Säkerhetspolicys för privata mobila enheter i organisationer

Oscar Larsson
Marcus Persson

LUNDS UNIVERSITET

Kandidatuppsats 15 högskolepoäng
SYSK02, Institutionen för Informatik

Handledare:
Odd Steen

Examinatorer:
Benjamin Weaver
Björn Johansson

Sammanfattning

Titel: Säkerhetspolicys för privata mobila enheter i organisationer

Författare: Oscar Larsson
Marcus Persson

Utgivare: Institutionen för informatik, Lunds Universitet

Handledare: Odd Steen

Examinatorer: Benjamin Weaver
Björn Johansson

Slutseminarium: Maj 2014

Uppsatstyp: Kandidatuppsats

Språk: Svenska

Nyckelord: Privata mobila enheter, BYOD, säkerhetspolicys, säkerhetsaspekter

Abstrakt

Genom en allt mer utbredd användning av privata mobila enheter på arbetsplatser har fler risker medförts till organisationer. Med denna studie vill vi undersöka de olika säkerhetspolicys som organisationer tillämpar för att minska de hot som tillkommer då känslig organisationsinformation används av privata mobila enheter. För att utföra denna studie tar vi hjälp av redan existerande litteratur inom området såväl som ett antal intervjuer där vi frågar IT-ansvariga inom organisationer hur de ser på säkerhetspolicys och beprövade ramverk för just säkerhet rörande privata mobila enheter. Vår studie visar att specifika aspekter för privata mobila enheter i säkerhetspolicys inte är vanligt förekommande. Organisationerna i vår undersökning använder sig av säkerhetspolicys som berör privata mobila enheter men vi har inte kunnat finna några specifika aspekter där policys särskiljer sig för privata mobila enheter jämfört med organisationsägda mobila enhter.

INNEHÅLLSFÖRTECKNING

1 INLEDNING **1**

1.1 PROBLEMOMRÅDE 1

1.2 FORSKNINGSFRÅGA 2

1.3 SYFTE 2

1.4 AVGRÄNSNINGAR 3

1.5 DEFINITIONER 4

1.5.1 SMARTA TELEFONER 4

1.5.2 POLICY 4

1.5.3 PRIVAT MOBIL ENHET 4

2 LITTERATURGENOMGÅNG **5**

2.1 SÄKERHESPOLICYS IDAG 5

2.2 ASPEKTER OCH UTFORMNING AV POLICYS 7

2.2.1 UTFORMNING OCH ASPEKTER 7

2.2.2 JÄMFÖRELSE RAMVERK OCH STANDARDER 10

2.3 KONSEKVENSER AV OTILLRÄCKLIGA POLICYS 12

2.4 ANSVAR OCH JURIDISKA KONSEKVENSER 12

2.5 UTBILDNING 13

2.6 SAMMANFATTNING 14

3 METODISKT TILLVÄGAGÅNGSSÄTT **16**

3.1 VAL AV METOD 17

3.2 VAL AV LITTERATUR 18

3.3 INTERVJU 18

3.4 URVAL AV RESPONDENTER 19

3.5 INTERVJUFRÅGOR 20

3.6 GILTIGHET OCH TILLFÖRLITLIGHET AV VÅR UNDERSÖKNING 23

3.7 KRITIK AV VÅRT METODVAL 24

3.8 ETIK 24

4 EMPIRISKT RESULTAT **26**

4.1 ASPEKTER 26

4.2 UTFORMNING 27

4.3 UTBILDNING OCH ANSVAR 29

5 DISKUSSION **31**

5.1 ORGANISATIONSSTORLEK 31

5.2 ASPEKTER 32

5.3 UTFORMNING 35

5.4 UTBILDNING OCH ANSVAR 36

6 SLUTSATS **38**

6.1 FÖRSLAG TILL VIDARE FORSKNING 41

7 BILAGOR **42**

8 REFERENSER **71**

TABELLFÖRTECKNING

Tabell 5.1 Jämförelse av aspekter mellan respondenterna 32

1 Inledning

Enligt Trendmicro.com's undersökning (2012) börjar många organisationer mer och mer att öppna sina nätverk och sin organisationsdata för mobil teknologi som berör privata enheter. Detta fenomen, även kallat 'BYOD'[1], ställer högre krav på de säkerhetspolicys som organisationer redan har implementerade i sina säkerhetsdokument. Dessa mobila enheter är ofta lätta att använda och ger anställda en större frihet då de inte nödvändigtvis behöver befinna sig inom organisationens väggar. Enligt Trendmicro.com's undersökning (2012) kan detta dock öppna upp för säkerhetsrisker vilket i sin tur tvingar organisationer till att revidera sina nuvarande säkerhetspolicys och förstå de risker som tillkommer med ett friare arbetssätt.

Trots en stor trendökning av BYOD är det enligt ISC undersökning (Suby, 2013) endast 17% av de organisationer som deltog som har en specifik policy för privata mobila enheter (PME) implementerad. Samma undersökning visar också att utbildning är en väldigt viktig del av säkerhetspolicyn. Detta resultat sammanfaller med SANS mobility survey (DeLaGrange, 2012) som tillhandahåller en undersökning där hela 50% av de svarande förlitar sig på utbildning om 'BYOD' för anställda som skydd mot potentiella hot.

I dagsläget finns det en rad olika ramverk och standarder som kan fungera som riktlinjer för organisationer inför en implementation av säkerhetspolicys. Enligt en undersökning gjord av Gartner.com (2013) pekar resultatet mot att 50% av arbetsgivarna inte kommer tillhandahålla mobila enheter till anställda år 2017. Specifika säkerhetspolicys för privatägda mobila enheter kommer med stor sannolikhet att ha väsentlig betydelse i framtida säkerhetspolicys och ämnet är därför intressant att undersöka.

1.1 Problemområde

Vi har valt att fokusera på PME inom organisationer, med en inriktning på specifika policys som används för att säkra användningen av dessa enheter sett från ett informationsäkerhetsperspektiv. För en organisation är det viktigt att preventivt skydda sig mot eventuella situationer där känslig information kan gå förlorad. Ett av de vanligaste sätten information läcks på eller går förlorad är genom okunskap och ignorans från människor varpå tekniska svagheter kan utnyttjas (Siponen, Mahmood, & Pahnila, 2009). Det är därför av största vikt att använda sig av policys och regelverk

1 Bring Your Own Device

för att reglera användningen av mobila enheter som har tillgång till information om organisationen.

Användning av mobila enheter på arbetsplatser är inte något nytt, mobila enheter såsom laptops har länge använts i organisationer. Användandet av PME för att utföra arbetsrelaterade uppgifter är däremot en relativt ny företeelse som fick sin början i och med intågandet av smarta telefoner och surfplattor på marknaden (B. W. Glisson & Storer; W. B. Glisson & Storer, 2013). Samma mönster, men nyare teknik. Innebär detta att det gamla regelverket måste förnyas, eller kan organisationer fortfarande använda sig av samma policys?

Vi har till denna uppsats försökt hitta tidigare forskning som besvarar detta för att undersöka ifall det finns specifika aspekter organisationer måste tänka på när de utformar policys för PME. Genom att söka efter olika nyckelord i ett antal databaser försökte vi finna tidigare forskning inom området. De nyckelord vi använt oss av i olika kombinationer är; policy, BYOD, security, privately owned devices, framework, education, standards, challenges, aspects, implementation, mobile device, research, survey, strategies, consequences.

Då vi inte hittat någon tidigare forskning som behandlar några specifika aspekter för PME leder detta oss till vår forskningsfråga.

1.2 Forskningsfråga

- Använder organisationer sig av säkerhetspolicys för privata mobila enheter för att skydda information?
    - Om organisationer gör det: skiljer sig dessa policys ifrån de policys organisationen har för mobila organisationsenheter?
    - Hur utformar organisationer sina säkerhetspolicys?

1.3 Syfte

Vårt syfte är att göra en explorativ undersökning om huruvida organisationer använder sig av specifika policys rörande PME för att skydda information samt hur dessa eventuellt skiljer sig från policys för mobila organisationsenheter. Vår förhoppning är att försöka definiera vilka nyckelaspekter som bör beaktas vid en definition av policys för PME.

Uppsatsen vänder sig främst till personer inom IT-branschen som är ansvariga för IT-policys, vilka vi tror kan dra nytta av de resultat vi får fram av undersökningen, vid utformningen av framtida säkerhetspolicys.

1.4 Avgränsningar

Vi kommer i första hand att undersöka de säkerhetspolicys som används specifikt för PME, för att kunna återkoppla dessa till uppsatsens syfte att definiera nyckelaspekter rörande säkerhetspolicys för PME.

Uppsatsen kommer framförallt fokusera på smarta telefoner, vilka vår empiriska undersökning kommer byggas kring. Vidare är vår uppfattning att smarta telefoner är ett mer utbrett användningsredskap inom arbetsrelaterade uppgifter än surfplattor och laptops, vad gäller privata enheter, och vi tror därför att det finns mer data att hämta om undersökningen fokuserar på smarta telefoner.

Vi har valt att lägga fokus på policys vid användandet av PME och kommer därför inte utveckla de mer tekniska säkerhetsaspekterna av ett sådant användande. Vissa tekniska aspekter kommer att tas upp för att komplettera och förklara säkerhetspolicys och konsekvenserna av bristfälliga sådana, men själva tekniken har ingen huvudroll i vår uppsats.

1.5 Definitioner

1.5.1 Smarta telefoner

Enligt Zheng och Ni (2005) kan en smart telefon förse användaren med någon form av trådlös kommunikation. Vidare har en smart telefon enligt Zheng och Ni (2005) en processor och kan utföra enkel informationshantering såsom e-mail, kalender och adressbok. Till skillnad från en vanlig telefon kan en smart telefon enligt vår definition utföra datahantering på liknande sätt som en enkel dator.

1.5.2 Policy

För att kunna föra en diskussion kring säkerhetspolicys behövs en definition av vad en policy är. Enligt LeVeque (2006, p. 131, egen översättning) kan en policy beskrivas som "ett påstående rörande beteendet en organisation förväntar sig eller vill avråda ifrån". Al-Hamdani och Dixie (2009, p. 73, egen översättning) skriver att en säkerhetspolicy "förklarar det ansvar som åligger personer som hanterar det tekniska sytemet". Utifrån dessa beskrivningar uppfattar vi det som att en säkerhetspolicy berör ett ansvar och beteende som organisationen uppmanar berörda parter att efterfölja.

Säkerhetspolicys används enligt LeVeque (2006) och Al-Hamdani och Dixie (2009) i organisationer för att preventivt skydda organisationens tillgångar mot olika typer av hot och därigenom minska risken för attacker och missöden.

1.5.3 Privat mobil enhet

Med PME syftar vi till enheter som har förmåga att kommunicera trådlöst och kunna ansluta till internet och som ägs av den anställde. Vår definition av PME innefattar också ett operativsystem som i sin helhet inte är lika utvecklat som en desktopdator eller laptop.

2 Litteraturgenomgång

I detta kapitel presenterar vi till en början en generell bild av säkerhetspolicys och utvecklingen av dessa över tid för att skapa en bild för läsaren vad en policy är. Vi går vidare med att presentera några av de vanligaste standarder och ramverk som finns för att utforma säkerhetspolicys. Vidare presenteras eventuella konsekvenser som kan uppstå för organisationer till följd av dåligt utformade och anpassade policys. Slutligen kommer vi diskutera vikten av utbildning för personal och problematisera kring ansvar och juridiska komplikationer som följer med användning av PME vid arbetsuppgifter.

2.1 Säkerhespolicys idag

Säkerhetspolicys kan idag enligt LeVeque (2006) beskriva vem som förväntas göra vad inom en organisation och utgör grunden för en organisations säkerhetsprogram samt fastställer vem som är ansvarig för säkerhetsstrategin. Vidare skriver LeVeque (2006) att en organisation kan ha olika säkerhetspolicys för olika organisatoriska enheter och en säkerhetspolicy kan omfatta alltifrån formatet på ett lösenord till vem som är ansvarig för vilka säkerhetsaktiviteter.

Säkerhetspolicys idag omfattar alltså ett väldigt brett område i kontrast till tidigare årtionden där policys främst behandlade snävare specifika tjänster i form av e-mail och användning av Internet. Detta ligger helt i linje med Porters (2011) beskrivning av tidig utformning av säkerhetspolicys vilken han hävdar främst fokuserade på kommunikation och procedurer kring detta snarare än det breda område det idag behandlar.

Säkerhetspolicys idag förutsätter ofta att organisationen står som ägare till de mobila enheter som policyn innefattar och därmed också har ett övergripande ansvar för säkerhet, åtkomst, samt andra services för enheten. Enligt en undersökning av ITIC (Eddy, 2014) hade 57 % av de tillfrågade organisationerna idag detaljerade säkerhetspolicys för PME. Som undersökningen visar är det idag vanligt inom organisationer att anställda har sina PME och använder dem både för eget bruk och för utförande av arbete rörande organisationen, vilket även Porter (2011) framhäver. En undersökning av Lumension.com (2014) visar dock att användningen av PME ofta överses av äldre säkerhetspolicys och kommunikationspolicys som inte uppdaterats i takt med teknologin.

En undersökning utförd i Tjeckien (Šedivá, 2013) modellerar användningen av mobila enheter med fem olika nivåer inom organisationer. De lägsta nivåerna rör kommunikation och tillgång till data inom organisationer, vilka Šedivá (2013) hävdar är vanliga användningsområden inom alla organisationer. Därmed blir det också enklare att utforma dessa policys för den typen av användning då det är en relativt vanlig form av användning, även rörande PME. Hantering av mobiler för de högre nivåerna bör enligt Šedivá (2013) skräddarsys för att passa organisationen. Detta är något som kan göras med hjälp av ramverk och riskbedömningar, vilket Smith och Forman (2013) rekommenderar för varje organisation. Dessa ramverk beskriver vi mer ingående i kapitel 2.2.

Hållbara säkerhetspolicys måste alltså formuleras även för PME då det är ett område på frammarsch enligt Fortinets undersökning (BYOD Brings Wave of Unknown Security Threats, 2012). Till skillnad från Smith och Forman (2013) rekommenderar LeVeque (2006) en standard för utformning av säkerhetspolicys som är framtagen av NIST. Strukturen för denna standard bygger på olika grenar av dokument där en central policy reglerar underliggande policys. Genom att utforma en säkerhetspolicy på detta sätt undviker organisationer enorma dokument som blir för komplexa att utveckla och avsluta enligt LeVeque (2006).

Dessutom kan man genom denna struktur eventuellt använda sig av de policys som redan finns utformade och endast införa en gren utifrån eventuella säkerhetspolicys för mobila enheter som redan existerar inom organisationen, vilket verkar rimligt då skillnaden i användning av organisationsägda enheter och privata enheter inte är stor. Enligt NIST's standard (LeVeque, 2006) bör alltså en policy för PME vara en specifik policy och inte ingå i ett större dokument, utan styras av en central policy vilken överliggande reglerar specifika mindre policys.

Idag är det många som rekommenderar att säkerhetspolicys för PME bör innehålla 'Mobile Device Management'(MDM), bland annat föreslår Vishal, Deepak och Lovekesh (2013) att 'MDM' bör anammas för att göra privat användning av mobila enheter säker inom organisationer. Enligt Vishal et al. (2013) är implementationen av 'MDM' ett första steg mot att säkra användningen av PME, och bör därför ingå i en säkerthetspolicy. Detta är en teknisk aspekt av säkerhetspolicys som framhålls av många idag, även NIST's dokument 800-124 (Souppaya & Scarfone, 2013), tillsammans med Jindal (2013) föreslår detta. Även en undersökning av ISC (Suby, 2013) visar på att 'MDM' är något som ofta används för att säkra användningen av PME.

Sammanfattningsvis kan vi konstatera att säkerhetspolicys har utvecklats mycket de senaste decennierna, från att endast beröra hur specifika tjänster bör användas i övergripande dokument, till en rad dokument som beskriver specifika delar och enheter, såsom PME, inom en organisation. Vilket undersökningen av ITIC (Eddy, 2014) visade är det dock många organisationer som fortfarande inte har uppdaterade policys rörande PME, vilket med stor sannolikhet utgör ett stort hot mot organisationen. En av kärnaspekterna rörande hur en säkerhetspolicy för PME ser ut idag verkar vara användningen av 'MDM' för att skapa kontroll över data som används inom organisationen. Med hjälp av ramverk och standarder utformar man idag säkerhetspolicys, något vi i nästa kapitel kommer presentera närmare.

2.2 Aspekter och utformning av policys

Det finns ett flertal olika standarder och ramverk som organisationer kan använda för att skapa säkerhetspolicys. I det följande presenterar vi några av dem som idag är vanligt förekommande.

2.2.1 Utformning och aspekter

Vi har studerat ett flertal olika standarder och ramverk som organisationer använder sig av och kan ta hjälp av inför en implementation av säkerhetspolicys för mobila enheter. Några av de idag vanligare ramverken är NIST (Souppaya & Scarfone, 2013), SANS (Guérin, 2008), CoBIT (Isaca.org, 2014) och ITIL (Itil-officialsite.com, 2014). ISO har utvecklat en standard för att upprätthålla de krav som krävs för ett 'Information Security Management System' (Iso.org, 2014). Gemensamt för dessa olika ramverk är att de har tre viktiga områden som ska styra en implementation av säkerhetspolicys:

- Riktlinjer
- Riskbedömning
- Aspekter

Dessa områden skiljer sig till viss del åt i de olika ramverken men sett ur ett övergripande perspektiv ser de väldigt lika ut. Dessa områden nämns också av Emery (2012) som en förutsättning för att kunna designa en bra säkerhetspolicy.

De policys som återfinns i NIST (Souppaya & Scarfone, 2013) och SANS (Guérin, 2008) dokument innehåller en klassificering av olika mobila enheter samt åtkomster för dessa klasser, såsom enheter ägda av organisationen kontra PME. En klassificering möjliggör en specificering av hur PME bör

hanteras inom organisationen. Trots detta visar undersökningar av både ISC (Suby, 2013) och SANS (DeLaGrange, 2012) att väldigt få organisationer använder sig av policys specifikt utformade för PME. En anledning till att så få organisationer enligt undersökningar inte har policys som är specifikt utformade för PME kan bero på att det helt enkelt inte behövs utmärkande aspekter för PME, något Reyes (2005) underbygger när hon skriver att vissa aspekter bör ingå i alla säkerhetspolicys.

Som exempel kan nämnas Govloops (P. Fiorenza, 2013; P. Fiorenza, Tepe, L., Ribeira, J., Vogel, V.) undersökning som visar på att uppgifter såsom e-mail och kalenderhantering är de vanligaste förekommande arbetsuppgifterna när det kommer till privat mobil hantering. Dessa arbetsuppgifter skiljer sig inte nämnvärt åt ifall det rör sig om organisationsägda eller PME och kan tänkas vara en anledning till att många organisationer enligt ICS (Suby, 2013) och SANS Mobility Survey (DeLaGrange, 2012) inte använder sig av någon specifik säkerhetspolicy för PME. NIST's (Souppaya & Scarfone, 2013) dokument 800-124 saknar exempelvis en specifik sektion som behandlar PME, och rekommenderar snarare en mer generell övergripande policy oavsett vilken klassificering av mobila enheter det rör.

Trots att undersökningarna visar på en liten skillnad rörande klassificeringen av mobila enheter har de ramverk vi undersökt en del viktiga aspekter som bör ses över när det gäller säkerhetspolicys. Både Carrillo (2013) och Reyes (2005) betonar hur viktigt det är med planering och efterforskning innan en säkerhetspolicys utformas och att involverade förstår organisationens krav innan policyn implementeras. Souppaya och Scarfone (2013) rekommenderar även att säkerhetspolicys för mobila enheter bör komplettera och vara konsekventa rörande övriga säkerhetspolicys inom organisationen som inte rör mobila enheter. Guérins (2008) mall kompletterar exempelvis ISO 27001 rörande bland annat privata handhållna enheter och hur de bör hanteras.

Enligt Reyes (2005) bör de aspekter som rekommenderas inkluderas oavsett vilket område säkerhetspolicyn rör, vilket talar för att dessa delar även bör användas som en grund för en säkerhetspolicy som rör PME. Whitman och Mattord (2013) har utvecklat ett ramverk för att ta fram en policy som rör just ‘BYOD’ och i denna återfinns samma aspekter som i Reyes (2005) mer generella utformning och som i många av de standarder och ramverk vi undersökt. Detta talar för att säkerhetspolicys för olika klassificeringar av mobila enheter nödvändigtvis inte måste se

annorlunda ut. Det viktiga verkar snarare vara att specificera att policyn även gäller PME, och eventuella tekniska aspekter som är nödvändiga särskilt för PME.

Även utbildning för sådan hantering verkar vara något som är nödvändigt. Utbildning är en aspekt som också återfinns i många av de ramverk och standarder vi studerat, såsom NIST (Souppaya & Scarfone, 2013), SANS (Guérin, 2008), ISO (Iso.org, 2014) och även Emery (2012) nämner detta i sin undersökning. Undersökningar av SANS Mobility Survey (DeLaGrange, 2012), Govloop (P. Fiorenza, 2013) och ICS (Suby, 2013) styrker detta påstående och visar att utbildning är en av de viktigaste faktorerna för att skydda sig mot hot som kan uppstå vid användning av PME. Det bör därför specificeras i säkerhetspolicyn hur utbildning av anställda ska ske för just PME.

Med hjälp av de aspekter som tas upp i de olika ramverken kan organisationen göra en riskbedömning för att bestämma hur policyn skall utformas. Tanken med riskbedömningen är inte att gå på djupet utan generellt klassificera och kategorisera olika risker enligt Reyes (2005). Riskbedömning anses som en viktig del av en säkerhetspolicy och går att finna i alla ramverk vi undersökt.

Vidare har vi i många standarder och ramverk funnit en rekommendation av tekniska tillämpningar för att skydda organisationen mot säkerhetshot vid användning av PME. En av de vanligast förekommande teknikerna är ‘MDM’, vilken också omnämns i SANS Mobility Survey (DeLaGrange, 2012) och ISC's (Suby, 2013) undersökningar som ett av de vanligaste redskapen för att skydda sig, och således verkar denna tekniska aspekt vara viktig att ha med i en säkerhetspolicy. Emery (2012) nämner också sex olika tekniska aspekter som bör specificeras i en policy för ‘BYOD’ för att skydda organisationen mot att data läcks. Tekniska lösningar såsom ‘MDM’ kan hjälpa organisationer att kontrollera sin information så den inte sprids på ett felaktigt sätt. En undersökning av Fortinet (Micrographics & optical Technology, 2011) visar nämligen att 30 % av dem tillfrågade kunde tänka sig att bryta policys och använda förbjudna applikationer. Det räcker därför inte med säkerhetspolicys som beskriver hur anställda bör bete sig utan även tekniska lösningar bör specificeras i policyn för att organisationer ska kunna skydda sig mot sådana hot.

2.2.2 Jämförelse ramverk och standarder

Utifrån vår litterära undersökning av olika ramverk och standarder kan vi konstatera att det finns en viss grundstruktur för säkerhetspolicys. Både Guérins (2008) mall, NIST's dokument 800-124 (Souppaya & Scarfone, 2013), Reyes (2005) och Whitman och Mattords (2013) förslag på säkerhetspolicys har samma aspekter liggandes till grund för en säkerhetspolicys uppbyggnad. Guérins (2008) mall bygger på ISO 27001 (Elachgar & Regragui, 2012), vilken även innehåller liknande aspekter men mer generella.

Dessa olika standarder beskriver inte enhälligt en struktur för privata mobila säkerhetspolicys, men då de rekommenderar en generell struktur för säkerhetspolicys är dessa aspekter något som även måste beaktas då en säkerhetspolicy för PME utformas i en organisation.
Nedan följer en sammanställning med de aspekter som nämnda författare rekommenderar;

- Förklaring av policy
- Publik för policy
- Identifiering av tillgångar
- Potentiella hot
- Roller och ansvar
- Säkerhetsträning
- Backup
- Fysisk säkerhet
- Åtkomstkontroll
- Autentisering
- Nätverkssäkerhet
- Kryptering
- Godtagbar användning
- Granskning och översyn
- Efterlevnad

Utöver dessa generella aspekter av säkerhetspolicys återfinns även en del rekommendationer rörande PME i standarderna. Souppaya och Scarfone (2013) uppmanar organisationer att använda

sig av 'sandboxing[2]' eller 'device integrity scanning application[3]' vid användning av PME för att säkerställa dem, något som kan kombineras med 'MDM', vilket Jindal (2013) rekommenderar. Vidare rekommenderar Souppaya och Scarfone (2013) att en organisation bör använda sig av olika säkerhetslager rörande behörighet inom organisationen där en klassificering av privat- eller organisationsägda enheter bör definieras.

Guérins (2008) mall beskriver en liknande klassificering av privata- eller organisationsägda mobila enheter vid olika säkerhetszoner samt ett förbud mot att koppla upp sig mot organisationens nätverk ifall enheterna inte är registrerade hos IT-avdelningen. De båda standarderna skiljer sig dock åt då Guérins (2008) mall beskriver vilka påföljder en avvikelse från policyn kan innebära, något Souppaya och Scarfone (2013) inte tar upp.

De objekt vi beskrivit här skiljer sig ifrån ramverken CoBIT och ITIL vilka inte specifikt beskriver detaljerad information kring vilka aspekter en säkerhetspolicy bör innehålla. Dessa ramverk erbjuder snarare verktyg för att kunna göra riskbedömningar, vilka senare kan resultera i säkerhetspolicys.

Brand (2013) har studerat CoBIT, ITIL och ISO 27001 och sammanställt en best practise för hantering av mobila säkerhetsrisker, vilken innehåller några av de aspekter som kan ses i ovanstående sammanfattning. Enligt Brand (2013) kan utformningen av säkerhetspolicys för att hantera mobila säkerhetsrisker ske med hjälp av 'Goosen's ramverk'. 'Goosen's ramverk' kombinerar CoBIT, ITIL och ISO 27001 genom att organisationen i ett initialt skede identifierar processer där det finns säkerhetsrisker med hjälp av CoBIT, för att sedan knyta dessa till ITIL, och eventuellt till vissa delar inom ISO 27000 eller dess släktingar. Detta tillvägagångssätt är alltså en mer skräddarsydd utformning av säkerhetspolicys än att använda Guérins (2008) mall eller Souppaya och Scarfones (2013) standarder.

2 Användning av virtuell teknik för att exekvera applikationer i en egen behållare (Greamo & Ghosh, 2011)
3 Scan för att upptäcka om operativsystemet har blivit kompromissat genom malware (Stigviewer.com, 2014)

2.3 Konsekvenser av otillräckliga policys

Användningen av PME i organisationer upplevs av många som ett stort säkerhetshot. I en studie av Fortinet (BYOD Brings Wave of Unknown Security Threats, 2012) ansåg hela 42 % av respondenterna att PME utgjorde ett potentiellt hot mot organisationen i form av dataförlust och exponering för IT-hot. Dessa risker är även stora orosmoln enligt Khanna (2013) där hela 62 % ser PME som det största säkerhetshotet mot organisationen. Enligt en sammanställning från Ey.com (2014) är dock sannolikheten att nya säkerhetsrisker uppstår till följd av att PME används till arbetsuppgifter låg. Däremot är det sannolikt att redan identifierade säkerhetsrisker ökar.

Att risken för läckage av information hamnar så högt i Fortinets undersökning indikerar att välformulerade säkerhetspolicys, som tydligt beskriver hantering av nämnda risker, är vitalt för organisationer idag. En undersökning av ITIC (Eddy, 2014) nämner säkerhetstestning och utbildning av personal som de vanligaste åtgärderna för att skydda sig. Detta belyser även vikten av säkerhetsutbildning för anställda, och vikten av att inkludera en formulering kring hur det hanteras i en säkerhetspolicy för PME. Undersökningen av ITIC (Eddy, 2014) visar dock på att organisationer som deltog i undersökningen var medvetna om den ökade exponeringen för IT-hot och mer än 57 % hade vid tillfället en policy för PME implementerad.

2.4 Ansvar och juridiska konsekvenser

Samtliga ramverk och standarder för säkerhetspolicys som vi undersökt uttrycker tydligt att organisationer ska tilldela olika ansvarsområden till de olika roller som finns inom organisationen. Guérin (2008) nämner specifikt att för varje roll ska namn till tillhörande roll registreras hos IT-säkerhets avdelningen och individer är inte begränsade till endast ett ansvarsområde och kan anta flera olika roller inom policyn.

Samtliga undersökta standarder och ramverk har fördefinierade roller som har som funktion att se till att de olika policys som existerar följs och används av samtliga inom organisationen. Olika roller har olika ansvarsområden, exempelvis 'IT-governance' som ska se till att säkerhetspolicys underhålls (Carrillo, 2013; Guérin, 2008; Sheikhpour & Modiri, 2012; Souppaya & Scarfone, 2013).

Varje enskild anställd inom organisationen har ett eget ansvar för att skydda sin mobila enhet från felanvändning och avslöjande av privat information som erhålls av organisationen (Guérin, 2008).

Missbruk av detta ansvar kan leda till en rad olika konsekvenser för användaren. Överträdelse av säkerhetspolicys, vare sig det är uppsåtligt eller oaktsamt, kan leda till diciplinära åtgärder eller rättsliga påföljder och bör enligt Guérin (2008) och Reyes (2005) specificeras i säkerhetspolicyn. Disciplinära åtgärder kan enligt Guérin (2008) skildra sig i avskedning eller mindre avstängningar medan de rättsliga påföljderna kan dömmas i olika grad beroende på applicerbar lag.
Här följer ett exempel på de ansvarsroller Guérin (2008) föreslår i säkerhetspolicyn;

- 'Business owner' - Ser till att IT-avdelningen har de resurser som behövs.
- 'IT governance' - Bibehåller säkerhetspolicys samt ser till att användare har tillräcklig utbildning
- 'IT department' - Är ansvariga för att policys följs av användare/anställda samt att services finns tillgängliga
- 'Users/employees' - Måste läsa och förstå säkerhetspolicys samt följa dem dagligen

2.5 Utbildning

Viktigt att tänka på vid utformning av säkerhetspolicys är att inkludera säkerhetsträning och skapa en säkerhetsmedvetenhet hos personalen. Siponen et al. (2009) skriver att det största hotet mot organisationer är vårdslösa anställda som inte följer organisationens säkerhetspolicys. Även Glisson och Storer (2013) hävdar att det är allmänt erkänt att den mänskliga faktorn ligger bakom större delen av informationsförluster vid incidenter.

Ett preventivt försvar mot denna typ av informationsförluster är att organisationen har ett program för personal där utbildning och medvetenhet kring säkerhet lärs ut (Bin Muhaya, Fazl e, & Ali Minhas, 2012). Säkerhetsträningen bör förse de anställda med kunskap och kännedom kring vilka policys som råder inom organisationen och hur de ska efterlevas. Bulgurcu et al. (2010) poängterar att kännedom om organisationens säkerhetspolicys inte ska förväxlas med allmän kännedom kring säkerhet. Som exempel beskrivs att en användare kan ha kännedom kring att ett starkt lösenord krävs, men sakna kunskap om att organisationens säkerhetspolicy kräver att lösenordet ändras periodiskt. Därför är det viktigt att en definition av vad säkerhetsträningen bör bestå av fastställs i säkerhetspolicyn. Framförallt för att klargöra om särskild träning eller utbildning krävs för användning av PME.

2.6 Sammanfattning

Efter vår litteraturgenomgång kan vi konstatera att det primärt finns två olika vägar att gå för organisationer vid en utformning av säkerhetspolicys;

- Använda befintliga mallar med kriterier
- Använda sig av ramverk med riskbedömningar

Genom att använda sig av befintliga mallar, som ISO 27001 och Guérins (2008) mall, blir det tydligt vilka aspekter som bör finnas med i en organisations säkerhetspolicy. Utifrån vår litteraturgenomgång har det blivit tydligt att aspekter i en säkerhetspolicy kan klassificeras utifrån PME och organisationsenheter.

Om organisationer väljer att utforma sina säkerhetspolicys genom att använda sig av ramverk, likt CoBIT och ITIL, eller en kombination av de båda enligt 'Goosens ramverk' (Brand, 2013), krävs en riskbedömning för att reda ut vilka aspekter som krävs för säkerhetspolicyn. Detta tillvägagångssätt ger en mer skräddarsydd säkerhetspolicy för organisationen. Då detta sätt att utforma en säkerhetspolicy utifrån litteraturgenomgången inte gett lika tydliga indikationer kring vad som specifikt ska beröra PME leder detta oss till en empirisk undersökning.

Vi kommer att gå vidare med en empirisk undersökning för att ta reda på hur organisationer utformar sina säkerhetspolicys för mobila enheter samt reda ut om det finns aspekter som särskilt rör PME. Det kan tänkas att det finns hittills onämnda aspekter som är viktiga att tänka på, vilka upptäcks först genom interna riskbedömningar som görs vid användning av ramverk. Vad vi kunnat konstatera utifrån vår litteraturundersökning skiljer sig säkerhetspolicys rörande privata och organisatoriska mobila enheter inte mycket åt.

Utöver de säkerhetspolicys som inte skiljer sig åt rörande privat- och organiationsägda mobila enheter har vi definierat sex specifika aspeker som rör PME;

- Registrering av privata mobila enheter
- Beskrivning av lämplig träning och utbildning för användning
- Definiera säkerhetslager med klassificering

- Använda sandboxing och device integrity application och 'MDM'
- Speciella säkerhetszoner för privata mobila enheter
- Specificera tillåtna uppkopplingssätt för privata enheter mot organisationsenheter

3 Metodiskt tillvägagångssätt

Målet med vår empiriska undersökning är att ta reda på hur organisationer utformar sina säkerhetspolicys för PME samt reda ut om det finns aspekter som särskilt rör PME.

Genom vår litteraturundersökning har vi identifierat ett antal aspekter som återkommit i olika standarder och ramverk och som vi uppfattar vara en viktig grund vid utformningen av privata mobila säkerhetspolicys. Data vi kommer samla in och som vi ser som nödvändig för att kunna dra en slutsats kring forskningsfrågan kan delas in i tre olika områden vilka vi i litteraturgenomgången funnit utgöra stommen för säkerhetspolicys;

1. Aspekter

Inom detta området vill vi ta reda på vilka specifika aspekter det finns som utmärker säkerhetspolicys rörande PME och ifall det finns aspekter som är mer utmärkande än andra.

2. Utformning

Vi vill med detta området ta reda på hur säkerhetspolicys utformas inom organisationen och om utformningen har någon påverkan på vilka specifika aspekter som definieras och används.

3. Utbildning och ansvar

Även utbildning och ansvar är viktiga områden vad gäller säkerhetspolicys och vi vill med hjälp av denna data försöka ta reda på om organisationer inkluderar efterlevnad och utbildning i säkerhetspolicys samt vilka ansvarsområden och roller som specificeras för att säkerställa en säker framtid.

3.1 Val av metod

Eftersom vår forskningsfråga syftar till att undersöka om organisationer använder sig av specifika aspekter rörande säkerhetspolicys för PME var vi i ett tidigt skede av vårt arbete inriktade på att göra en kvantitativ empirisk undersökning. En sådan enkätundersökning verkade i ett initialt skede lämplig för att kunna sammanställa potentiella aspekter. Längre in i arbetet blev det dock uppenbart att en kvalitativ undersökning i form av intervjuer var att föredra. Främst med anledning av att vi med undersökningen behövde nå ut till en IT-ansvarig inom organisationen för att kunna försäkra oss om att respondenten kunde svara på de frågor vi behövde få svar på. Detta upplevde vi kunde bli svårt med ett utskick av en enkät.

Genom att använda oss av en kvalitativ undersökningsmetod fick vi även möjlighet att ställa följdfrågor vilket gav oss en mer ingående sammanfattning av våra huvudfrågor och i sin tur ett större djup på vår insamlade data. En kvalitativ undersökning skulle även tillåta oss att utföra en karaktäriserad generalisering av insamlad data. Av dessa anledningar beslutade vi därför att enligt Jacobsen et al. (2002) rekommendationer göra en deduktiv undersökning i form av kvalitativa intervjuer istället. Vi skickade ut intervjuförfrågningar till 23 olika organisationer som matchade våra urvalskriterier och av dessa var det endast fem som valde att ställa upp i undersökningen.

Respondenter för vår undersökning är främst IT-säkerhetsansvariga inom de organisationer som vi valt ut för undersökningen. Genom vår litteraturgenomgång av forskningsfrågan har vi framställt en rad aspekter av privata mobila säkerhetspolicys som ligger till grund för den empiriska undersökning vi kommer utföra. Den empiriska undersökningen samt den litterära undersökningen kommer att sammanställas för att de likheter och olikheter som finns mellan en teoretisk värld (litterära undersökningen) och en praktisk värld (empiriska resultat) ska kunna diskuteras. Genom att utföra denna analys hoppas vi kunna besvara våra forskningsfrågor och ta reda på vilka specifika aspekter organisationer använder sig av i säkerhetspolicys för PME och hur utformningen av dessa kan se ut.

3.2 Val av litteratur

Större delen av vår litteraturgenomgång bygger på akademiska artiklar från LUBSearch artikeldatabas. Eftersom vår forskningsfråga rör ett relativt nytt område och det är först på senare år som organisationer har börjat utforma specifika säkerhetspolicys rörande PME medför detta att informationspoolen i ämnet är något begränsad. Vi har därför främst varit hänvisade till artiklar inriktade på generell IT-säkerhet och policyutformning för att skapa en teoretisk grund för vår empiriska undersökning. Vi har också med anledning av det begränsade utbudet av artiklar undersökt många ramverk och standarder, dels då vår forskningsfråga behandlar det, dels för att skapa oss en teoretisk bild kring säkerhetspolicys. Vidare har vi också sökt teori i litteratur som vi använt oss av under vår utbildning.

3.3 Intervju

Vi valde att använda oss av en öppen intervjuteknik (Jacobsen et al., 2002) där vi hade ett antal grundfrågor vilka vi utgick ifrån under intervjun och byggde vidare beroende på utfall under intervjuns gång. Detta val baserades på att vi inte riktigt visste vilket resultat vi kunde förvänta oss. Vi intervjuade också relativt få respondenter, då det enligt Jacobsen et al. (2002) är väldigt tidskrävande med öppna intervjuer, och därför passar de bäst för få respondenter där informationsmängden blir väldigt omfattande.

Intervjuerna utspelade sig någonstans mot det helt öppna hållet i Jacobsen et al. (2002) struktureringslandskap, med fast ordningsföljd och endast öppna svar. Användningen av en förstrukturering gör enligt Jacobsen et al. (2002) att vissa aspekter kan fokuseras på mer under intervjun, vilket gagnar vårt ämne, där vi går in med en mer generell överblick men vill komma ut med mer specifika aspekter.

Vi har även valt att utföra intervjun en gång, då det är alltför tidskrävande med upprepade intervjuer för denna uppsats. Vid oklarheter i intervjun har vi i efterhand via respondenterna per email eller telefon försökt få svar på oklarheterna.

3.4 Urval av respondenter

Vid urval av våra respondenter valde vi att inte begränsa oss till en viss sektor utan vi har med respondenter från såväl offentliga som privata organisationer. Vi valde att ha med både stora och små organisationer i vår undersökning. Detta val gjorde vi då vi ansåg det viktigt att ta del av säkerhetspolicys från olika stora organisationer för att i vår empiriska del kunna dra eventuella slutsatser rörande huruvida detta påverkar utformning och användning av säkerhetspolicys.

Vi har begränsat oss till organisationer verksamma främst i Skåneregionen då vi föredrog att göra en intervju på plats, dock hade vissa av dem tillfrågade organisationerna centralstyrda säkerhetspolicys vilket gjorde att en intervju inte blev möjlig.

Vi skickade ut intervjuförfrågningar till 23 organisationer i Skåneregionen varav fem svarade att de hade möjlighet att delta. Vissa av organisationerna angav som anledning till att de tackade nej att det rörde deras säkerhet och att de av denna anledning inte ville delta. De flesta organisationer gav dock ingen anledning till varför de inte ville delta i vår undersökning. Av de fem organisationer som deltog i vår undersökning var det tre offentliga och två privata organisationer. Efter det första urvalet av respondenter var vi tydliga i våra utskick med att efterfråga huruvida organisationen använder sig av PME till arbetsrelaterade uppgifter för att undvika slöseri med både vår och respondentens tid.

Vi har valt respondenter inom organisationerna som har en roll som ansvarar för säkerhetspolicys eller IT, då respondenten annars förmodligen inte haft den kunskap om ämnet som krävs för att kunna svara på våra frågor. Vi skickade ut intervjufrågorna innan intervjun så att respondenterna skulle ha kännedom om dem och kunna förbereda sig, alternativt tacka nej ifall de ansåg att organisationen inte var relevant för vårt område.

R1 är en mindre organisation med 30 anställda i dagsläget. Den respondent som deltog i vår intervju var ansvarig för verksamheten.

R2 är en mindre organisation med 73 anställda i dagsläget. Den respondent som deltog i vår intervju var IT-ansvarig.

R3 är en större offentlig organisation med 21000 anställda. Den respondent som deltog i vår intervju var samordnare för organisationens informationssäkerhetsarbete.

R4 är en större offentlig organisation med 1200 anställda. Den respondent som deltog i vår intervju var IT- och servicechef.

R5 är en större offentlig organisation med 6000 anställda. Den respondent som deltog i vår intervju var IT-chef.

3.5 Intervjufrågor

Våra intervjufrågor är baserade på den teoretiska del vi har belyst i kapitel 2. Utifrån denna del har vi utformat intervjufrågorna för att kunna diskutera de teoretiska aspekterna av vår forskningsfråga som vi funnit i litteraturgenomgången med det empiriska resultat vi hoppas uppnå.

Det vi främst ville få reda på under våra intervjuer var om organisationerna använder sig av specifika aspekter i säkerhetspolicys för PME, och ifall de aspekter vi identifierade i litteraturgenomgången isåfall används. Vidare försökte vi reda ut hur säkerhetspolicys efterlevs och vem som ansvarar för att detta dokumenteras och följs samt hur utformningen av dessa ser ut.

Nedan följer en kort beskrivning av våra intervjufrågor och en koppling till de områden vi specificerade inledningsvis i kapitel 3.

Område: Aspekter

- *Har ni specifika säkerhetspolicys för privata mobila enheter?*
  Detta är vår forskningsfråga och därför viktig fråga för att kunna fastställa om organisationen har specifika säkerhetspolicys för PME eller endast för mobila enheter inom organisationen.

- *I hur stor utsträckning används privata enheter för arbetsuppgifter? Är det alla anställda som har tillåtelse att använda privata enheter?*
  Denna fråga är utformad för att kunna utvärdera frågan som tidigare ställts om specifika

säkerhetspolicys finns inom organisationen eller ej. Denna frågan gör att vi vidare kan analysera resultatet av föregående fråga.

- *Registreras privata mobila enheter på något sätt inom organisationen?*
  Frågan baseras på en av de sex specifika aspekter som rör mobila enheter och intressant för att få reda på om organisationen håller någon form av arkiv för vilka enheter som kan kopplas upp mot deras nätverk.

- *Rekommenderar säkerhetspolicyn tekniska applikationer för att följa säkerheten? Vilka, och är dessa obligatoriska? Specifika applikationer för olika OS?*
  Precis som föregående fråga är denna en av sex specifika aspekter som rör mobila enheter och är relevant för att få reda på hur organisationen ser till att deras data hålls säker när det gäller användning av PME.

- *Vilket operativsystem är vanligast bland organisationsägda respektive privata enheter?*
  Denna fråga är intressant för att få reda på hur och vilka säkerhetskrav som finns för just de enheterna, vilka program som körs och hur organisationen gör ifall de tillåter fler än en typ av mobil enhet.

- *Skiljer säkerhetspolicyn sig rörande privata kontra organisationsägda enheter? Vilka aspekter skiljer sig isåfall åt?*
  Syftet med denna fråga är att få reda på om de specifika aspekter vi har i vår teoretiska del överenstämmer med aspekter som organisationen själv har utformat för privata enheter.

- *Specificeras tillåtna uppkopplingssätt för mobila enheter mot nätverket i säkerhetspolicyn? Är det olika för privata kontra organisationsägda enheter?*
  Syftet med denna fråga är att få en uppfattning om vilka säkerhetsaspekter organisationen använder sig av, mer åt det tekniska hållet som VPN användning exempelvis.

- *Vilka aspekter anser du är viktigast vid utformningen av säkerhetspolicys för privata mobila enheter?*
  Genom att ställa denna intervjufråga får vi en bättre översikt rörande vilka aspekter som olika organisationer anser viktigast vid utformning av säkerhetspolicys och gör det möjligt för oss att analysera denna data gentemot den teoretiska grund vi skapat innan intervjufasen.

Område: Utformning

- *Hur har ni utformat era säkerhetspolicys för privata mobila enheter? Ex. använt er av ramverk, ISO?*
  Eftersom vi i vår teoretiska undersökning behandlar både ramverk och färdiga standarder är det intressant att veta vad de har för grund för sin utformning av säkerhetspolicys.

Område: Utbildning och ansvar

- *Har ni någon form av utbildning rörande säkerhetspolicys och hur dessa skall följas? Är denna isåfall obligatorisk?*
  Många artiklar inom området 'BYOD' anser att utbildning är en viktig del av säkerhetspolicys och en av de viktigaste aspekterna när det kommer till utformning av säkerhetspolicys.

- *Vem ansvarar för att era säkerhetspolicys hålls uppdaterade? Hur ofta ses de över? Har ni någon klassificering av roller i er säkerhetspolicy?*
  Roller är en viktig aspekt inom säkerhetspolicys och därför relevant för vår frågeställning, denna fråga kan leda till att vi får en förståelse för hur viktiga säkerhetspolicys är för organisationen då de genom att ha dedikerade roller för policys visar på ett aktivt intresse för att de uppehålls och uppdateras.

- *Hur efterlevs säkerhetspolicyn av anställda? Hur ser ni till att alla anställda tar del av den?*
  Efterlevnad är en viktig aspekt enligt samtliga författare till de ramverk vi har tagit upp i uppsatsen och detta berör även utbildning.

- *Hur hanteras privata mobila enheter när någon slutar? Tas några speciella åtgärder?*
  Intressant att se hur organisationerna hanterar detta problem. Möjligen finns det legala komplikationer vilket medför att organisationerna inte kan vidta nödvändiga åtgärder.

Övriga frågor

- *Tillhandahåller ni organisationsägda mobila enheter till anställda?*
  Intressant att veta ifall organisationen tillåter både PME och organisationsägda, och i vilken utsträckning anställda använder båda, och om det är tillåtet. Dessutom, vilken skillnad finns det på enheterna, är det samma applikationer som krävs?

- *Vilka anser du är de största hoten med att anställda använder privata mobila enheter?*
  Intressant att veta om organisationen anser att det finns fler tekniska eller otekniska hot när det kommer till 'BYOD'.

3.6 Giltighet och tillförlitlighet av vår undersökning

För att skapa en giltighet och tillförlitlighet rörande vårt empiriska resultat har vi följt Jacobsen et al. (2002) rekommendationer för ett kritiskt förhållningssätt vad gäller våra intervjuer. Vi har vidtagit en rad åtgärder vilka vi nedan redovisar för att försäkra oss om att det empiriska resultatet ska gå att använda i vår slutsats.

Vi har kategoriserat våra intervjufrågor utifrån de olika områden som vi i litteraturdelen funnit utgöra stommen för säkerhetspolicys för att vara säkra på att det vi frågar faktiskt är relevant för vår undersökning. Vidare har vi skickat ut intervjufrågorna till respondenterna i förväg så att de hunnit sätta sig in i frågorna och eventuellt ta reda på fakta de var osäkra på. Våra respondenter har innehaft positioner som innebär att de är ansvariga för säkerhetspolicys inom de olika organisationerna, vilket medför att dem haft god kännedom kring ämnet och de frågor vi har ställt.

Under intervjuerna har vi gjort ljudupptagningar vilka vi senare har transkriberat för att inte gå miste om viktig information som respondenterna delgett. Transkripten har också skickats ut till respondenterna för validering. Slutligen har alla respondenter blivit upplysta om förutsättningar för intervjun, att materialet kommer att publiceras, att de är fullständigt anonyma och att de inte behöver svara på frågorna ifall dem inte vill. Detta kan öka trovärdigheten på respondenternas svar då incitamenten att undanhålla information minskar.

3.7 Kritik av vårt metodval

Att göra en intervju rörande säkerhetspolicys kan vara problematiskt då det handlar om känslig information om en organisation och respondenten kan välja att undanhålla fakta rörande vissa frågor.

Genom att göra en intervju tillkommer det problem rörande tolkning. Vårt val av en öppen intervju kan innebära att frågorna tolkas på olika sätt beroende på olika omständigheter, och följdfrågor kan formuleras på olika sätt. Detta kan innebära att svaren från respondenterna varierar trots att intentionen bakom intervjufrågorna var samma vid de olika tillfällena och respondenterna kanske hade samma svar egentligen.

Antalet intervjuobjekt för denna undersökning är fem, detta gör slutsatsen till en kvalitativ generalisering enligt Jacobsen et al. (2002). Vårt val av stora och små organisationer som intervjuobjekt innebär att resultatet av vår empiriska undersökning i viss mån kan vara representativt för denna typ av organisationer. Vår undersökningsmetod, och antalet intervjuobjekt, kan innebära att slutsatsen är sannolik, men detta är svårt att bevisa.

3.8 Etik

Vi utförde den empiriska undersökningen enligt tre grundkrav som bör beaktas då man utför en intervju: informerat samtycke, krav på privatliv samt krav på att bli korrekt återgiven (Jacobsen et al., 2002).

Genom att utgå ifrån dessa krav då vi utförde intervjuerna såg vi till att vi följde vissa etiska principer. Viktigt är att respondenten inte har fått påtryckningar uppifrån, d.v.s. från chefer. Vi har under vår mejlutskickning skickat vår intervjuförfrågan direkt till IT-säkerhetsansvarig för de olika organisationerna för att minska detta. Vid de tillfällen då vi gått genom chefer för att få kontaktinformation har vi fått ta del av mejlkonversationen mellan chef och respondent. Vi har

också efter bästa förmåga sett till att respondenten förstått den undersökning som skall göras samt att den kommer att bli publicerad.

Vi kommer också återge intervjuresultatet i rätt sammanhang och i rätt kontext. Detta är inte bara viktigt för att respondenten inte skall bli felciterad utan också för att data inte ska bli korrupt, d.v.s. vi måste återge rätt för att inte oaktat förfalska data eller resultat. All information som samlats in under intervjuerna finns bifogat i form av transkript, se kapitel 7.

4 Empiriskt resultat

I detta kapitel delger vi de svar som vi fått under våra intervjuer. Frågorna är uppdelade i de områden som vi redogjorde för i kapitel 3 men uppdelningen är även baserad på hur respondenterna har svarat. Basfrågorna behandlar följaktligen områdena aspekter, utformning samt utbildning och ansvar. Med första området aspekter har vi försökt att ställa frågor angående utsträckning på säkerhetspolicys rörande mobila enheter och om policys skiljer sig mellan enheter inom organisationen för att få reda på vad organisationer lägger vikt på i sina säkerhetspolicys. Utformningsfrågorna behandlar hur organisationer utformat sin säkerhetspolicy. Med sista området ville vi få reda på i vilken utsträckning organisationerna utbildar sin personal och hur säkerhetspolicys hålls uppdaterade.

4.1 Aspekter

Generellt sett har organisationerna relativt lika syn på de frågor som ställts rörande detta område, de största skillnaderna märks mellan de stora och små företagen. Samtliga organisationer har för tillfället ingen större skillnad på sina policys rörande privata och organisationsägda mobila enheter. R3 håller på att implementera nya policys rörande mobila enheter för att följa med i den ständigt utvecklande marknaden. R1 använder två olika nätverk för privatägda samt organisationsägda mobila enheter som enda skillnad rörande säkerhetspolicys mellan enheterna.

Samtliga organisationers anställda använder sig av PME i en viss utsträckning, dock skiljer det sig åt då R3s och R5s styrdokument är reglerat i lag vilket gör användandet av PME för vissa roller restriktiv. För R4 är det heller inte tillåtet att använda sig av PME på organisationens nätverk, men användning utöver det är förekommande. R5 tillåter endast enheter som har blivit godkända att användas inom organisationen. De använder sig även av 'Zitrix' vilket ger tillåtelse att komma åt vissa delar av organisationen från vilken dator som helst under förutsättning att vissa restriktioner följs. De använder sig också av ‘direct access’ som ligger i Microsoftmiljö som gör det möjligt att jobba hemifrån om man använder sig av en av organisationen godkänd enhet. Både R1 och R2 hävdar att det används PME för jobbrelaterad aktivitet men mestadels används organisationsägda enheter.

Registrering av PME sker endast hos R1 då de använder sig av Office365 som innehåller olika funktioner som gör detta möjligt. R2, R3, R4 och R5 kan se aktivitet när en enhet kopplas upp mot deras databaser eller mejl men det finns ingen direkt registrering av PME. R3 svarade dock

restriktivt på våra frågor rörande detta med anledning av teknisk karaktär. Office365 tillsammans med 'Exhange Active sync' och 'Propertymanager' är de enda tekniska lösningar som används av de organisationer som vi intervjuat och dessa lösningar används endast av R1 respektive R4. Resterande organisationer ser snarare sin säkerhetspolicy på en strategisk nivå där de anser att det räcker med att kunna stänga av de applikationer som anställda använder sig av, som mejlkonton och rättigheter i nätverket. De förlitar sig på att anställda använder sitt sunda förnuft då de handskas med känslig information på sina PME.

Att ha full kontroll på vilken information som lämnar företaget är den viktigaste aspekten för samtliga organisationer, för R1 innebär detta att organisationen kan se till att PME som lämnar företaget kan tömmas på innehåll på distans med hjälp av en tjänst i Office365 som tar bort den information som finns lagrad i den molntjänst som Office365 tillhandahåller. För R2, R3, R4 och R5 innebär samma aspekt att organisationerna försöker skapa en medvetenhet hos den anställde som gör att den hanterar så lite känslig data som möjligt på sin privata enhet och R4 nämner att det helt enkelt är den anställdas skyldighet enligt lag att vara medveten om detta.

4.2 Utformning

Enligt R1 har det inte skett någon genomgående utvärdering kring vilka säkerhetspolicys som behövs, utan organisationen har endast valt att använda sig av en befintlig teknisk lösning som de redan använder och arbetar inom, nämligen Office365. Office365 erbjuder en 'MDM' vilken R1 framhåller är den primära anledning till att organisationen har en säkerhetspolicy, denna lösning används till både organisationsägda och privata enheter. Vidare framhäver R1 att organisationen är medveten om att det finns tämligen mer avancerade och omfattande lösningar men att det kräver en egen infrastruktur vilket ansågs vara lite mycket med tanke på att de inte är så många anställda. Även R2 tar upp Office365 och berättar att organisationen för närvarande håller på att gå över till den lösningen, där anställda kan lagra information, mycket med anledning av att organisationen redan arbetar mycket med annat i Office365. R2 nämner liksom R1 att det inte är ekonomiskt hållbart med en egen infrastruktur för säkerhet då det är en relativt liten organisation, och därför passar Office365 lösning bra.

R2 har varit med och utformat organisationens säkerhetspolicy tillsammans med en grupp där HR-ansvarig är ytterst ansvarig för säkerhetspolicys. Under intervjuns gång upprepar R2 ofta att

organisationen förlitar sig mycket på sina anställdas sunda förnuft, och gjorde även det innan en officiell säkerhetspolicy utformades. R2 berättar att anledningen till att de utformade en officiell säkerhetspolicy var för att organisationens kunder krävde det, alltså främst för att skydda det material och den information som berör kunden. Vi uppfattar det som att organisationen inte använt sig av något ramverk eller mall utan har med hjälp av en mindre intern riskbedömning uppfyllt de krav som kunderna ställt.

R3, R4 och R5 är betydligt större organisationer och har andra krav på sig då de är offentliga organisationer, bland annat i form av krav på diarieföring. Vid utformningen av R3s, R4s och R5s säkerhetspolicys har organisationerna fått ta stor hänsyn till olika lagrum, personuppgiftslagen, sekretesslagen och förvaltningslagen är några av de som nämns. Med utgångspunkt i lagarna har organisationen enligt R3 skapat ett underlagsmaterial vilket sedan har diskuterats med en rad olika avdelningar, bland annat HR och juridiska avdelningen. Enligt R3 har organisationen utöver lagrummen byggt upp policydokumenten efter ISO 27000-serien, där organisationen valt ut de specifika aspekterna som behövdes och passade dem.

Precis som R3 till viss del har baserat sina policys på lagrum har även R5 gjort det, dock använder organisationen sig utöver det också av en policystandard, BITS (Bits.org, 2014), vilken dock ska revideras inom en snar framtid. R4 förlitar sig på den säkerhetspolicy som organisationen har generellt för mobila enheter inom organisationen, vilken är baserad på olika lagrum, samt sekretesslagen för att behandla känslig information som bearbetas på mobila enheter.

Rörande revidering och uppdatering av policydokument försöker R2 och R3 uppdatera säkerhetspolicyn årligen medan R1 inte kunde svara på frågan. R1 är tillförordnad säkerhetsansvarig då personen som vanligtvis sitter på tjänsten är tjänstledig och framhäver att hen inte har full koll på vad som står i deras säkerhetspolicy. R4 i sin tur säger att de inte uppdaterar säkerhetsspolicyn då den är så baserad på lagrum. R5 ställer sig lite osäker till hur ofta organisationens policys ska revideras men hen säger att det sker varje gång organisationen inför nya ändringar i systemet, men inte oftade då det enligt hen är väldigt tidskrävande att förankra en ny policy.

Vår uppfattning är att varken R1, R3 eller R5 har utvecklat sina säkerhetspolicys för att skydda sig mot eventuella problem som kan uppstå vid användning av PME, utan har snarare utformat sina säkerhetspolicys för att skydda informationen från det andra hållet så det inte spelar någon roll vilken typ av enhet som når informationen.

4.3 Utbildning och ansvar

Både R1 och R2 har viss utbildning rörande säkerhetspolicys. Det rör sig om en genomgång av tekniska detaljer och mer generell information vid nyanställning exempelvis. Både R1 och R2 säger att det är upp till den anställde själv att lära sig om policys efter den initiala presentationen. Detta skiljer sig inom större organisationer då R3 och R5 har ett annat tillvägagångssätt vad gäller utbildning. R3 berättar att de har informationskampanjer för att nå ut till alla i ledningen och förklara för dem hur de ska förhålla sig till säkerhetspolicyn och hur de ska hantera det med sin personal, det står också definierat i R3s policydokument att utbildning ska ske och i vilka former. Detta tillvägagångsätt använder även R4 då de har ett introduktionsprogram där anställda får ta del av utbildningen. De får även ta del av dem säkerhetspolicys som råder samt de lagrum som gäller vid användning av mobila enheter. R5 har också introduktionsprogram som nyanställda kan ta del av samt utbildning som sker via deras intranät. Vidare har olika delar av organisationen också tillgång till specialutbildningar.

Utöver det har alla anställda enligt R3 möjlighet till interaktiv utbildning om säkerhetspolicyn via en webbplattform. Detta är inget som i dagsläget är obligatoriskt men R3 säger att de håller på att se över det. För att skapa en medvetenhet kring säkerhet rörande IT-utrustning, poängterar R3 också vikten av att kommunicera vad som står skrivet i ett policydokument ut till de anställda som berörs. Detta är alltså något R3 ständigt arbetar med.

Rörande ansvarsområden berättar R3 att det är hen som är ansvarig för att revidera och se till att säkerhetspolicys följs. R1 däremot kan inte exakt svara på vem, men säger att det finns specificerat vem som är ansvarig för säkerhetspolicys, dock vet R1 ej om det finns dokumenterat i policyn. R3 och R5 berättar att det förekommer olika roller, och det finns även specificerat i säkerhetspolicyn, medan R1, R2 och R4 inte nämner några specifika roller.

När någon slutar inom organisationen hanteras det på liknande sätt av alla organisationerna, R1 ser till att låsa kontot för den anställde, Office365-kontot i det här fallet, och R2 och R5 avslutar mejlkonto så anställda inte längre kan komma åt organisationens information. Däremot har varken R2 , R3, R4 eller R5 någon säkerhetspolicy som hanterar lagring på externa tjänster såsom exempelvis dropbox. Anledningen enligt R3 och R4 är att de är offentliga organisationer. R5 poängterar dock att lagring på exempelvis Dropbox inte bör göras men saknar en policy som uttalar det. Rörande specifikt PME beskriver R3 att det är väldigt svårt då en anställd slutar att kunna kontrollera dessa, men att organisationen har försökt skapa vissa begränsningar rent tekniskt för att preventivt hindra att felaktig information försvinner från första början.

5 Diskussion

I denna del av uppsatsen jämför vi de empiriska resultat vi fått genom intervjuer med den litteraturbaserade teorin tidigare i uppsatsen. Vi kommer att gå igenom de skillnader och likheter som kan finnas mellan de båda delarna. Upplägget av detta kapitel kommer vara detsamma som föregående för att skapa en lättare förståelse för våra fynd.

5.1 Organisationsstorlek

Då vårt empiriska resultat visade på en viss skillnad mellan organisationerna med anledning av dess storlek är det nödvändigt att göra en mindre klassificering av organisationernas storlek för att senare kunna göra en karaktäriserad generalisering i vår slutsats. En karaktäriserad generalisering innebär att vi kan härleda resultatet till att om en tredje (i fall avseende en mindre organisation) eller en fjärde (i fall avseende en större organisation) organisation skulle delta i undersökningen skulle resultatet med stor sannolikhet likna de föregående organisationernas policys.

Vår klassificering härrör främst ifrån EU-lagstiftningen för företag (Europa.eu, 2014) men även ifrån insamlad fakta från våra intervjuer.

Vi har valt att klassificera organisationerna som deltog i vår undersökning som stora om organisationerna har:

- Fler än 250 anställda
- Omsättning som överstiger 430 miljoner kr/år
- En IT-avdelning med minst 10 anställda

Organisationer som placerar sig under dessa siffror klassificerar vi som små. De organisationer som betecknas som stora från vår undersökning blir följaktligen R3, R4 och R5. Respondenter R1 och R2 betecknas i vår uppsats som små organisationer.

5.2 Aspekter

Att samtliga organisationer i vår empiriska undersökning saknar en mer specifik säkerhetspolicy för sina PMEs visar på att de undersökningar som gjorts tidigare av ISC (Suby, 2013) och SANS Mobility Survey (DeLaGrange, 2012) sammanfaller med det resultat som vi fått från våra interjvuer. Vidare visar detta på att organisationer fortfarande är i ett tidigt stadie när det gäller kompletta säkerhetspolicys specifikt utvecklade för PMEs. I tabell 5.1 återfinns respondenternas svar rörande de aspekter vi härledde ifrån vår litteraturundersökning i kapitel 2.6.

Tabell 5.1 Jämförelse av aspekter mellan respondenterna(aspekter från kapitel 2.6)

Aspekter	R1	R2	R3	R4	R5
Beskrivning av lämplig träning och utbildning för användning	Ja	Ja	Ja	Ja	Ja
Definiera säkerhetslager med klassificering	Nej	Nej	Ja	Ja	Ja
Använda sandboxing och device integrity application och 'MDM'	Ja	Nej	Nej	Ja	Ja
Speciella säkerhetszoner för privata mobila enheter	Ja	Nej	Nej	Nej	Nej
Specificera tillåtna uppkopplingssätt för privata enheter mot organisationsenheter	Ja	Nej	Ja	Nej	-
Registrering av privata mobila enheter	Ja	Nej	-	Nej	Ja

De organisationer som vi har intverjuat har policys för hur kommunikation ska ske och hur man håller denna säker genom olika tekniska lösningar för mejl men saknar policys för hur de löser problem som kan tillkomma med bortappade eller stulna mobiler. De enda respondenterna som hade en lösning på detta problem var R1 och R4 som kunde tömma enheterna på innehåll från distans vilket dessutom förutsätter att enheten är uppkopplad mot ett nätverk.

Detta faktum stämmer överens med Fortinets undersökning (BYOD Brings Wave of Unknown Security Threats, 2012) där förlust av organisationsdata sågs som ett av de största hoten. Organisationerna vi intervjuat förlitar sig istället på att deras anställda är medvetna om de risker som medföljer av att ha känslig information på sina smarta telefoner, här utmärker sig R2 och R4 främst. Office365 skapar lösningar till viss del, men det kan hända att användaren bryter

säkerhetspolicys och sparar information på annat ställe på mobilen, vilket Fortinets undersökning (Micrographics & optical Technology, 2011) visar, än i just Office365s inbyggda molntjänst och då är en tömning av innehåll med hjälp av Office365 inte möjligt.

Att organisationerna inte har eller håller på att utveckla policys specifika för PME stämmer överens med den undersökning som ITIC gjort (Eddy, 2014) gjort där 43 % av organisationerna svarade att de fortfarande inte har en detaljerad policy för PME. Dock revideras för tillfället R3s nuvarande säkerhetspolicys för att de ska innehålla mer specifika åtgärder för PME, samma gäller för R2 som i framtiden ska implementera Office365 till sina nuvarande säkerhetspolicys. Detta skapar ökad säkerhet för organisationerna då de introducerar nya säkerhetspolicys och är ett steg i rätt riktning för att försöka hänga med i teknologins takt. Detta ligger helt i linje med Vishal et al. (2013) som anser att en implementation av ett ‘MDM’ är första steget för att säkra användning av PME.

Utifrån de ramverk och standarder som vi undersökt i litteraturgenomgången kunde vi härleda sex säkerhetspolicys som var ofta förekommande rörande PME. En av dem är registrering av PME, vilket är en viktig del av säkerheten. För att kunna hålla information säker bör organisationen ha ett överskådligt sätt att se vilka enheter som faktiskt finns och används på organisationens nätverk och i databaser. De enheter som kan komma åt känslig organisationsinformation bör därför registreras och övervakas för att kunna utreda potentiella hot mot organisationen. Av bland annat denna anledning har R1 och R2 svarat att de har eller håller på att utforma ett sätt för att kunna registrera och övervaka den information som PME tar del av i form av ett ‘MDM’. R4 har för tillfället en till viss del fungerande 'MDM' i form av Apples egna 'Propertymanager'.

Samtliga organisationer har utan att använda någon form av ramverk för utformandet av sina säkerhetspolicys ändå fått med några av de viktiga aspekter som vi identifierade efter vår litteraturundersökning:

- **Åtkomstkontroll** - I form av lösenord på mobila enheter samt på de program som används.
- **Nätverkssäkerhet** - Genom att ha två olika nätverk har R1 sett till att bara organisationsägda enheter kommer åt deras huvudnätverk.
- **Granskning och översyn** - Office365 bidrar med översyn för R1 och snart även för R2 då organisationerna håller på att implementera denna lösning, samt 'Propertymanager' och

'Exchange Active sync' för R4's del.

- **Roller och ansvar –** Finns tydliggjorda för samtliga organisationer i viss mån.
- **Förklaring av policys** - Samtliga respondenter har utbildning för sina anställda.
- **Backup** - Sker mot Office365 eller andra cloudbaserade lösningar samt Exchange Active sync.
- **Potentiella hot** - De största hoten för samtliga företag är att information skall komma i fel händer och samtliga organisationer är medvetna om de hot som finns kring PME.

5.3 Utformning

Rörande utformningen av säkerhetspolicys har vi fått ett annat resultat i vår empiriska undersökning jämfört med vad vi fick i litteraturundersökningen. Det står klart för oss att de ramverk och standarder som vi fann i litteraturen kan användas, men främst vid storskalig användning.

R1 och R2 är så pass små organisationer att en utformning av en säkerhetspolicy enligt CoBIT eller ITIL är för omfattande för att vara rimlig. Däremot har R3, vilken är en väsentligt större organisation bland annat använt sig av ISO 27000-serien (Iso.org, 2014), och har även utformat sitt policydokument på liknande sätt som NIST förespråkar (LeVeque, 2006) med grenar av olika policys. Även R5 har använt sig av en policystandard, i detta fall BITS (Bits.org, 2014).

Även om R1, R2 och R4 inte uppger att de använt sig av något specifikt ramverk eller tillvägagångssätt återfinns det i deras säkerhetspolicys vissa av de aspekter vi sammanfattade i kapitel 2.2.2. R3 och R5 använder nästan samtliga av dessa aspekter i sin säkerhetspolicy. Detta tyder på att även om organisationer inte utformar sina säkerhetspolicys i enlighet med ett specifikt ramverk eller enligt en på förhand bestämd standard är dessa säkerhetsaspekter ändå återkommande i många säkerhetspolicys.

Vidare kan också konstateras att Souppaya och Scarfones (2013) förslag till tekniska lösningar för att preventivt skydda sig mot konsekvenser av användning av PME inte är något som beaktats vid utformningen. Ingen av respondenterna använde sig exempelvis av 'sandboxing', och varken R1 eller R2 använde sig av klassificeringar rörande behörighet eller rekommendationer rörande teknik för att säkerställa PME, bortsett från användningen av Office365 för R1's del.

Under vår empiriska undersökning har det också blivit klart att samtliga organisationer främst använder PME för kommunikation och tillgång till data, de lägre nivåerna av mobilt användande enligt Šedivás (2013) undersökning, och därmed är det mindre komplext att utforma säkerhetspolicys. Detta kan vara en bidragande orsak till att R1 och R2 inte använt sig av något speciellt ramverk som stöd.

Baserat på vår empiriska undersökning kan vi konstatera att vissa aspekter är återkommande, exempelvis Reyes (2005) exempel på vad som bör ingå i en säkerhetspolicy stämmer överens med

de säkerhetspolicys vi fått ta del av. Våra intervjuer har visat att organisationer inte nödvändigtvis måste använda sig av erkända standarder eller ramverk vid utformningen, utan kan i mindre eller större grad använda ett smörgåsbord av vad som finns att tillgå inom området. För mindre organisationer är det helt enkelt enklare att göra en egen riskbedömning och formulera säkerhetspolicys utefter det.

De ramverk och standarder vi funnit vid litteraturgenomgången kan användas som stöd vid utformningen av en säkerhetspolicy, men fyller störst funktion avseende mer komplext utformade organisationer, vilket R3 och R5 vittnar om.

5.4 Utbildning och ansvar

Enligt vår litteraturundersökning identifieras vårdslösa anställda som det största hotet rörande användning av PME och utbildning kring hur sådana ska hanteras bör därför ingå i en säkerhetspolicy. Detta påstående bekräftas av vår empiriska undersökning där samtliga respondenter beskriver att de har utbildning kring säkerhetspolicys.

Bin Muhaya et al. (2012) föreslår ett träningsprogram för att skapa en medvetenhet kring säkerhetsaspekterna av privat mobilt användande, vilket är något som inte i lika stor utsträckning återfinns bland våra respondenter. Det är endast R3 som erbjuder ett kontinuerligt utbildningsprogram, medan R2 och R1 endast har en heldagsutbildning initialt vid nyanställning eller vid revidering av säkerhetspolicys. Även R4 och R5 har ett introduktionsprogram för anställda som innehåller de policys och lagrum som ska följas vid användning av mobila enheter inom organisationen.

Ett utbildningsprogram där anställda själva får lära sig kring säkerhetsaspekter är enligt Bulgurcu et al. (2010) ett bra preventivt sätt att motverka hot som kan uppstå. I R1 och R2s fall kan det skapa komplikationer i senare stadie när man under okontrollerade former låter anställda lära sig om säkerhetspolicys. Även R4 hanterar utbildning på ett relativt okontrollerat sätt där R4 poängterar att det är upp till den anställde själv att lära sig om säkerhetspolicys och lagrum efter den initiala introduktionen. Detta kan lätt åsidosättas till förmån för andra arbetssysslor och syftet med utbildningen kan helt försvinna och öppna upp för exempelvis vårdslöshet, som Siponen et al. (2009) nämner. R3s förfaringssätt att använda sig av interaktiva utbildningar på webben är en mer

kontrollerad form av utbildning där incitamentet till att lära sig om säkerhetspolicys torde vara större även om R3 nämner att det ännu ej är obligatoriskt.

Vad gäller ansvar verkar det som att samtliga respondenter förespråkar sunt förnuft över definierat ansvar i sina säkerhetspolicys, något som även nämns av Guérin (2008). De enda respondenterna som har definierade roller i sin säkerhetspolicy på det sätt som Carillo (2013) och Sheikhpour och Modiri (2012) beskriver är R3 och R5. Alla respondenter har definierat en roll för den ansvarige av säkerhetspolicys, men inga övriga roller mer än så. I R3s fall handlar det om behörighetsroller för olika säkerhetsnivåer, men inget som berör övriga ansvarsområden. Det kan vara så att i R1 och R2s fall behövs inga rollbeskrivningar då de är lite mindre organisationer, och det kan helt enkelt vara så att det inte är någon annan än IT-ansvarig som behöver en rollbeskrivning.

Alla respondenter ser också till att avsluta anställdas konto så fort de avslutar sin tjänst. Då det främst rör sig om mejlhantering hos alla respondenter fick vi uppfattningen att det inte är en särskilt komplicerad process, och ingen av respondenterna berörde heller de privata mobilerna, eller hade som krav att de skulle återställas. Detta minskar klart komplikationer som kan uppstå ur laglig synvinkel.

6 Slutsats

Genom vår undersökning i uppsatsen har vi kommit fram till en rad slutsatser rörande vår forskningsfråga. Forskningsfrågan löd;

- *Använder organisationer sig av säkerhetspolicys för privata mobila enheter för att skydda information?*
    - *Om organisationer gör det: skiljer sig dessa policys ifrån de policys organisationen har för mobila organisationsenheter?*

Vårt undersökningsresultat har visat att få av våra tillfrågade organisationer har specifika säkerhetspolicys för PME. Vi har identifierat en rad aspekter i säkerhetspolicyn som hjälper organisationerna att skydda sig mot eventuella hot vid en användning av PME men dessa aspekter är i de flesta fall inte specifika för PME utan används för att hantera samtliga mobila enheter inom organisationerna vi undersökt. Vi har därför inte kunnat härleda några nyckelaspekter som specifikt rör PME från vår undersökning.

En anledning till att större organisationer i vår undersökning, alltså R3, R4 och R5, inte i större utsträckning utformat specifika policys för PME kan vara för att det är svårt att på ett vettigt sätt hålla god uppsikt över de enheter som används inom organisationen. Mindre organisationer som R1 och R2 har lättare att implementera en lösning för detta, som de i detta fall gjort med hjälp av Office365. De mindre organisationerna i vår undersökning, R1 och R2 behöver bara hantera ett fåtal mobila enheter till skillnad mot större organisationer som måste hitta en lösning för flera tusen anställda. Detta bidrar till att organisationerna istället försöker hitta en lösning som inte är specifik för PME utan för deras sätt att hantera data. Istället för att försöka identifiera säkerhetsproblem med PME försöker organisationerna i vår undersökning skydda värdefull information genom att begränsa åtkomst till den från alla mobila enheter. Det ska alltså inte spela någon roll om en anställd använder sig av en privat enhet eller en organisationsägd.

För tillfället finns en teknisk lösning för att kontrollera eller hindra data från att spridas inte implementerad hos någon av våra respondenter utan de har en mer informell policy när det gäller säkerhetspolicys. Den informella policyn som existerar hos de mindre organisationerna i vår undersökning uppfattar vi som en av huvudanledningarna till att dessa inte implementerat specifika

säkerhetspolicys för PME.

Organisationerna i vår undersökning förlitar sig i hög grad på att anställda inte kommer att delge någon känslig organisationsinformation, även om detta kan fungera för mindre organisationer som R1 och R2, där det är lättare att ha en kontroll över mobila enheter, visar ändå en undersökning av Forrsight (Khanna, 2013) att 62 % av all informationsförlust beror på att människor är vårdslösa. Att organisationer ska ha ett förtroende för att anställda håller känslig information säker är en självklarhet, men information kan delges utan att användaren är medveten om det. Det är därför viktigt att se till att anställda inom organisationen har en en medvetenhet om de faror som kommer med 'BYOD'.

En av aspekterna som vi identifierat som viktig i vår litteraturundersökning, utbildning, visade sig också användas av samtliga organisationer vi undersökt. Organisationerna använde sig av olika typer av utbildning men alla ansåg ändå att utbildning är viktigt att ha med i en säkerhetspolicy för PME för att preventivt skydda sig mot missöden. Detta var återigen ingen aspekt som var specifik för PME.

Vidare hade vi även en forskningsfråga rörande hur organisationerna har valt att utforma sina säkerhetspolicys;

- *Hur utformar organisationer sina säkerhetspolicys?*

Vårt undersökningsresultat visade på att utformningen av säkerhetspolicys för de undersökta organisationerna sker med hjälp av interna riskbedömningar på ett närmast godtyckligt vis. Undersökningen visade också att de större organisationernas säkerhetspolicys till viss del var reglerade av olika lagrum. Vi trodde efter litteraturundersökningen att vårt resultat skulle visa på att organisationerna använde sig av definierade ramverk och standarder, som ett hjälpmedel att utforma säkerhetspolicys. Undersökningen visade dock att sådana hjälpmedel främst är till för väldigt stora och komplexa organisationer, det var bara två av organisationerna i vår undersökning som använt något av de ramverk vi fann i vår litteraturundersökning och i dessa fall endast små delar av dem. En anledning kan vara avsaknaden av resurser i de mindre organisationer vi undersökt. De mindre organisationerna hade ingen stor IT-säkerhetsavdelning utan endast en eller två anställda som fungerade som IT-säkerhetsansvariga.

Däremot användes många av de aspekter som finns att finna i ramverken och standarderna vi undersökt. Detta visar på att de undersökta organisationerna trots allt är medvetna om var de största hoten finns och vilka aspekter som behövs tas upp i en säkerhetspolicy för PME, utan att behöva använda sig av alltför definierade och strukturerade hjälpmedel.

Vår undersökning visade att det i dessa fall fanns en viss skillnad rörande säkerhetspolicys för PME beroende på organisationers storlek. Resultatet tolkar vi som att det är mer troligt att större organisationer, jämfört med mindre, använder sig av delar av olika ramverk och standarder vid utformningen av sina säkerhetspolicys. Samtidigt särskiljer de inte säkerhetspolicys rörande PME och organisationsägda mobila enheter, förmodligen då det är svårare att kontrollera. Vad gäller aspekten utbildning har vår undersökning också visat att de större organisationerna mer troligt har en mer kontrollerad form av utbildning i sina säkerhetspolicys än de mindre organisationerna.

Vi kan med sannolikhet generalisera vårt undersökningsresultat vad gäller stora och små organisationer och vid en mer omfattande undersökning med ytterligare respondenter borde inte resultatet skilja sig nämnvärt. För att med säkerhet kunna bevisa att vårt resultat är generaliserbart hade dock fler respondenter krävts.

Alla organisationer i vår undersökning tillåter sina anställda att i större eller mindre form använda sig av PME, och verkar anse att det är behövligt för de anställda att ha denna möjligheten. Avslutningsvis uppfattar vi det som att de flesta organisationerna i vår undersökning har ett synsätt på användning av PME som vi summerar i: “Frihet under ansvar”.

6.1 Förslag till vidare forskning

I vår undersökning var utbildning en av de viktigaste aspekterna att ha med rörande en säkerhetspolicy för PME. En beskrivning av hur denna bör ske och vad den ska innehålla är av stor vikt i en organisation. I framtiden hade det varit intressant att göra en undersökning rörande olika typer av utbildningsformer.

I vår undersökning använde sig en del av organisationerna av ett mer fritt angreppsätt där det var mycket upp till de anställda att lära sig om policys och ta reda på själva vad det innebär och vilket ansvar som tillkommer. Den lite större organisationen i vår undersökning använde sig däremot av en interaktiv webbutbildning, som eventuellt i framtiden kunde bli obligatorisk.

Dessa två angreppsätt på utbildning är de sätt som våra respondenter använt sig av vid utbildningsfasen, och det finns säkerligen andra synsätt på hur man bäst utbildar sin personal. Detta ämnet hade varit intressant att undersöka i framtiden och ta reda på om typen av utbildning påverkar medvetenheten kring säkerhetsfrågor rörande ‘BYOD’ och potentiellt kan innebära ett bättre skydd och därmed ett minskat hot för organisationen.

7 Bilagor

Respondent 1

R1: Respondent 2, **M**: Marcus, **O**: Oscar

M: Börja med att du kanske kan prata lite allmänt om organisationen
R1: Ja, ni har kommit till ett företag som heter [Namn] som levererar främst intranätlösningar till medelstora och större bolag.
och jag heter [Namn] och jag är ansvarig för den verksamheten här.
O: Hur många anställda är det som arbetar här?
R1: Vi är trettio anställda idag
O: Och då har ni några specifika säkerhetspolicys för privata mobila enheter här på [Namn]?
R1:Ja, vi har egentligen samma säkerhetspolicy oberoende, hyffsat, man kan, antingen så har man en mobil som bolaget äger eller så har man en egen device. Det är inte så vanligt med telefoner för de äges oftast av bolaget, men det kan vara ipads eller windows 8 plattor eller den typen av devices, och policyn går egentligen ut på att såfort du kopplar, kopplar en mobil, en sånhära enhet till vårt mainsystem, så tvingar vi registrering av den i vårt system för att hantera det, och också att man måste ha en lösenkod på maskinen och det gör då att vi kan strukturera det där med att om någon tappar en telefon tex så kan vi wipea den centralt för att säkerställa då att vi inte blir av med ganska mycket data som innebär då när man syncar mail och kalender
O: Detta förutsätter då att den är uppkopplad mot nätverket när den
R1: Ja, precis då, och att den fortsätter att vara det så att säga
M: Den här lösenordstjänsten är det någon extra tjänst ni har eller
R1: Nej den ingår i, vi använder något som heter Office365 som är en vad kan man säga, en cloudlösning för e-post och lite andra tjänser men det är främst det vi använder och i den så finns den funktionen så vi kan gå in, tex, vi kan gå in på mig själv och titta på vad jag har för enheter. Säg att jag har en ipad och jag har en iphone och så har jag min vanliga dator, så ser jag de vanliga devicerna där då, så om det är någon som kommer till oss då och säger att jag har tappat min mobil eller vad det är så kan vi gå in där och se där om man får en heartbeat mot den och så kan vi tömma den.
O: När någon då, med sin privata, om någon går in med sin privata enhet då och vill registrera sin

mail. Då är detta något man kan göra bara sådär eller är det något ni måste godkänna?
R1: Nej, det görs eftersom vi har den policyn så gör vi det, då kan vi säkerställa att vem som helst inte kan komma åt den utan man behöver en viss pinkod, och så löser vi det på detta sättet
O: Har ni någon nedskriven policy för vem som håller roller och ansvar och vem som skall se till att detta sköts?
R1: Ja, vi har, jag är dålig på det, egentligen inte mig ni ska fråga om det, saken är den att han som egentligen är ansvarig är på tjänstledighet och den nya [otydligt] har inte riktigt kommit up to speed än och det var lite därför jag tog det så jag har lite dålig koll på om det står nedskrivet men det finns en specifik roll som ansvarar för all dessa grejer som rapporterar uppåt
M: Har ni någon form av utbildning för de som jobbar här så att de vet hur de ska hantera de olika program, som 360 osv?
R1: Ja de, absolut det tas oftast när de är nyanställda, så tar vi och förklara hur det fungerar med detta och de får använda vilken enhet du vill men du är själv ansvarig för att informationen hålls säker så att säga.Sen vad gäller datorer och sådana grejer så försöker vi se till att all data finns på servrar som ägs av oss så att säga, vi har ingen restriktion på dropbox och sådana grejor men genom policys så ser vi till att de inte använder det helt enkelt, så det är inte bara mail och sådant utan vi tänker på en helhet där.
M: Det spelar inte heller någon roll vilket OS eller telefon de använder sig av, det kan vara en samsung eller iphone, ios eller andriod?
R1: Nej det enda vi är intresserade av är att vi kan ta bort det, wipea den och att vem som helst inte kan komma åt den om de tappar den, dvs om det finns ngn extra kod på den det är det som styr på så att säga.
O: Hur funkar det, ni sa att ni har lite utbildning, hur funkar det om någon potentiellt slutar? hur hanterar ni det då med deras privata enheter?
R1: Då ser vi till, vi låser dem grejerna och så ser vi till att de privata enheterna, vi ser till att de visar att de är wipeade, för vi vill inte att de ska ha tillgång till informationen heller så den är cloudbaserad.
O: Hur har ni bestämt att ni ska använda denna lösningen, alltså denna tekniska lösningen?
R1: Det är inte så att vi har utvärderat, det finns ju sådana sjukt avancerade lösningar för att hantera det, men eftersom denna fanns inbyggd och vi redan hade den lösningen och vi blev flera så var vi tvungna att implementera ngt och då var det denna som fanns närmast till hands, och sedan är det ju så att större lösningarna kräver ju oftast en liten egen infrastruktur och egna appar osv så att då blev

det lite [otydligt] i den här bemärkelsen.

M: Fick de också välja om de vill ha en mobil från eller det är bara privata, ger ni ut datorer osv?

R1: Jo vi ger ut allt, men vill man då ha något annat så, det finns ju folk som typ såhär. Nej nu har jag ändrat mig, nu vill jag köra det. Då är det helt fine det finns folk som har ipads privat som vill köra mail på det, javisst då är det inga konstigheter men alla får en dator och en mobiltelefon, så att, men surfplattor osv är det bara vissa som har, mest är det privata

O:Har ni några olika policys för domhär organisationsägda enheterna, alltså är det striktare?

R1: Nej, det är precis ingen skillnad nej,som jag sa tidigare, vi har liksom definierat upp dom här grejerna vi vill liksom bara säkerställa att grejerna inte bara försvinner att vi kan ta bort det

O: Vilket OS är vanligast bland anställda?

R1: Skulle gissa att det är ios7

O: Okej

M: Är det något allmänt du skulle vilja kasta ut eller gällande era policys?

R1: Nej egentligen inte, det är väl ja...

M: Har ni kollat på ISO standarder eller färdiga ramverk som NISTS eller sådana?

R1: Nej vi har inte kollat på något, vi ville bara kolla upp vad vi behövde, vi behövde säkra på något jävla sätt och då tog vi det som var enklast för oss

O: Ni gjorde en intern riskbedömning kan man säga?

R1: Ja, precis, vi kan liksom inte börja dra ihop massa, det är klart vi hade kunnat, vi hade kunnat applicera någon sådan guide men det känns onödigt

O: Har ni haft några komplikationer, med det någon gång? Att någon har försvunnit? Någon enhet och sådär

R1: Nej, men vi har testat det, ett scenario där så att, men det var nog längesedan vi gjorde det sist, men vi försöker, jag vet att vi var, nu har han iofs varit borta 2 månader men förra året testade vi nog två gånger med olika lösningar, bara för att försöka se om det verkligen fungerar, sålänge den är uppkopplad. Den policyn är egentligen ganska safe, eftersom om man inte är uppkopplad så kan man inte använda telefonen överhuvudtaget och då har de ju förmodligen wipeat den om det är någon som har stulit den och då har de ju wipeat den själv, för de vill ju oftast kanske inte ha kvar alla de grejorna som ligger där och påsätt är det ju lite självsanerande just det med mobiler, det är ingen som, antingen så resetar de den eller så gör vi det innan

M: Fixar sig själv liksom

R1: Ja exakt

O: Är det någon form av sandboxing historia detta Office365? Den lösningen ni använder är den byggd på sandboxing om du vet vad det är?

R1: Nej

O: Att man separerar ja då på privata enheter, så separerar man då det här mailprogrammet från resten av telefonen så att de inte kan kopplas överhuvudtaget

R1: Nej vi har ju inte det,större företaget använder ju det, dvs du kan inte ens koppla upp den mot mailen, ne, men isåfall måste du ju ha en app men det är lite nästa steg i allt detta och det är många av de stora företagen som har detta för de kan ju inte hålla reda på alla enheter. Det är helt omöjligt. Alltså säg att du har tusen anställda då måste du ha en anställd som jobbar endast med detta, med privata enheter så det blir liksom, ja, så vi har inte någon sådan lösning utan vi tillåter det helt enkelt, det handlar bara om att folk ska kunna arbeta på ett enkelt sätt.

M: Hur fungerar den registreringen du talat om tidigare? Är det första gången du kopplar upp så går det in på ditt konto, registreras?

R1: Så registrerar den ja, så kan man gå in på min och har jag haft tio mobiler så kan man förmodligen se tio telefoner där.

M: Kan man komma åt grejerna på telefonen eller det visas bara vilken telefon det är

R1: Ja precis, och när den senast hade anslutits

O: När ni utformade när ni bestämde det här vem var det som var med i processen då och bestlutade det, var det IT-killen och du?

R1: Ja vi två

O: Och det är inga konstigheter? Man kan koppla upp mot alla enheter här och så på arbetet även om man har privata? Det är inte specificerat på något sätt några säkerhetszoner som man inte får koppla upp sig mot? Ni har inget spec nätverk osv?

R1: Nej, det finns ett gästnätverk för vissa saker men, vad gäller de enheterna så ser vi inte det som en sådan risk att det är privata datorer och det är nästan ingen som har det nu så att det problemet finns inte.

O: Ne som vi nu bara

R1: Ja precis, men då är de på ett gästnät så att de kopplas inte, så har man dem med sig och vill surfa så kopplar man dem mot det nätet och då är man aldrig exponerad mot företags nätet det är helt separerat

M: Det var nog nästa, jag har inga fler specifika frågor

O: Nej, det har nog inte jag heller

M: Vi fick väldigt raka bra svar så det gick lite snabbare än vi trodde

O: Men om vi kommer på något i efterhand så kanske vi kan höra av oss?

R1: Ja absolut, perfect, snabbt och smidigt!

M: Ja, tack för att ni tog er tid

Respondent 2

R2: Respondent 2, **M**: Marcus, **O**: Oscar

M: Okej
O: Ja, då börjar vi då. Jag tänkte att du kan berätta vem du är och vad du har för befattning här på [Organisationsnamn].
R2: Ja, [Namn], jag är IT-ansvarig här. Det är mitt huvudområde. Sen är jag ungefär 25 % teknisk konsult, gör installationer av Sharepoint, SQL, allt möjligt sånt.
O: Okej. Och hur många anställda är ni som jobbar här?
R2: Vi är 73 stycken idag.
O: 73? Okej. Är det du som är högst ansvarig för säkerheten här? Eller är ni en avdelning som jobbar med det eller hur ser det ut?
R2: Eh, vi är.. Vi är väl egentligen, det är HR-chefen [Namn] som är högst ansvarig.
O: Okej.
R2: Men sen sitter jag inom en grupp som heter Tech-support som har en teknisk chef som är mer, ja vad ska man kalla det, utvecklingschef. Men HR-chefen är han som är policy-ansvarig.
M: Okej, så det är de som utformar, och sen så kollar ni lite på dem?
R2: Ja, nu har det varit, det är jag som skriver och sen så kollar de igenom och tycker och tänker om det.
M: Okej. Vad var dina tankar när du satte dig ner och började göra dem? Hade ni något från början eller?
R2: Eh.. Från början var det nog att vi inte hade någon särskild säkerhetspolicy utan.. eh, ja, det var mer samvetet som spelade in vad man gjorde och inte gjorde med sin dator, och sen fick vi in nya större kunder som hade ganska känslig information så dem krävde att vi satte upp ordentliga riktlinjer.
M: Så, anpassar ni litegrann emot vilket företag ni jobbar med också? Alltså, har ni specifika policys när ni jobbar med ett företag eller ett annat?
R2: Eh.. Nej, nu, vi kör så säkert som vi kan.
M: Ja, okej.
O: Uhm, ja. Har ni några specifika policys för just privata mobila enheter eller ser de likadana ut som de här organisations.. Alltså ni leasade ju här?
R2: Ja.

O: Ja precis.

R2: Eh, nä det är ju samma policys för alla enheter. Och sen.. i och med, det blir ju ett större ansvar att ha känslig information på en privat enhet så.. Vi brukar trycka på att, tänk på vad du har på din enhet. Den ligger hemma, om barnen använder den och så.

O: Okej. Ja. Är det många som använder privata mobila enheter? Det är tillåtet som jag förstår, men är det många som faktiskt gör det också eller?

R2: Jag tror inte det är så många som använder det i sitt dagliga arbete, utan det är mer att vi har online-kurser som man kan titta, och det använder dem helst när de sitter på bussen och så. Och så är det väl ta emot mail.

O: Kalender också kanske?

R2: Kalender också ja.

O: Vanligaste uppgifterna helt enkelt.

R2: Ja.

M: Ni har liksom inte nån form av sandboxing? Eller liknande så att ni inte kan komma åt era typ mail om ni inte har installerat ett visst program på dem?

R2: Nej det har vi inte än.

M: Så ni kör liksom lösenord och sånt då, mer?

R2: Ja, ja det brukar vi nog också rekommendera att man inte skickar det via mail, i alla fall inte samma mail.

M: Mmm, ja nej.

R2: Men det är.. Det har vi nog inte egentligen riktig koll på hur, hur mycket som..

O: Okej. Och alla får lov att använda privata enheter? Det finns inga, alltså ansvarsområden eller roller på det sättet att, jag vet inte, det bara är ledningen som får använda det och sådär?

R2: Nej. Alla får använda det.

O: Ehm.. Har ni någon utbildning rörande det här då? Ja, policys för nya personer som börjar här och sånt, eller om ni nu uppdaterar det och så?

R2: Ja, nya anställda har ju en halv dag ungefär där dem, man går igenom alla policys och tidrapportering och allting som man behöver veta när man är nyanställd. Och.. Ja.. jag tror inte att man mer än visar vart policyn finns och går igenom de viktigaste. Sen är det väl upp till var och en att läsa så noga som möjligt.

O: Ja, det finns att hitta på något intranät antar jag?

R2: Ja det finns det.

M: Hur ofta ser du över? Jag har förstått att det är du som uppdaterar nu när, hur ofta är det alltså, när du tror att det behövs eller?

R2: Eh, ja.. nu kanske det har blivit en gång per år. Bara kolla igenom hur man byter standard operativsystem, antivirusprogram och såhär. Så den uppdateras inte jätteofta skulle man kunna säga.

M: Mer än när du känner att det behövs alltså?

R2: Ja.

O: Registreras dem, eller har ni någon koll på vilka privata enheter som används? Någon form av, den anställda har så många privata enheter som den använder, något register eller sådär?

R2: Nej, vi har inget egentligen register utan det är ju.. det vi kan se i till exempel mailservern, ser man alla enheter som använder ett mailkonto och sådära. Det är nog där vi kan kolla om det skulle, om vi skulle känna att vi behövde det.

O: Okej. Ehm.. ja.

M: De telefonerna ni får, jag har inte hunnit läsa igenom, är det något specifikt ni, iphone eller vad är det för sorts OS?

R2: Ehm.. vi har.. brukar ha tre olika modeller att välja på. Och det är iphone och någon android och windows phone. Och sen, finns det alltid möjligheter att ta in några önskemål också.

M: Vilka kör ni mest? Eller det är, det kanske inte du kan se? Vad är vanligast?

R2: Nej, jag tror det är ganska lika mellan iphone och android, sen är det lite färre windows.

M: Ja, förståeligt.

O: Hur eh.. hur ser det ut om någon skulle sluta och såhär? Hur hanterar ni det? Om de nu har använt sin privata telefon? Kolla mail och sånt, det kan ju finnas data där som måste bort och så?

R2: Ja, vi stänger ju användarkonton eh.. samma dag som folk slutar.

O: Alltså mailkonton?

R2: Ja. I och med att användarkontot stängs så kommer de inte åt någonting.

O: Men det kan ju fortfarande finnas saker som ligger kvar?

R2: Ja, det är ju svårt att styra om de använder dropbox eller någon sådan extern tjänst så kan det ju finnas dokument där.

O: Ni har inga regler och policys för, hur man hanterar det, vad för tjänst man får använda, som dropbox till exempel då?

R2: Nej, det har vi egentligen inte, vi håller på och går över till Office365 och då kommer man ju få en personlig typ av dropbox kan man säga, så då rekommenderar vi att använda den så långt som möjligt.

M: Varför har ni valt att gå över till just det? Är det för att få bättre koll på allt?
R2: Ja, dels är det att vi är ett så litet företag så det är inte riktigt ekonomiskt att ha en egen mailserver stående här och egna servrar för alla tjänster när de finns i molnet. Och sen är det ju att vi säljer konfigurationen av Office365 till andra så är det ju, vi kände att vi vill, vi behöver göra den resan själva också, liksom förstå vad som händer.
O: Ja, har ni någon form utav, om då folk tar med sig sina privata telefoner här till arbetet.. Har ni något gästnätverk eller så som dem får koppla upp sig på eller får dem koppla upp sig på det vanliga nätverket också? Har ni några restriktioner och så?
R2: Nej, det har vi egentligen inte. Vi.. vi säger väl att de ska använda gästnätet i första hand. Men sen, om de ska komma åt, liksom testa någonting, som är inom de egna systemen så måste dem ju vara på det interna nätet. Då tillåter vi det också.
O: Ni har inga slags regler heller för.. att man får inte koppla upp sig mot vissa zoner, eller vissa enheter här på arbetet?
R2: Nej.
O: Det kan ju finnas vissa saker som kanske innehåller hemligare information än andra eller vad man ska säga.
R2: Ja, vi har ju egentligen inte så mycket hemlig information här, utan det blir ju mer att vi får vår testdata från kunderna. Sen använder vi den under tiden, och sen tar vi bort den.
O: När ni utvecklade den här säkerhetspolicyn, var det för att kunderna efterfrågade det? Du kanske sa det i början? Jag missade det.
R2: Ja ja, det var det.
O: Okej, har ni kollat något på, alltså använt er av några ramverk eller kollat på ISO-standarder och sånt här eller hur har ni tänkt när ni utformade just denna?
R2: Nej vi har inte kollat på det. Utan..
O: Okej, så en intern riskbedömning istället?
R2: Ja, enklare riktlinjer för det.
M: När du skapade de här policys, var det några specifika hot som du kände att detta måste vi skydda oss mot eller det var bara mer..
R2: Nej det var väl mer att den kunden är ett säkerhetsföretag och de har själva väldigt hårda policys, och ja, de vill väl att vi ska vara så säkra som möjligt också då.
O: Har ni haft några komplikationer som har berott på policys, eller att folk har använt sina privata telefoner?

R2: Nej, det har vi faktiskt inte. Och jag tror faktiskt inte vi har haft någon telefon eller platta som har blivit stulen. Vi har haft några datorer men inga telefoner. Så det har vi nog haft tur med.
O: Ja, vi får hålla tummarna att det fortsätter så. Ni har inte funderat på.. ehm.. att implementera något sånt här remote wipe och såhär? Om de nu skulle bli stulna?
R2: Eh.. jo..
O: Det kan man ju göra rätt så enkelt med appar till exempel som de måste installera.
R2: Ja, jo, iphones är ju förhållandevis lätta att göra om man skulle vilja ha någon sådan, och jag tror även det går att göra ifrån mailservern. Att man stoppar mailkontot, så..
O: Ja det går redan kan man säga?
R2: Ja. Till viss del. Ja det är väl eftersom vi inte har haft något problem med det, så har vi inte funderat på det.
M: Nä då ska man inte röra det.
O: Jag vet inte, har du något annat?
M: Nej jag tror nog att vi har fått det mesta. Det går lite snabbare än vad man tror de här intervjuerna. Är det något du själv känner att vi inte har tagit upp som du gärna vill nämna?
R2: Eh, nää det tror jag inte egentligen.
M: Nä, då var det nog allt.
O: Ja, om det är någonting vi har glömt eller sådär som är oklart kanske vi kan höra av oss via mail eller bara ringa?
R2: Ja.
O: Ja men då tackar vi väl så mycket.

Respondent R3

R3: Respondent 3, **M**: Marcus, **O**: Oscar

O: Ja då kan du börja berätta vad din position är inom den här organisationen
R3: Ja jo, jag är samordnare för [organisationsnamn] informationssäkerhetsarbete och det innebär att beslut och budget och dom där grejerna som ligger ute hos varje verksamhet och varje verksamhetschef, så att deligationen är då att är man ansvarig för en verksamhet är man också ansvarig för att säkerheten kring de här områdena och att man följer dem. Så min roll är då mer att se till att vi har fungerande styrdokument och sen då få dem förankrade på olika sätt både i våra verksamheter men också politiskt i de fall det behövs och sen därefter är egentligen min roll också att stödja och vägleda verksamheten och revidera styrdokumentet. Så jag är en form av intern konsult kan man säga.
O: Ja då kan vi gå vidare med frågan om ni har några specifika säkerhetspolicys för privata enhter?
R3: Ja det har vi, det har vi de senaste beslutades i november faktiskt, 2013 då ja, och vad vi håller på med nu nu svarar jag på några av frågorna längre fram men det vi gör nu egentligen att implementera dom riktlinjer och anvisningar, och det är en stor organisation så att då får man ju ha förståelse för att det tar tid att föra också, vi har inte varit jättetydliga tidigare detta är ju en marknad som har formligen exploderat och så att det vi gör nu är att vi försöker att fånga upp och putta ut de förhållningssätt som skall hålla.
M: Hur har ni tagit reda på dessa policys, alltså har ni kollat på andra policys eller ramverk?
R3: Ja det kan man säg, dels har vi haft våra gamla styrdokument att luta oss mot men de är ju utformade sen några år tillbaka och ger ju, det är därför jag reviderar dem för att de ger inte det stöd man behöver helt enkelt, nej det är lagstiftning i grund och botten som reglerar det. Vi är en offentlig verksamhet en förvaltning och är ju ganska lagreglerad verksamhet också. Med hyfsat tunga lagstiftningar i botten då offentlighets sekretesslagen, förvaltningslagen, PUL och en rad andra lagrum som ställer krav och det innebär också att ju mer vi börjar använda mobila enheter desto mer angeläget blir det ju också att vi hanterar dem på rätt sätt, mobila enheter och framförallt smarta telefoner och plattor och sådär skapar helt nya förutsättningar, där många saker som är enkla att använda och lätt skapar beronde

bara är något klick bort, så det försöker vi ta ett grepp kring nu.

O: Hur många anställda, en fingervisning har ni som är anställda, och lyder under dessa riktlinjer?

R3: Ja det har jag ju, det är alla, jag tror att vi är något runt 21 000 anställda sen har vi 50 000 modaliteter och till viss utsträcking påverkas av det också, det kan ju innebära en viss inskränkning till hur man får lov att, till vad man får använda utrustning för internet osv.- så det ska ju vara fritt, [organisationsnamn] är en flexibel arbetsgivare och vi försöker tillmötesgå behoven så absolut långt det går för att inte försöka lägga ett lock på det så, utan snarare vara tillmötesgående men det är klart vi har etiska och moraliska saker att förhålla oss till som vi tycker är, det hära är inte okej tex, och då ska det gälla alla som använder vår utrustning och även våra datorer på medborgarcenter och bibliotek och så, någon form av rätt tar vi oss där.. vad var det vad skulle jag säga så lagrummen då ja, våra policys tar vi hänsyn till en stor portion suntförnuft då såklart och så standarderna som ni nämnde men egentligen kan man säga att våra styrdokument bygger på 27000 serien så att ja, eller standarden som har ett antal, det gör det ju sen har vi valt ut en del godbitar där, vi certifierar oss inte och vi har ingen ambition att certifiera oss heller tex. alltså en jättestor apparat.

O: Alla anställda då som får använda privata enheter eller finns det olika roller? Som har tillåtelse till mer eller mindre?

R3: Ja det förekommer ju, läser man vår nya riktlinje som beslutades i november, så när man har bläddrat igenom de 40-45 sidorna så får man nog en känsla av att det är ganska restriktivt när det gäller användandet av privata enheter och det är återigen kopplat till vilka lagrum som reglerar en verksamhet, krav på diarierföring, hantering av personuppgifter eller annan skyddsvärd information, vilket gör att såfort du blandar in en privat enhet så blir det lite juxigare, men idag har vi ju, idag är det möjligt att använda privat utrustning där.

M: Hur används den då, till mail eller till andra arbetsrelaterade uppgifter?

R3: Ja alltså man kan synka sin mail och sin kalender och så kan man göra. Det finns möjligheter till att göra det.

M: Du nämnde också det nya 40-50 sidor, hur gör ni då med utbildning av nyanställda osv, hur får folk reda på policys, hur får de reda på ändringar när ni reviderat dem?

R3: Vi är just nu inne i en informations kampanj, så nu är jag ute och besöker alla förvaltningar och ledningsgrupper och chefer och bjuder in mig till arbetsplatsträffar och

pratar dels om vad vi behöver att förhålla oss till men pratar också och vägleder i hur respektive verksamhet stöttar sin personal och då använder vi oss av msbs kostnadsfria webutbildning disa, vet inte om ni har sett den? den ligger på msb.se myndigheten för samhällsskilldrad beredskap och så söker ni på d i s a i fritexfältet det är en interaktiv utbildning på 40-45min som tar upp tio viktiga områden framförallt faktiskt kring hur man förhåller sig till IT och IT utrustning men också lite kring information i övrigt och den är grundläggande som allmän brandutbildning eller utrymningsövningar på högskolan eller ngt såntdära typ,så riktar den in sig på vad som är viktigt att tänka på, återigen en jättestor portion suntförnuft men det är relativt det med sunt förnuft, därför är det bra att göra den. Det enda man behöver är 40-45min fri tid och en dator

O: Är detta något obligatoriskt som man måste göra eller...?

R3: Inte ännu, vi arbetar för att föra in den i, alltså detta är egentligen, vi har tagit ett omtag i [organisationsnamn], denna tjänst har varit vacant i ett och ett halvt år så att vad vi gör nu är att vi tar ett rejält omtag, vi tittar både på våra styrande grejor va, och tar hand om det praktiska och kommunicerar också ut, för det är egentligen där det är viktigt att alla användare eller alla medarbetare, att det står något jättefint i ett dokument är ju en sak att kommunicera ut det är en helt annan sak.

M: Ja att alla ska ta del av det och förstå det

R3: Ja, så vi jobbar aktivt med det att försöka få in den här utbildning i , som alltså obligatorisk i introduktionen vid nyanställning, i checklistan där helt enkelt, vi har inte haft det innan men vi kommer att fånga upp det framöver.

O: Registreras de här enheterna på något sätt, har ni någon koll på vem som använder privata enheter, nu är ni ju väldigt många anställda men

R3: Jag vill backa lite på den punkten där, vi har ju såklart koll på antal och så som anslutar till våra servrar och så det finns det ju såklart koll på , jag vågar inte svara på till vilken omfattning det går att urskilja privat respektive tjänsteenhet, jag är inte tekniker i botten utan jag är mer angelägen om att vi har möjligheter att ha koll

M/O: Det svaret är helt okej

O: Då när ni, era nya reviderade policys finns det några specifika tekniska åtgärder som ni uppmanar till eller rekommenderar? Det finns ju vissa applikationer, sandboxning tex om du hört talas om det för att komma åt mail osv,

R3: Vi har inte sagt exakt hur lösningar ska se ut eller kallas osv, utan det är återigen, vi

har valt att sätta dem på en strategisk nivå där har vi ju sagt att vi ska ha såklart, precis som vi har koll på datorer och andra digitala enheter i vår struktur så ska vi ha koll på mobila enheter. Så det innebär ju någon form av ett centralt bandageringssystem för det. för att kunna ja, dels konfigurera dem och sätta upp dem innan användaren får dem såklart men också kunna ha koll på dem över tid, och den dag de inte längre används.

M: Men det är mobiler du pratar om som organisationen äger

R3: Ja men det finns ju också möjliheter att styra såklart privata enheters rättigheter eller möjligheter sålänge man är i nätverket

M: Hur gör ni då om någon slutar hur ser ni till att de inte kommer åt information

R3: Ja det är ju krux, det är det ju, och då är det återigen, det går ju strikt säkerhet tror jag, jag är inte tekniker, men att reglera detta tekniskt att strypa detta och inte göra, sådana saker men vi jobbar rätt mkt med att försöka skapa medvetenhet och insikt också för att vi återigen, vi är en offentlig förvaltning, vi är ju inte till för oss själva riktigt va vi är till för kommunens medborgare och det perspektivet måste vi ha och bli påminda om, det är både en HR fråga och till viss del teknisk blir det ju.

O: Ja finns det några speciella aspekter rörande de här privata jämfört med andra mobila enheter som du vill framordna eller som är specifikt bara för privata?

R3: Ja, alltså, det viktigaste är ju att säkerställa att vi inte får in något skräp i vår infrastruktur att det inte finns någon information som [organisationsnamn] äger och som vi är skyldiga
att hantera utifrån lagkrav och annat kommer oberhöriga tilldels eller sprids på ett okontrollerat sätt och det är ju..

M: Ja det blir ju lite annorlunda att hantera på privata

R3: Ja det blir det ju och du kan ju aldrig, det här med sandbox och olika miljöer kommer in i enheterna men du kan aldrig hindra en medarbetare som har sin privata utrustning att ladda ner appar och göra som den vill med sin utrustning såklart, och därför har vi också sagt att, eller lagt in i vårt styrdokument, vissa begränsningar som gör att man måste stanna till, det kanske fortfarande är teknisk och praktisk möjligt att göra det men vi jobbar mycket med att upplysa medarbetare om att även om det är tekniskt och praktiskt möjligt att genomföra så är det kanske inte praktiskt att genomföra ändå.

O: Ja, skapa en vi medvetenhet så att det kanske, ja, de kanske inte tänker på att de gör det för att, menar du så

R3: Ja vi är vanliga människor och vi jobbar, man följer sina rutiner och så, man gör det man tycker fungerar bra för en själv och så såklart, men återingen vi försöker jobba mycket med medvetenhet hos användaren så att man får en förståelse för att det kan finnas gränser ibland, sen är det ju så att det mesta i vår verksamhet är ju också tillgängligt för allmänheten, offentligt va, men det innebär ju inte att man kan vika flygplan och kasta ut pappret genom fönstret kanske alltid va, det innebär ju också att även om handlingen är offentlig och allmän så ska den ju ändå granskas ur ett säkerhetsperspektiv innan man lämnar den ifrån sig och det är ju där kruxet är då om man skickar upp den till dropbox eller använder evernote eller synkar sina enheter med olika molntjänster och kör på automatisk säkerhetskopiering där man kanske inte har tittat igenom inställningar vad är det nu vi säkerhetskopierar, kopierar vi alla dokumenten i telefonen eller inte, i min privata tex så klickar jag på en bifogad fil i min mail, då har jag inte jobbet på min privata, jag särbeskiljer det, av ren självbevarelsedrift.. men iallafall klickar jag i den telefonen jag har, klickar jag på en bifogad fil där så lagras den i filarkivet så sen måste jag sen fysiskt gå in och plocka bort den, det kanske inte är så i alla telefoner men i just min är det iallafall, vilket ställer krav på mig då om jag hade nu använt den för tjänsteutövning

O: Det är ju vissa telefoner som kommer förinställda på det sättet, då måste man alltid gå in och det är inte alla som vet det.

R3: Det är komplicerade enheter idag, det är inte alla som vet det, det är det ju.. man lämnar mycket åt användaren och som samhället ser ut idag så har man inte den tiden och lusten kanske eller orken att sätta sig in i alla de inställningar som man kanske måste göra.

O: Specificerar ni några speciella uppkopplingsätt för privata, är det okej att koppla upp dem mot datorn eller nätverket och sådär, specificeras det på något sätt?

R3: Ja det gör det, vi har det i riktlinjerna, vilka regler och rutiner som gäller för anslutning till nätverket. Så att där står det om

O: Man kan ju koppla in telefonen i datorn med sladd och sådär också, det är också specificerat?

R3: Ja, det vågar jag inte svara på, men det är säkert möjligt va, det är säkert möjligt, det är mycket som är möjligt va..

O: Vem är det som har utformat den här, du är ju dels ansvarig för det men ni är en grupp personer?

R3:Ja precis det har varit en ganska lång resa, jag har tagit fram ett utgångsmaterial som

vi har diskuterat utifrån, inledningsvis avdelningarna här på statskontoret, HR, juridiska, vår IT-avdelning då, kommunikations avdelning så har vi diskuterat och så och när vi har känt oss tillfreds så har vi lyft politiskt för att få en stämpel alltså få en check, sen därefter har det gått ut i alla våra förvaltningar i en intern remiss runda. där man har fått tycka till och gett synpunkter sen har de paketerats sen har vi dansat en runda till på statskontoret sen har man lyft det för politiskt beslut

M: Väldigt lång process

R3: Ja, 8 månader

M: Hur ofta brukar ni uppdatera policyn, sker det kontinuerligt, en gång om året eller hur fungerar det?

R3: Ja, det är ju precis sant ja, den kommer att revideras, gås igenom en gång per år det står även inskrivit i beslutet att det ska göras så, det innebär kanske inga förändringar men den skall gås igenom och hållas uppdaterad på årsbasis

M: Då är det inte samma process utan kortare?

R3: Ja då är det betydligt kortare process

O: Vilka tycker du är de största hoten med mobila enheter?

R3: Ja vi har kanske tangerat det redan men det största skillnaden är väl egentligen att tjänsteenheter går ju att kontrollera är ett hårt ord men går ju att bandagera på ett annat sätt än privata, så att vi kan förhålla oss till dem på ett annat sätt än privat utrustning ju, eftersom där har du ju alltid den enskilda medarbetarens egna liv att förhålla dig till men så det är det vi försöker det vi försöker ta kontroll över om vi ska säga så är ju informationen.

O: Informationen snarare än enheten kan man säga

R3: Att det är informationen som är viktig att skydda så att

R3: Ja men det är ju vi har ju det diariet är ju en grej va, alla appar och de rättigheter som de kräver för att fungera är ju en annan grej där man sällan har koll på avtalen skrollar man ner till sidan 27 och så klickar man okej

M: Är det kanske något speciellt, någon fråga som du gärna vill berätta eller belysa

R3: Nej, jag kan inte komma på något direkt, nej

M: Är det möjligt att kika på er policy eller den får man inte ta del av?

R3: Jodå, jag kan skicka den till er två, den är ju politiskt beslutat så det är inte nått hemligt så i den, utan det är mer på en strategisk nivå, säger ju inte hur de tekniska lösningarna ska se ut heller, den säger inte heller inte till vilken omfattning vi har det eller inte har det, den anger liksom att här

har vi ribban, och alltså vad vi ska kunna hoppa över med eller utan spikskor

O: Ja man får väl göra det mer så när man är en stor organisation så får man ta det lite mer lokalt sen, lite mer specifika lösningar

R3: Ja vi har ju en jättestor IT-drifts avdelningar också satt om vi jobbar med e strategiska frågorna här så bryter de ner dem sen i tekniska lösningar på vår driftenhet, där är ju inte jag alltid med på det sättet, och även om jag är med så har jag svårt ibland att hänga med, om vi säger så. men det är ju en fördel att ha ett politiskt beslutat styrdokument och det innebär ju också att det är lättare att få till stånd lösningar och sådär

O: Är det färgat av vem som bestämmer för tillfället sådär, kan det då va att ena året är det social demokraterna som sitter här och nästa år kanske moderaterna blir det, vill de ha olika osv då eller ändras det då? hur fungerar det?

R3: Nej, det kan jag absolut inte påstå, i det här fallet det är här, det vi pratar om just nu det styrdokument som jag refererar till hela tiden, det är ju i mångt om mycket lagreglerat, det här är i många fall, för ett företag är det liksom upp till skall vi skall vi inte göra det dem har lagen om företagslagen om företagshemligheter att förhålla sig till men i vårt fall så är det ju ta alla vård och omsorgsenheter tex, dom regleras ju bland annat under patientdatalagen som socialstyrelsen tar och ger ut riktlinjer för hur man ska förhålla sig, det står inte i vägledningen, i handledningen till patientdatalagen så står det uttryckligen att man ska arbeta systimatiserat med informationsäkerhetsfrågor, och det står patientdatalagen men det är ju inte bara ettor och nollor i information utan är all vårdrelaterad information oavsett hur den är förpackad och där ställer politisk majoritet och vilken färg man har inte roll, så det är utöver det rent självbevarelsedrift liksom, så att nej det kan jag inte påstå, inte i detta fall

M: Tror nog att vi har fått reda på allt vi vill och lite till!

R3: Ja hör gärna av er om det är något mer ni vill ha reda på!

M/O: Ja vi tackar så mycket

Respondent R4

R4: Respondent 4 **M**: Marcus **O**: Oscar

R4: Däremot så har vi ju en informell policy om mobilerna som är uttalad från mig om vad som gäller
O: Alla känner till den?
R4: Ja det kan man säga, den har diskuterats i ledningsgruppen så när det gäller devices i [organisationsnamn] så har vi offantligt många, inte mobiler kanske så men ipads tex, hela högstadiet är utrustat med det
O:Tänkte bara börja, du har fått frågorna och så innan och hunnit kolla igenom?
R4: Nej, kör igen
O: Då kan vi börja med vilken befattning du har här på [organisation]?
R4: Jag är it och service chef
O: Hur många anställda har ni här, hur många lyder under era policys?
R4: 1200
O: Okej, är det inkluderat med skola och såhär?
O: Så har ni några specifika policys för mobila enheter?
R4: Alltså naturligtvis man får ta med sin privata mobil till [organisationen] men man får inte på något sätt koppla upp sig mot våra nät i dagsläget så när det gäller denhära hypen med BYOD så har vi varit ganska så svala i frågan och egentligen faktiskt från ett perspektiv och det är att det finns så mycket devices där ute redan som [organisationen] måste ta hand om, om man ser på ipaden på högstadiet och så, så har vi ju beräknat det trådlösa nätverkets kapacitet efter detta. Sen skulle vi helt plötsligt börja slå på privat användning av mobiler så hade vi förmodligen behövt bygga ut nätet med 30% kontra dagens då va. Det är nog ingen kostnad som som våra politiker skulle vilja ta va för att våra anställda ska kunna ha sina mobiler mot [organisationen].
O: Så det är en teknisk fråga då om kapacitet?
R4: Ja rent principiellt så hade jag kanske inte haft något imot att man kopplar sig mot [organisationen] trådlösa nät va för vi använder oss av 82x[otydligt] i [organisationen], vilket medgör att vi har väldigt bra koll på vilka devices som är i nätet och då liksom bara kunna skapa en åtkomst för just internet med detta. Så vi är inte så oroliga från just det perspektivet, säkerhetsperspektivet det är vi inte, utan det är mer en kapacitetsfråga.

O: du säger att man inte får koppla upp mot just ert nät här, men kan man använda det hemifrån använda jobbmail osv?

R4: Ja det är det

O: Har ni någon form av policys där eller är det någon slags teknisk app för det?

R4: nej vi använder oss av activ sync så sålänge du kan ditt användarnamn och lösenord så är det frittför dig att koppla upp din mail, där säger vi inte att man inte får

O: om man tex vill ladda ner något från sin mail, en pdf tex eller liknande, då kan det hända att man sparar det på en privat dropbox eller något sådant hur ser ni på det?

R4: Varje person som anställs i [organisationen] har skrivit på ett anställningsavtal så skriver man på en sekretesförbindelse också, i samband med det och då är det upp till den personen att veta om sina skyldigheter och om man då tittar på vår sociala verksamhet som kanske kanske då just är mest utsatt när det gäller sekretessbelagt material så är man väl medveten om det där vad man får och inte får göra med just filer. Det ingår i deras yrke och utbildning om hur man hanterar sekretessen, men sen kan det finnas annan personal som kanske inte är så medveten om sekretessbestämmelser men där har du ett personligt ansvar att följa de sekretesserna, det är lagen ju att följa dem. Och det är lite så att dethära sekretessreglerna som gäller finns tillgänliga och man kan därför inte hävda att man inte läst dem. För att man har skrivit på ett anställningsavtal så är du defaktivt skyldig att ta reda på vilka lagar och policys som gäller.

O: erbjuder ni någon form av utbildning eller hur gör ni med anställda osv, webutbildning eller liknande?

R4: Nej ingen webutbildning därimot finns det ett introduktionsprogram och där är en del av dessa delgivningar och defintitivt inom den socialaverksamheten.

O: Är detta obligatoriskt när man blir anställd eller är det något ni uppmanar?

R4: det fallar ganska naturligt att man ska göra det, bland annat så får man en sånhära paketerad låda då va. när man börjar, där finns foldrar, information om vart du ska anmäla lönekonto någonstanns och det finns policys, och då också om sekretesspolicys. Så det blir svårt att hävda att man inget visste.

M: Hur ses dessa säkerhetspolicys över? hur ofta görs detta?

R4: Det är en lag så att,

M: Ni bygger alltså inte på den? Alltså utvecklar policys utifrån den

R4: Nej, lagen är ju liksom ganska tydlig vad man får och inte får göra med sekretess och det räcker med den lagen.

O: Ni har någon form av policy antar jag för organisationsägda telefoner som ni får eller är det också bara sekretessbelagda och sådär. Ni sa att ni inte hade några specifika för privata men har ni några som utvecklats för telefoner som man får av [organisationen]?
R4: Nej inte mer än den säkerhetspolicy som gäller generellt för [organisationen] alltså, den hanterar vissa frågeställningar och där är inte mobiler specifikt utsatta som någon särskild enheter i sig själv utan den appliceras på hela säkerhetsframen för [organisationen] där den ingår som en device liksom, det är precis som en dator liksom samma princip
O: Du sa innan något om registrering, se vilka som är anslutna till nätet?
R4: Vi har väl inget fullt utvecklat MDM system men när vi till 90% bara använder IOS i [organisationsnamn] så använder vi apples propermanager för att hantera telefoner då har vi liksom det finns två vägar via detta kan man remotewipea telefoner eller låsa upp dem. Men sen har vi också via exchangen möjlighet att wipea. Det ingår i active sync protokollet och changen om man då kopplar sig mot exhangen med en mobil så får du, så kommer den liksom, så kommer där en, så accepterar du detta här. Kan vi göra följande liksom? På telefonen. Och när dem trycker ok där så aktiveras det med autosyncen, och då kan man liksom remotewipea det hållet också.
O: Ah, okej. Att man tvingar på policys till telefonen kan man säga?
R4: Ja, det kan man säga ja.
O: Ehh, det här med Apple du nämnde, är det applicerbart även på Android-telefonen om ni gör det? Och du har en windowstelefon där va?
R4: Ja, det är en windowstelefon.
O: Det funkar på allt eller?
M: Än så länge.
R4: Ja, nä men så är det. Alltså active sync ingår ju som en del i protokollet. Däremot så vet jag ju kanske, är osäker, på huruvida hela telefonen kan wipeas. Ehh, men definitivt den mailkorg som finns på telefonen. Men jag har för mig att.. jag är lite osäker där.
O: Ja okej.
M: Hur tas de här mobila enheterna omhand om någon eventuellt slutar? Har ni någon policy för det också eller? Eller hur fungerar det? Det bara lämnas in också eller?
R4: Det är ju den ansvarige chefen som ser till att produkten, eller arbetsrelaterat material återvänder, så det är upp till varje chef att sköta det.
O: Också stängs konton av antar jag?
R4: Vi har ju en metakatalog i [organisationsnamn], så när en person blir anställd och börjar jobba i

personalsystemet så skjuts den per automatik in i adn va. Och öppnar och ger rätt behörighet och så, och när personen slutar så stängs det per automatik också. Det är en metakatalog som sköter hela det.

O: Ehm.. ja vad tror du är de stora, eller anser du är de största hoten med att använda privata mobila enheter? Om ni nu kommer expandera det i framtiden och tillåta det på ert nätverk? Vad tror du är det största hotet med det?

R4: Nä, inte hot kanske.. ja..

O: Eller risk då.

R4: Ja, eftersom jag är oerhört nyfiken på en aspekt. Man har ju hört de här till exempel, vissa kommuner som erbjuder gratis wifi. Och eh.. de måste ju lyda under ungefär samma lagar som gäller för dem som är internetleverantörer. Nu visserligen är det uppe i EU nu och har ju kanske dödat IPRED-lagen i Sverige, men där har man ju faktiskt en skyldighet att lagra data i sex månader. Jag menar, hur betraktar man då en privat mobil där? Eh, då blir vi ju som [organisationsnamn] helt plötsligt internetleverantör ju, eller hur? Lyder vi under samma lag då? Jag skulle gissa det ju.

M: Det bör ju bli så ja.

R4: Mm. Och det innebär ju att vi helt plötsligt ställs inför helt nya utmaningar. Vi måste införskaffa utrustning som ser till att logga det här i den tiden, det är väl IPRED-lagen som reglerar det. Sex månader tror jag att det är. Och hur tusan har man gått runt detta? Till exempel Helsingborg som erbjuder wifi. Gör man det där uppe då? Jag är väldigt nyfiken på det. Ehh.. nu har ni inte fått något svar på er fråga men, det är väl en sån utmaning. Men sen, det är klart alltså, där finns väl inget IT-system i världen som är 100%-igt säkert. Så är det ju.

O: Nej..

R4: Men man får ändå förlita sig på 800x-protkollet. Så om en telefon skulle bli nedsmittad av nåt skit till exempel va, av något slag då, som bara händer Android för den delen. Men ehh.. Så då har man ju i princip bara tillgång till internet. Du kan ju inte accelerera ditt hack och gå vidare in i [organisationsnamn] servrar. Men däremot så är det ju också intressant där om nu det här hacket kommer utifrån [organisationsnamn] servrar, ja vilket ansvar har vi då?

O: Ja precis.

R4: Ehm.. och det matchar väl litegrann det här, det här att vara internetleverantör. Men sen i grund och botten är ju det här också en ekonomisk fråga som jag nämnde i början.

O: Ja..

R4: Är [organisationsnamn] beredd att träta på vårt trådlösa nät för att man skall ha privata enheter med? Jag är oerhört tveksam att politiken skulle anslå 300-400 000 för att göra det. För att folk ska ha med sig sina egna devices.

O: Ja. Nej.

R4: Jag tror inte det. Jag tror de pengarna är mycket nyttigare att lägga på skolan. Eller till några andra tjänster eller nånting.

O: Ja..

R4: Så det är jag nästan övertygad om. Däremot kan jag tänka mig att man skulle vara intresserad i politiken av att erbjuda till exempel gratis wifi. Till exempel i vissa valda delar av [namn]. [Namn] är ju oerhört populärt till exempel. Då kan jag tänka mig att de kanske skulle kunna få för sig att.. men då återigen, då får man verkligen vara ytterst medveten om vilket åtagande man tar på sig som offentlig verksamhet alltså. Så att om man skulle tillåta en device i [organisationsnamn] nät då är det ju, om jag skulle behöva komma åt min mail till exempel på den devicen då är det ju ut på internet och in, via active sync på det hållet alltså. Jag hade ju aldrig nått upp, det är jag säker på.

O: Ehh.. jag vet inte, jag glömde nog fråga dig i början, men vem är det som är ansvarig för säkerhetsgrejer? Är det bara du eller är det fler? Är ni en avdelning eller nåt eller hur ser det ut?

R4: Nej, alltså vi är ju, vi har en säkerhetschef på [organisationsnamn] som är med också. Men de här frågorna hamnar ju oftast på mitt bord. Utan tvekan så. Så att det jag nämnde i början, det här med att hitta en lämplig policy för hur en offentlig organisation anskaffar telefoner ska få lov att hanteras, det är nånting som vi ska titta på. Där finns ju många aspekter på det faktiskt ju. Ehh.. till exempel kan man ladda ner facebook? Kan man använda facebook? De här telefonerna har ju inte heller access in i våra nät eller känsliga servrar.

O: Nä

R4: Utan de kopplas ju också på samma, samma, ett VLAN som bara gäller internetaccess, och ger inte tillgång till några andra servrar eller sånt alltså, utan hanteras ju som icke säkra enheter alltså.

O: Så det finns olika säkerhetszoner kan man säga för vilka enheter som får koppla var?

R4: Ja, och det vi [otydligt] så har man ju den möjligheten att bygga..

O: Olika lager liksom?

R4: Ja.

O: Har du några mer frågor sådär?

M: Jag tror inte det.

O: Jag tror vi fått med det mesta.

R4: Ja men det var ju bra ju. Hur är era egna tankar?

M: Om detta?

R4: Ja.

O: Då kanske vi ska stänga av här först så behöver vi inte skriva det två gånger.

Respondent R5

R5: Respondent 5 **M**: Marcus **O**: Oscar

M: Ja då kanske vi kan börja med vad du gör här, vad du jobbar me?
R5: Jag är itchef för [Organisation] så jag ansvarar för itverksamhet och den strategiska utvecklingen och hur vi använder IT, tillsammans med andra verksamheter såklart.
O: Hur många anställda är det som arbetar här
R5: på avdelningen?
O: ja eller som då lyder under eventuella policys, är det hela lunds kommun?
R5: Ja det är det, vad är vi 6 000 ungefär
O: Är det inkluderat med skola och så?
R5: Ja, inte elever då
O: Nej men lärare osv
R5: ja
O: Ja, har ni då några specifika säkerhetspolicys för privata mobila enheter?
R5: ja, vi har en informationssäkerhetspolicy som jag tänkte att jag kan maila till er, den är inte nere på detalj i alla frågor men sen har vi, alltså du kan använda din privata enhet men du kommer in åt saker, alltså så utan att vi har godkänt det
M: Så det är mer mot mail, kalender och så?
R5: Ja, jag kan synca min epost och kalender på min privata mobil om jag vill men då lägs det en teknisk policy att jag måste ha vissa lås på den och det går in stjärnspärr och så så att vi löser det
O: det är en tekniskpolicy som tvingas på om man vill göra det?
R5: ja
O: Är det om man kopplar upp sig mot nätet här i lunds kommun eller kan man kolla hemma också?
R5: Ja man kan kolla hemma också men jag måste verifiera att jag är jag med mitt användar id och så
O: Vad är det för lösning då teknisk vet du det
R5: äm, nej det är lika olika beroende på vad du använder för mobil enhet. Om du har en sånhär dator som jag har idag som vi har installerat så kan jag sitta hemma och jobba i stort sett på samma sätt som jag gör på kontoret och det har vi löst genom någon som heter direct access som ligger i

Microsoft miljö, att man har ett certifikat på datorn och så, nu är jag lite nere på teknik som jag inte kan, äm, om sen har vi så att man kan logga in sig via zitrix och köra från vilken dator som helst, men då har du en begränsning på vad du kan komma åt.

O:Tänker mest med smartphones eller tablets, har ni något... det är mest det vi skriver om

R5: ja okej, ja egentligen kan du göra rätt mycket oberoende av vilken utrustning du ansluter med, det här är ju en platta tex, så den är ju ganska ny då men annars är det många som har mobila datorer eller så idag finns det ju nästan inget annat än smartphones, men sen är det inte alla som använder dem som smartphones, många använder dem fortfarande som telefoner, så det ser lite olika ut i olika verksamheter.

O: ja hur har ni utformat de här policys som ni har? något specifikt för privata, hur har ni tänkt det finns massa ramverk man kan använda och ISO också tex

R5: vi gjorde en revision...

O: ja ni har kanske reviderat dem till viss del sedan ni gjorde dem från början

R5: vad det gäller informationssäkerhets planerna vad gäller våra system som sen egentligen reglerar [Otydligt].. så har vi även redan en bits, vi kommer revidera dem nu igen

O: Bits vad är det?

R5: Det är en sånhär standard, men den gäller egentligen inte längre, utan så vi behöver revidera den

O: hur ofta gör ni det, tittar på policys och reviderar dem ,ser om de behöver updateras?

R5: nu är det nog tre år sedan

O: Så det är inget stående att det ska göras årligen?

R5: nej det borde göras oftare, jag kan inte exakt säga om det står i policyn hur ofta det ska göras,sen ser vi över dem när vi gör förändringar i system. men själva policyn i sig försöker vi att inte förändra för mycket. Det tar ju tid att förankra en policy.

M: Hur tar anställda del av denna policy, har ni någon utbildning när de anställs och så?

R5: Det ser lite olika ut i olika verksamheter, lite grann beroende kanske på, men en del har det ju i sina introduktionsprogram, men annars har vi det på vårt intranät

M: så det är lite upp till var och en att se till att de förstår

R5: Ja medan vård och omsorg har specialutbildningar för sina, alltså det kan se lite olika ut beroende på hur man jobbar

O: Men det finns ändå en grundläggande tanke och nerskrivet att man ska ha utbildning

R5: ja, och informeras om det

O: ja ta del av det, vet du till vilken utsträckning folk använder privata mobila enheter?

R5: jag tror inte man använder

O: kanske svårt att säga om ni är 6 000 men..

R5: Jag tror att man använder privata mobila enheter väldigt lite omfattning för sina arbetsuppgifter. därimot kan man göra det som jag kanske, alltså göra det för att man tycker att det är enklare med en kalender och då vill jag ha kalendern även på min privata telefon. äm, för att tanken är ju att behöver man mobila enheter så skall arbetsgivaren tillhandahålla det.

O: Och det gör ni också då ja.

R5: Ja.

M: Har ni några specifika tekniska applikationer på mobiler då, som gör att det inte läcks eller så att ni kan ta bort information på mobilen om den skulle tappas bort?

R5: Nej.

M: Så ni kan bara stänga av konton då?

R5: Ja idag är det så.

O: Har ni något sätt att veta, registreras enheter när de används på nätverket,vet ni vilka som är uppkopplade, jag antar att ni vet om det är telefoner som [Organisation] äger men kan ni se på något sätt annars?

R5: Ja jag tror vi kan se, jag är lite osäker på det så det kan jag kolla upp och återkomma med om ni vill men vi kan ju se vilka utrustningar som är uppkopplade. Sen kan vi inte spara loggarna hur länge som helst. men både på datorer och telefoner. vilka, man kan tex se på mitt mailkonto att jag har två items som syncar allting och så.

O: Vem är det som ansvarar för säkerhetspolicys? Ja det är ju du bland annat har ni en avdelning?

R5: Nej, det står lite om roller och ansvar i säkerhetspolicyn.

R5: Övergripande ansvar har kommunstyrelsen och kommundirektören. Ehm, på det ligger ju verksamhetsansvaret. Sen har ju vi på IT-avdelningen ett samordningsansvar för säkerhetsavdelningen och sen finns det ju då ansvarsroller för systemnivå, eller informationsmängdsnivå är det ju egentligen.

O: Hur många är det som jobbar på IT-avdelningen?

R5: Vi är 50.

M: Vilket operativsystem kör ni mest?

R5: Eh.. Windows 7.

M: Ni kör inga Apple-produkter?

R5: Jo.. skolan kör Apple-produkter, men den biten är mest elever. Och då kör de ju inte i verksamhetens system. Iphones har vi såklart.

O: Jag vet inte, vi kanske redan har svarat på frågan lite sådär svävande men jag bara, skiljer sig säkerhetspolicys mellan privata och organisationsägda, finns det något, finns det nån speciell aspekt som gör att? Som är bara för privat så att säga?

R5: Alltså du kan inte tekniskt komma åt lika mycket saker med utrustning som inte vi certifierar.

O: Okej..

R5: Och det gäller egentligen både telefoner och datorer och så. Och då ligger det ju, i denna har vi certifikat som godkänner att vi släpper in, medans en privat dator kommer du bara åt då via de här fjärråtkomsttjänsterna och då ligger säkerheten på en annan nivå.

O: Säkerhetslager kan man säga då alltså?

R5: Ja.

O: Ja okej. Finns det specificerat också på något sätt om man har med sin privata telefon på jobbet, som väl många gör antar jag, även om dem inte använder den privat.. eller jag menar att arbeta med. Ehm.. finns det specificerat då att man får koppla upp sig till exempel mot arbetsdatorn eller sådana här saker?

R5: Nej

O: Alltså hur man får göra?

R5: Nej det tror jag inte.

O: Okej. Vad har vi mer vi ska fråga?

R5: Alltså vi har ju riktlinjer för till exempel hur man hanterar dokument. Oavsett om du lägger en film på en dator eller USB eller skriver ut den eller faxar den fel så styrs det oftast av lagrum. Att du ska vara aktsam. Men vi har inte satt någon begränsning.

O: Okej, men det finns alltså lagrum och sådana saker som styr?

R5: Ja.

M: Hur hanteras mobiler, eller mobiler och datorer när någon slutar?

R5: Eh, då ska de ju lämnas tillbaks. Så verksamheten avställer ju de då och använder dem till något annat. Och då ser vi ju till att installera om dem. Ja.. Men just telefoner är det nog lite sådär..

M: Ger ni ut telefoner också då? Det är datorer ni ger ut, ger ni ut telefoner också om det önskas?

R5: Ger ut?

M: Ja alltså till anställda.

R5: Jaja, men det får verksamheterna beställa. Behöver de en mobiltelefon så beställer de en

mobiltelefon. Och det ökar jättemycket. Och sen så, när den medarbetaren slutat så är det ju fortfarande kommunens telefon. De kan ju inte ta den med sig. Men den kan ju användas till någon annan eller så skrotar man den.

O: Ehh.. men det kan ju tänkas då att när någon slutar så har de kommit åt ett mail då som man kan göra via sin privata telefon. Sedan kan det hända, det kan ju vara att man inte vet. Ibland kan det hända att det synkas automatiskt via dropbox och sådana här saker om man kollar på en fil via mailen. Finns det någon teknisk begränsning för det eller? Någon policy som säger hur det ska hanteras? Det kan ju liksom vara omedvetet.

R5: Nej det har vi inte riktig stenkoll på.

O: Okej. Nä.

R5: Du kan ju..

O: Så det kan vara en potentiell läcka? Omedvetet och så men..

R5: Ja det kan det vara.

O: Det är ju svårt att hantera också, speciellt om man tänker på lagar och så.

R5: Ja, nej. Alltså generellt sett så säger vi ju att ingenting ska synkas i dropbox. För vi har ju ingen koll på var dropbox finns. Alltså så.

M/O: Nej det ägs ju av dem också.

R5: Haha ja. Så nej.. vi har ju egentligen ingenting som ska lagras lokalt och så. Utan det ska ju ligga i systemen eller våra nätverksplatser. Visst, tar någon och flyttar en fil medvetet.. men det kan man ju göra i pappersform också.

O: Men då bryter man ju å andra sidan.. ni har ju policys som säger att man inte får det, lagar och sånt. Så man bryter ju det då liksom.

R5: Ja.

O: Det går ju inte att skydda sig mot allt tekniskt kanske. Det är nästan omöjligt.

R5: Nej.. då blir det lite svårt att jobba också kanske.

O: Vilka är de största hoten som du ser det med att ni tillåter användning av privata enheter? Eller i framtiden, vad som kan vara?

R5: Alltså jag skulle inte säga att vi tillåter det för vi använder ju inte det. Det du kan göra är att du kan synka din epost eller din inkorg. Sen ska man ju inte skicka sekretessmaterial med mailen. Står också i så.. Ehm.. Jag tror ju den största risken kanske är att man får in virus eller att man får in saker i systemet. Mer än att man sprider information. Och överhuvudtaget.. alltså de mobila lösningarna.. det händer saker hela tiden.

O: Ja. Svårt att hålla 6000 enheter uppdaterade.

R5: Ja.. och alltså det kommer ny teknik hela tiden och så. Man såg ju den här luckan som var nu. Kring lösenord och kryptering. Man kan tycka man har koll.

O: Se om det var någon mer fråga här.

M/O: Finns det något annat du vill nämna som du tycker att vi har missat? Eller som du gärna vill berätta?

R5: Ja alltså.. jag tror att den stora utmaningen ligger, och det har jag upplevt i många år, just det här med balansen mellan säkerhet och integritet. Och att tekniken oftast går före både lagar och rutiner och praxis. Alltså molntjänster är ju en typisk sådan. Ehh.. och det kommer det nog alltid att ha. Mobiliteten möjliggör så mycket bra så man tänker kanske inte igenom. Man börjar använda det innan man kanske har tänkt igenom hela kedjan. Det handlar liksom mer om att jobba. Man blir aldrig färdig.

O: Man bara försöker hänga med.

R5: Ja lite så. Och man försöker... det som är viktigt det är det vi skyddar. Kärninformationen. Och ehh.. sen är människan full av misstag. Man kan göra fel, men man måste göra det så enkelt som möjligt.

O: Man kan sammanfatta det med att det är viktigast, eller en bra strategi att försöka skydda informationen ifrån att läcka istället för att skydda enheter från att komma åt den? Kan man säga så?

R5: Ja att man...

O: Om ni är en så stor organisation så kanske det är lättare att försöka skydda det som är viktigt än att skydda 6000 olika enheter.

R5: Ja. Jag tror det. Jag tror kanske förr att man mer byggde säkerheten genom att man låste liksom åtkomsten och så hade man jättekoll på allt inom. Medans nu låser vi in det som är viktigt i kassaskåpet och sen så får vi ha koll på hur man kommer åt det. Och vissa saker är kanske okej att man kommer åt och vissa är absolut inte. Eh.. så man får liksom ha dem klassningsmodellerna helt enkelt.

O: Då har jag ingenting mer. Har du?

M: Nej jag tror vi fick med allt.

O: Så då tackar vi så mycket.

R5: Ja tack.

8 Referenser

Al-Hamdani, W. A., & Dixie, W. D. (2009). *Information security policy in small education organization*. Paper presented at the 2009 Information Security Curriculum Development Conference, Kennesaw, Georgia.

Bin Muhaya, F. T., Fazl e, H., & Ali Minhas, A. (2012). ON THE DEVELOPMENT OF COMPREHENSIVE INFORMATION SECURITY POLICIES FOR ORGANIZATIONS. *International Journal of Academic Research, 4*(1), 16-22.

Bits.org, (2014). BITS – Home,
http://www.bits.org/,
(Hämtat: 20 Maj 2014) [Elektronisk]

Brand, J. C. (2013). *The governance of significant enterprise mobility security risks.* (Master of Commerce (Computer Auditing)), Stellenbosch : Stellenbosch University.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS. *MIS Quarterly, 34*(3), 523-A527.

BYOD Brings Wave of Unknown Security Threats. (2012). *CIO Insight*, 1-1.

Carrillo, J. (2013). IT Policy Framework Based on COBIT 5. *ISACA Journal, 1*, 24-27.

DeLaGrange, K. J. a. T. (2012). SANS Survey on Mobility/BYOD Security Policies and Practises.

Eddy, N. (2014). BYOD Businesses Still Lack Effective Security Policies. *eWeek*, 2-2.

Elachgar, H., & Regragui, B. (2012, 2012 / 01 / 01 /). *Information security, new approach*.

Emery, S. (2012). Factors for Consideration when Developing a Bring Your Own Device (BYOD) Strategy in Higher Education *AIM Capstone 2012*. Univeristy of Oregon: Applied Information Management.

Europa.eu, (2014). Definition av mikroföretag, små och medelstora företag, http://europa.eu/legislation_summaries/enterprise/business_environment/n26026_sv.htm, (Hämtat: 17 Maj 2014) [Elektronisk]

Ey.com, (2014). Bring your own device mobile security and risk, http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf, (Hämtat: 4 April 2014) [Elektronisk]

Fiorenza, P. (2013). Mobile Technology Forces Study of Bring Your Own Device. *Public Manager, 42*(1), 12-14.

Fiorenza, P., Tepe, L., Ribeira, J., Vogel, V. Exploring Bring Your Own Device in the public sector. *Research report*.

Gartner.com, (2013). Gartner predicts by 2017, half of employers will require employees to supply their own device for work purposes, http://www.gartner.com/newsroom/id/2466615, (Hämtat: 3 Maj 2014) [Elektronisk]

Glisson, B. W., & Storer, T. Investigating information security risks of mobile device use within organizations.

Glisson, W. B., & Storer, T. (2013). Investigating Information Security Risks of Mobile Device Use within Organizations. *Proceedings of the Nineteenth Americas Conference on Information Systems, Chicago, Illinois, August 14-17, 2013.*

Greamo, C., & Ghosh, A. (2011). Sandboxing and virtualization: Modern tools for combating malware. *IEEE Security and Privacy, 9*(2), 79-82. doi: 10.1109/MSP.2011.36

Guérin, N. R. C. (2008). Use of Handheld Devices in a Corporate Environment.

Isaca.org, (2014). Cobit 5 - A Business framework for the governance and management of Enterprise IT, http://www.isaca.org/COBIT, (Hämtat: 4 April 2014) [Elektronisk]

Iso.org, (2014). ISO - International Organization for standardization, http://www.iso.org, (Hämtat: 4 April 2014) [Elektronisk]

Itil-officialsite.com, (2014). ITIL Home, http://http://www.itil-officialsite.com, (Hämtat: 4 April 2014) [Elektronisk]

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

Jindal, A. K. (2013). *Protecting Android Devices Following BYOD Policy Against Data Security and Privacy Attacks.* (M.Tech), New Delhi. (IIT-D-MTech-CS-IS-13-MT11003)

Khanna, R. (2013). Feature: Data breaches: the enemy within. *Computer Fraud & Security, 2013*, 8-11. doi: 10.1016/S1361-3723(13)70071-X

LeVeque, V. (2006). *Information Security: A Strategic Approach*: Wiley.

Lumension.com, (2014).BYOD & Mobile security - How to respond to security risks, https://www.lumension.com/more-info/BYOD-and-Mobile-Security.aspx, (Hämtat: 4 April 2014) [Elektronisk]

Micrographics & optical Technology. (2011). *International Journal of Micrographics & Optical Technology, 29*(4/5), 1-1.

Reyes, C. (2005). What makes a good security policy and why is one necessary?

Šedivá, Z. (2013). Mobile Policy in Enterprise Information System. *Systémová Integrace, 20*(3), 109.

Sheikhpour, R., & Modiri, N. (2012). A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management. *Indian Journal of Science and Technology, 5*(2), 2170-2176.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2009). Are Employees Putting Your Company At Risk By Not Following Information Security Policies? *Communications of the ACM, 52*(12), 145-147.

Smith, K. J., & Forman, S. (2013). Bring Your Own Device-Challenges and Solutions for the Mobile Workplace. *Employment Relations Today (Wiley), 40*(4), 67-73. doi: 10.1002/ert.21436

Souppaya, M., & Scarfone, K. (2013). Guidelines for Managing the Security of Mobile Devices in the Enterprise. (National Institute of Standards and Technology Special Publication 800-124 Revision 1), 29.

Stigviewer.com, (2014). stigviewer.com - Mobile OS devices, http://www.stigviewer.com/check/V-30567,
(Hämtat: 3 April 2014) [Elektronisk]

Suby, M. (2013). The 2013 (ISC)2 Global Information Security Workforce Study. Frost & Sullivan.

Trendmicro.com,(2012). Key strategies to capture and measure the value of consumerization of IT, http://www.trendmicro.com/cloud-content/us/pdfs/business/whitepapers/wp_forrester_measure-value-of-consumerization.pdf,
(Hämtat: 3 Maj 2014) [Elektronisk]

Whitman, M., & Mattord, H. (2013). *Management of Information Security*: Cengage Learning.

Vishal, G., Deepak, S., & Lovekesh, D. (2013). An Approach to Implement Bring Your Own Device (BYOD) Securely. *International Journal of Engineering Innovations and Research*(2), 154.

Zheng, P., & Ni, L. M. (2005). *Smart Phone and Next Generation Mobile Computing [Elektronisk resurs]*: Burlington : Morgan Kaufmann 2005.