarbete och utbildning

Precis som både teorin (Tabell 1, Åtgärder och riktlinjer) och intervjun med Baggesen och Bergdahl visar så är det viktigt att ha en hög medvetenhet kring vikten av att skydda sig på ett bra sätt, och att man ser till så att de anställda blir utbildade och aktivt tar del av säkerhetsarbetet på en daglig basis.

### 5.2.1 BYOD policy

Precis som teoridelen föreslår är det av yttersta vikt att etablera en BYOD policy om man vill implementera BYOD möjligheter inom ett företag. En BYOD-policy är extremt viktig då den hjälper individer att utbilda sig själva inom säker IT-användning och ger även riktlinjer för hur man får in säkerhetstänket i de dagliga rutinerna (Tabell 1).
Följer arbetet de uppsatta riktlinjerna från BYOD-policyn minimeras även riskerna för lagbrott. En bra policy hjälper också till att klargöra för de anställda vem som äger den data som lagras på privata enheter och vilka åtgärder som kan följa vid förlust av en enhet.

Efter analys av de utförda intervjuerna på Uppsala kommun så var det inte självklart att en BYOD policy behövdes då de inte riktigt hade någon etablerad BYOD-användning.
Dock fanns möjlighet att använda egna enheter förutsatt att man har rätt fabrikat och korrekta inställningar på operativsystem och webbläsare. Utifrån ett framtidsperspektiv lär fenomenet BYOD växa ytterligare, även inom kommunen, och det kan därför vara bra att förbereda policyarbetet och börja förhandla med ledningsgrupperna och kommunfullmäktige för att underlätta arbetet när det blir aktuellt att implementera en policy.

Kommunens nuvarande IT-policy reviderades senast 2009 vilket bör åtgärdas.
Precis som teorin föreslår, bör en policy uppdateras regelbundet, rimligtvis en gång om året för att vara aktuell och användbar. Uppsala kommun har utifrån dessa kriterier ett stort förbättringsarbete framför sig, vilket de är medvetna om.
Utifrån den genomförda enkätstudie har SLL ett ännu större behov av att upprätta en specifik BYOD-policy då de tillåter användning av privata enheter i en större utsträckning.

### 5.2.2 Utbildning av personal

Den viktigaste delen när det kommer till att implementera nya IT-lösningar, införa nya policys och framförallt för att jobba på ett säkert sätt, är att se till att utbilda och upplysa sin personal om säker IT-användning. Det blir ännu viktigare i och med att användningen av privata enheter inom arbetet ökar riskerna med dataförlust.

Litteraturgenomgången visar att den största anledningen till dataförlust är den mänskliga faktorn vilket visar på vikten av att utbilda sin personal så att man minimerar risken för dataförlust (Tabell 1, Åtgärder och riktlinjer).

I intervjun med Bergdahl och Baggesen hade de positiva åsikter kring vikten av utbildningar. Båda tyckte att kommunen bedriver ett otillräckligt arbete när det kommer till att utbilda sin personal inom IT-området. De borde lägga mycket mera tid på att uppdatera sina anställda, och att även utveckla och förbättra deras nuvarande IT-utbildningar.

En annan viktig punkt som togs upp under intervjun var uppföljning av utbildning, Baggesen menade på att det är viktigt att försöka få in säkerhetsarbetet i de dagliga rutinerna, detta genom att integrera de frågor som tas upp under utbildningar i det dagliga arbetet.
Under telefonintervjuerna som utfördes med de anställda på kommunen så togs även frågan om utbildning upp, svaren blev att den ena hade genomgått en väldigt grundläggande utbildning för länge sedan medan den andra inte visste om det fanns någon IT-utbildning. Detta visar på att kommunen borde förbättra sitt arbete gällande utbildningar för anställda. På frågan gällande graden av delaktighet i säkerhetsarbetet mellan 1 och 5 svarade de båda 1 respektive 2. Detta är alarmerande då de anställda på en organisation som behandlar känslig information, till exempel personuppgifter, bör vara delaktiga i säkerhetsarbetet.

Enkätstudien visar att även SLL har ett stort förbättringsarbete att utföra angående utbildningar för anställda. Endast 32 % av de 75 svarande hade genomgått någon form av IT-utbildning vilket återigen är oroande med tanke på att även de dagligen arbetar med känslig information.

### 5.2.3 Skydd av data

Den teoretiska bakgrundsforskningen (Tabell 1, Åtgärder och riktlinjer) pekar på att de ovanstående aspekterna gällande tydligt uppsatta regelverk och utbildning är kritiska för att upprätthålla en god informationssäkerhet då den mänskliga faktorn är det enskilt största hotet. Denna åsikt återkommer i intervjun med Bergdahl och Baggesen i svaret på hur de skulle förbättra säkerheten om de hade fria händer.

En god informationssäkerhet och en smidig implementering av BYOD kräver dock mer än en medveten personalstyrka. Lösenordskyddade enheter, installation av antivirusprogram, kryptering av känslig data och användning av VPN-tunnlar för åtkomst till interna system bidrar alla till att minska risken för läckage av data och kontaminering av systemen.
För att denna implementation ens ska kunna påbörjas krävs en grundlig genomgång av den bakomliggande infrastrukturen för att säkerställa driften av verksamheten.

Vid oundviklig enhetsförlust kan verktyg som Mobile Device Management användas för att via fjärråtkomst låsa ner eller radera all data på en borttappad enhet. Tillsammans med åtkomstinriktade lösningar i form av Access Control Lists och Mobile Content Management kan riskerna för kontaminering och obehörig åtkomst till känslig data minimeras om än inte elimineras helt. (Tabell 1, Åtgärder och riktlinjer)

# 6. Slutsats, diskussion och framtida forskning

Arbetet hade som utgångspunkt att undersöka för- och nackdelarna med att implementera BYOD inom en organisation samt hur det bör ske för att upprätthålla en god informationssäkerhet, den senare med inriktning på arbete kring policys och utbildning.

De fördelar som litteraturstudien lyfte fram var förväntade och passade väl in i de antaganden som gjordes innan arbetet påbörjades. I kontrast till det förmodade resultaten var det dock endast enstaka källor som kunde ge konkreta siffror eller data över hur stora vinster eller ökning av produktivitet BYOD som arbetssätt har potential att medföra. Denna brist på konkreta fakta kring de positiva aspekterna tyder på att urvalet av källor i underlaget kunde varit bättre alternativt att forskningen inom ämnet behöver kompletteras ytterligare. De källor som visar på faktiska resultat ger dock en vink om att en utbredd och genomtänkt implementering av BYOD kan leda till imponerande resultat (Tabell 1, Fördelar med BYOD).

Den ökade hotbilden BYOD medför framgick väldigt tydligt både genom den teoretiska och empiriska forskning som utfördes. Här överraskade dock komplexiteten och utbredningen av hotbilden och flera aspekter hade inte tagits med i beräkningarna då arbetet påbörjades. Sammantaget upplevs resultaten kring studien av för- och nackdelar som tillfredsställande om än något förbryllande rörande de positiva aspekternas brist på konkreta siffror. Slutsatsen kring hur riskerna kan hanteras visar på att en mängd olika parametrar behöver tas i åtanke. Den information en organisation hanterar är avgörande för om en implementering av BYOD är försvarbar och därför bör en tydlig inventering och analys av denna göras innan arbetet fortskrider. Att lägga ner extra tid och resurser för att säkra systemet och samtidigt behålla kontrollen inom organisationen är aspekter som inte alltid verkar få den uppmärksamhet som krävs för att implementera BYOD på ett säkert sätt.

Lösningarna på problemen är många och varierar kraftigt mellan olika författare, samma sak gäller de risker som en organisation kan råka ut för. Beslut om införandet av BYOD bör därför planeras och analyseras ordentligt inom varje enskild organisation då en universell lösning eller mall för hur detta bör ske i dagsläget inte existerar. I de fall då BYOD anses som rätt väg att gå bör organisationen gå igenom all sin IT-verksamhet. Dessutom se till att de har motivationen och resurserna för att upprätthålla en hög nivå på säkerheten genom kontinuerlig utveckling, övervakning och uppföljning av systemet samt utbildning av personal.

De organisationer uppsatsens empiri kom i kontakt med hade båda inslag av BYOD-användning men uppvisade samtidigt betydande brister kring hur personalen informerades och kontrollerades vilket ger en hänvisning till att implementeringen skett utan tillräcklig analys eller planering.

För att fortsätta forska ännu djupare inom ämnet BYOD och hur utvecklingen med BYOD kommer se ut i framtiden skulle man förutom att studera en stor organisation även kunna utföra en studie på mindre företag och även mer IT-relaterade företag för att se skillnader på hur BYOD arbetet ser ut i mindre företag jämfört med stora organisationer, och därav få ett resultat på hur storleken på en organisation påverkar problematiken med att införa, eller upprätthålla BYOD. Ett annat förslag är att formulera om frågeställningen och titta närmare på själva säkerhetsarbetet och utbildning av personal då detta är en stor faktor till att BYOD ska fungera på ett bra sätt inom en organisation.

Resultatet av detta arbete bör kunna vara användbart i framtida forskning då det ger en bred sammanställning av BYOD:s för- och nackdelar, vilket är ett aktuellt och samtidigt relativt nytt forskningsområde.

# 7. Källförteckning


Beckett, P. (2014) *BYOD – popular and problematic*, Network Security, Volume 2014, Issue 9, September 2014, Pages 7-9, ISSN 1353-4858, Hämtad 2016-04-20 från http://dx.doi.org/10.1016/S1353-4858(14)70090-X

Cisco IBSG. (2012). *BYOD A Global Perspective.* Hämtad 2016-04-20 från http://www.cisco.com/c/dam/en_us/about/ac79/docs/re/BYOD_Horizons-Global.pdf

Cisco IBSG Horizons. (2013). *The Financial Impact of BYOD.* Hämtad: 2016-05-09 från *http://www.cisco.com/c/dam/en_us/about/ac79/docs/re/byod/BYOD-Economics_Econ_Analysis.pdf*

D'Arcy, J., Hovav, A., Galletta, D. (2009). *User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research*. Hämtad 2016-04-20 från http://dx.doi.org/10.1287/isre.1070.0160

Eschelbeck, G., Schwartzberg, D. (2012). *BYOD Risks and Rewards How to keep employee smartphones, laptops and tablets secure.* Hämtad 2016-04-21 från http://cloudtss.com/content/BYOD%20Risks%20and%20Rewards.pdf

Gabriel, C. (2013). *No byod policy? Time to grasp the nettle.* Hämtad 2016-04-22 från http://cxounplugged.com/2013/01/byod-policy/

Gartner. (2016). *Worldwide Device Shipments to Grow 1.9 Percent in 2016, While End-User Spending to Decline for the First Time.* Hämtad 2016-05-18 från http://www.gartner.com/newsroom/id/3187134

Hassell, J. (2012) *7 Tips for Establishing a Successful BYOD Policy.* Hämtad 2016-0611 från http://www.cio.com/article/2395944/consumer-technology/7-tips-for-establishing-a-successful-byod-policy.html

Infonetics Reserarch. (2012). *Enterprises rate mobile device security vendors, reveal BYOD concern.* Hämtad 2016-04-20 från http://www.infonetics.com/pr/2012/Enterprise-Mobile-Security-Strategies-Survey-Highlights.asp

Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. *Network Security* Hämtad 2016-04-21 från http://dx.doi.org/10.1016/S1353-4858(12)70111-3

Oates, B. J. (2006). *Researching Information Systems and Computing.* London: SAGE Publications Ltd.

Pillay, A. Diaki, H. Nham, E. Senanayake, S. Tan, G. & Deshpande, S. (2013). *Does BYOD increase risks or drive benefits?*

Securelist. (2014). *Mobile Malware Evolution: 2013.* Hämtad 2016-0615 från https://securelist.com/analysis/kaspersky-security-bulletin/58335/mobile-malware-evolution-2013/

Stockholms läns landsting. (2016). *Så fungerar landstinget.* Hämtad 2016-05-16 från http://www.sll.se/om-landstinget/det-har-ar-landstinget/

Softpedia News. (2014). *56% of Corporate Employees Haven't Had Security Awareness Training*. Hämtad 2016-0215 från http://news.softpedia.com/news/56-of-Corporate-Employees-Haven-t-Had-Security-Awareness-Training-436734.shtml

Thomson, G. (2012) BYOD: enabling the chaos. *Network security.* Hämtad 2016-04-20 från http://dx.doi.org/10.1016/S1353-4858(12)70013-2

TIM Review Magazine. (2016). *IT Consumerization: A Case Study of BYOD in a Healthcare Setting.* Hämtad 2016-04-20 från http://timreview.ca/article/771

Tokuyoshi, B. (2013) The security implications of BYOD. *Network Security.* Hämtad 2016-04-20 från http://dx.doi.org/10.1016/S1353-4858(13)70050-3

Uppsala Kommun. (2016). *Så fungerar kommunen.* Hämtad 2016-05-10 från https://www.uppsala.se/organisation-och-styrning/sa-fungerar-kommunen/

# 8. Bilagor

## 8.1 Intervjufrågor Baggesen och Bergdahl

Nedanstående frågor är hämtade från transkriberingen av intervjun med Baggesen och Bergdahl, då de är tagna ur sin kontext kan de upplevas som vardagliga i språket och hänsyn bör av läsaren tas till att de ställts under ett pågående samtal. Motivet bakom att inte bifoga de ursprungliga frågorna från intervjunplaneringen är att bifogandet av de faktiska frågorna som ställdes ger en klarare bild av hur intervjun utfördes.

- Berätta lite om er själva, vad har ni för arbetsuppgifter här på kommunhuset?
- Hur ser ert säkerhetsarbete ut på en daglig basis?
- Vilka fördelar ser ni med att använda sig av just BYOD inom en verksamhet?
- Om man vänder på det hela, vad ser ni för nackdelar med BYOD?
- Skulle ni säga att det finns några specifika nackdelar eller svårigheter för just kommunen, det här med integritet blir det självklara, men om det finns något annat som man kanske inte alltid funderar eller tänker på?
- Hur används BYOD inom kommunen, i vilken utsträckning? Vi tänker då inte bara på datorer, mobiler och surfplattor, utan även hur det är med portabel lagrings media och sådant.
- Hur anser ni att den här BYOD vågen som har kommit, har den påverkat dels er, men också om ni har upplevt att den har påverkat kommunens anställda, och på vilket sätt?
- Hur ser era policys och regelverk ut, framförallt när det gäller just BYOD men även lite mer generellt också, och på vilket sätt den kommuniceras ut till de anställda, sker det vid anställning? Och hur ser uppföljningen ut?
- Har kommunen nån relaterad IT- utbildning för personalen?
- Hur välinformerade upplever ni att personalen är just när det kommer till säkerhetsarbetet vad det är som gäller när det kommer till regler och policys och annat?
- Vilka typer av incidenter är vanligast?
- Vilka skulle ni säga är de största svårigheterna när det kommer just till utbildning och informering av personal?

- Vilken respons brukar ni få från de anställda rörande policys och utbildningar. Finns det en förståelse för vikten bakom det? Tas informationen på allvar?

- Rent praktiskt när det kommer till just policyarbete och också utbildningsarbete, vad tror ni man skulle kunna ändra på? Har ni, som har hållit på lite mera praktiskt med just det här än vad vi har gjort, vad tycker ni att man ska tänka på? Om ni skulle leva i en drömvärld där ledning och allting förstår precis varför det här är viktigt och ni fick den tid och de resurser som ni ville, hur skulle ni lägga upp en utbildning, hur skulle ni vilja arbeta för att implementera ett ordentligt säkerhetstänk?

- Hur ser ni på framtiden för BYOD, och vad tror ni att det kommer ta vägen? Kommer det att eskalera eller kommer det att svalna av?

## 8.2 Intervjufrågor telefonintervjuer

- Har du möjlighet att använda privata enheter inom jobbet? Här innefattas tillgång till jobbmail eller liknande.

- Tillhandahåller din arbetsplats mobila enheter (bärbara datorer, mobiltelefoner och surfplattor) för dig att använda inom jobbet?

- Har du någon gång lagrat jobbrelaterad information på en privat enhet? (Hit räknas även lagringsenheter så som USB-minnen)

- Använder du dig av någon form av molntjänst (Google Drive, Icloud, One Drive, Dropbox etc)?

- Existerar en policy gällande IT-säkerhet på arbetsplatsen?

- Har du genomgått någon utbildning inom IT-säkerhet på arbetsplatsen?

- Känner du att du har koll på vad som gäller när det kommer till IT-säkerheten på arbetsplatsen? Exempelvis vilka regler som gäller för hantering av känslig data, skydd av inloggningsuppgifter m.m?

- Känner du dig delaktig i säkerhetsarbetet på arbetsplatsen?

- Följer du de regler som finns uppsatta kring IT-säkerhet?

## 8.3 Enkätfrågor

Frågorna listas här i punktform med svarsalternativen som underpunkter i den ordning de dök upp i enkäten. Vid svarsalternativ *övrigt* fick den svarande själv skriva en text.

- Vilket kön anser du dig tillhöra?
    - Kvinna
    - Man
    - Annat/ Vill inte uppge

- Hur gammal är du?
    - 19-29
    - 30-49
    - 50 +

- Har du möjlighet att använda privata enheter inom jobbet? Här innefattas tillgång till jobbmail eller liknande.
    - Ja
    - Nej
    - Vet ej

- Tillhandahåller din arbetsplats mobila enheter (bärbara datorer, mobiltelefoner och surfplattor) för dig att använda inom jobbet?
    - Ja
    - Nej
    - Vet ej

- Har du någon gång lagrat jobbrelaterad information på en privat enhet? Hit räknas även lagringsenheter så som USB-minnen
    - Ja
    - Nej
    - Vet ej
    - Övrigt

- Använder du dig av någon form av molntjänst (Google Drive, Icloud, One Drive, Dropbox etc)?
    - Ja, men endast för privat användning
    - Ja, men endast för jobbrelaterad användning
    - Ja, för både privat och jobbrelaterad användning
    - Nej

- Känner du dig delaktig i säkerhetsarbetet på arbetsplatsen?
    - Ja, väldigt
    - Ja, till en viss mån

    - Ja, lite grann
    - Nej, inte alls
    - Övrigt

- Existerar en policy gällande IT-säkerhet på arbetsplatsen?
    - Ja
    - Nej
    - Vet ej

- Om ja: har du tagit del av denna policy?
    - Ja, via någon form av utbildning/ genomgång
    - Ja, men jag fick leta reda på den själv
    - Nej, jag har inte tagit del av någon policy

- Har du genomgått någon utbildning inom IT-säkerhet på arbetsplatsen?
    - Ja
    - Nej
    - Övrigt

- Känner du att du har koll på vad som gäller när det kommer till IT-säkerheten på arbetsplatsen? Exempelvis vilka regler som gäller för hantering av känslig data, skydd av inloggningsuppgifter m.m?
    - Ja jag har stenkoll
    - Jag har bra koll på vad som gäller men vissa delar är jag osäker på
    - Jag har dålig koll på vad som gäller
    - Jag har ingen koll alls på vad som gäller
    - Övrigt

- Följer du de regler som finns uppsatta kring IT-säkerhet?
    - Ja jag följer alltid de regler som finns uppsatta
    - För det mesta, det har hänt att jag brutit mot de regler som finns uppsatta
    - Jag följer inte reglerna som är uppsatta
    - Vill inte svara / vet ej