

Högskolan i Halmstad
Sektionen för Informationsvetenskap, Data och Elektroteknik
Valfritt Informatik Program

Den mänskliga faktorn som säkerhetsrisk vid mobilt arbete

Uppsats i Informatik, 10p
Slutseminarium 2007-05-30

Författare:

Dennis Möller
Axel Nordin-Svensson

Handledare:

Michel Thomsen

Abstrakt

Den här uppsatsen belyser hur den mänskliga faktorn påverkar säkerheten vid mobilt arbete och ger förslag på åtgärder för att öka säkerheten inom mobilt arbete. Vi har genom litteraturstudie och kvalitativ undersökning studerat hur den mänskliga faktorn påverkar säkerheten inom mobilt arbete. Många av de säkerhetsproblem som identifierats inom mobilt arbete är inte specifika för området utan har sitt ursprung i traditionell IT-säkerhet. Det största problemet är användarna, inte tekniken de använder sig av. Även de nya problem som uppkommit inom mobilt arbete är kopplat till användarna.

Vår undersökning visar att användare inte har tillräcklig medvetenhet inom säkerhet och att det krävs bättre utbildning på användarnivå för att kunna arbeta mobilt på ett säkert sätt.

1. INLEDNING	4
1.1 BAKGRUND	4
1.2 PROBLEM	5
1.3 SYFTE.....	5
1.4 MÅLGRUPP.....	5
1.5 AVGRÄNSNINGAR.....	6
2. TEORI.....	7
2.1 INFORMATIONSSÄKERHET	7
2.2 MOBILT ARBETE.....	8
2.3 RISKER OCH HOT INOM MOBILT ARBETE.....	9
2.4 ANSVAR FÖR PLANERING OCH UPPDATERING AV SÄKERHET	10
2.5 POLICY SOM SÄKERHETSSKYDD	11
2.6 DEN MÄNSKLIGA FAKTORN SOM SÄKERHETSRIK	12
3. METOD	15
3.1 ANGREPPSSÄTT	15
3.2 LITTERATURÖVERSIKT	15
3.3 SÖKMETOD.....	15
3.4 UNDERSÖKNINGSMETOD	16
3.5 RIMLIGHET OCH TROVÄRDIGHET.....	16
3.6 URVAL AV INTERVJUPERSONER.....	17
3.7 INTERVJUTEKNIK.....	18
3.8 KONSTRUKTION AV INTERVJUFRÅGOR	18
3.9 ANALYSMETOD	19
3.10 METODDISKUSSION	19
4. EMPIRI.....	21
4.1 PRESENTATION AV INTERVJUPERSONER	21
4.2 MOBILT ARBETE.....	21
4.3 RISKER OCH HOT INOM MOBILT ARBETE.....	22
4.4 ANSVAR FÖR PLANERING OCH UPPDATERING AV SÄKERHET	23
4.5 POLICY SOM SÄKERHETSSKYDD	25
4.6 DEN MÄNSKLIGA FAKTORN SOM SÄKERHETSRIK	25
5. ANALYS	28
5.1 MOBILT ARBETE.....	28
5.2 RISKER OCH HOT INOM MOBILT ARBETE.....	28
5.3 ANSVAR FÖR PLANERING OCH UPPDATERING AV SÄKERHET	29
5.4 POLICY SOM SÄKERHETSSKYDD	29
5.5 DEN MÄNSKLIGA FAKTORN SOM SÄKERHETSRIK	30
6. DISKUSSION.....	32
6.1 FÖRSLAG TILL FORTSATT FORSKNING.....	33
7. SLUTSATS	34
8. REFERENSER.....	35
TABELL 2:1 SÄKERHETSLAGER ENLIGT WHITMAN & MATTORD (2005).....	7
TABELL 3:1 TEMATISERING AV INTERVJUFRÅGOR.....	19
FIGUR 2:2 ATTITYDKARTA (THOMSON & SOLMS, 1998)	13
FIGUR 4:1 VARIABLER I SÄKERHETSARBETET.....	24
BILAGOR.....	38
BILAGA 1: FÖRFRÅGAN TILL INTERVJUPERSONER.....	38
BILAGA 2: INTERVJUFRÅGOR	39

1. Inledning

I detta kapitel presenterar vi bakgrunden till de problem vi identifierat samt presenterar den problemformulering och de syften denna uppsats grundar sig på. Vi redogör också för de avgränsningar och definitioner som gäller för uppsatsen samt målgruppen den riktar sig till.

1.1 Bakgrund

Den tekniska utvecklingen ökar ständigt möjligheterna för företag att låta de anställda utföra sitt arbete i stort sett oavsett geografisk position. Mobila enheter bidrar till att anställda flexibelt kan utföra arbetsuppgifter på ett likartat sätt som på det fysiska kontoret. Det finns dock frågetecken som behöver redas ut innan det sker en omfattande spridning av mobilt arbete.

Mobilt arbete ses idag som ett sätt att skära ner kostnader för organisationer genom bland annat minskat antal kontor. För de anställda kan mobilt arbete innebära ökad produktivitet, större möjligheter att planera sin tid, minskade pendlingskostnader och mindre restid. Informationsteknologin har inte bara förenklat utvecklingen av mobilt arbete, utan också gjort det effektivare och lättare att handskas med (Sturgeon, 1996). Datorer, mobiltelefoner, Internet och e-mail är exempel på teknik som gör det möjligt att arbeta mobilt (Kelly & Locke, 1999).

Enligt en undersökning från 2006 kommer det att bli ett omfattande generationsskifte i många företag då 40-talisterna går i pension. Förutom att ett stort antal tjänster kommer att ersättas av en ny generation kommer det även att innebära en ökad efterfrågan på mobilt arbete. Mer än 50 procent av företagen i undersökningen anser att portaler, mobiltelefoner och bärbara datorer blir allt viktigare arbetsredskap [1]. Generationsskiftet kommer med mobila enheter att möjliggöra en ny syn på det traditionella kontoret. Detta bidrar till att den geografiska friheten ökar och de anställda inte längre är lika bundna till det fysiska kontoret.

Datorsystem och applikationer är skapade för människan, inte tvärtom. Därför måste utmaningen ligga i att engagera användarna att skapa och upprätthålla en hög säkerhetsnivå. Det räcker inte med policys och hårdvara för att upprätthålla en hög säkerhet eftersom dessa enheter är statiska. Människan däremot handlar innovativt och emotionellt i nya situationer och anpassar sig till den verklighet som råder. På samma sätt som hårdvara inte kommer att följa de regler den inte förstår så kommer människan inte att följa de regler de inte tror på. En viktig del för att förstärka säkerheten är att utbilda användarna (Tipton & Krause, 2003).

Mobila enheter är ofta konfigurerade för att ge anställda åtkomst till företagets information och kräver högre säkerhet än de system som befinner sig i företagets byggnader (Whitman & Mattord, 2005). Detta ställer i sin tur högre krav på de som arbetar mobilt i företaget då de, enligt Clear och Lee-Kelley (2005), är den svagaste länken. 80-90% av alla säkerhetsrelaterade problem i organisationer kan härledas till den mänskliga faktorn vilket ger en ökad förståelse för den mänskliga faktorns påverkan avseende IT-säkerhet (Gonzales & Sawicka, 2002). Detta bekräftas också av Arce och Levy (2003) som skriver att datorbaserade säkerhetsapplikationer inte kan ersätta eventuella brister i organisationens säkerhetsstrategi vad gäller användarna.

Enligt Badamas (2001) får svårigheten med att säkra ett företags data en ny dimension i takt med att mängden av känslig information ökar till och från de mobila enheter som används utanför företaget. Vi har i vår förstudie identifierat problem kring mobilt arbete som vi anser

vara viktiga i säkerhetsarbetet. Ett säkerhetsproblem är att mobila enheter tappas bort. En förlorad enhet kan innebära att känslig information hamnar i fel händer vilket är ett allvarligt säkerhetsshot mot företaget (Walter et al., 2004). Ett annat problem är att många företag idag saknar säkerhetsrutiner för säkert användande av mobila enheter [2]. Hur framgångsrika företagen blir i att hantera säkerhet avgörs av hur väl förberedda de är att hantera de risker och hot som finns. En undersökning gjord av Economist Intelligence Unit visar att det finns brister i säkerheten för företags mobila enheter. Undersökningen visar också att många företag väntar med införandet av mobilt arbete på grund av säkerhetsriskerna [3].

Vi har utifrån litteraturen och branschtidningar blivit nyfikna på säkerhet inom mobilt arbete med fokus på den mänskliga faktorn. Vi har fördjupat oss i ämnet genom att studera forskningsartiklar som behandlar säkerhet för mobilt arbete och informationssäkerhet där en del är den mänskliga faktorn. Med den mänskliga faktorn som säkerhetsrisk avses säkerhetsproblem som kan härledas till människors beteende vid mobilt arbete och hantering av enheter och information. Litteraturgenomgången indikerar på att det inte finns en enhetlig bild av hur dessa områden tillsammans kan underlätta ett säkert införande av mobilt arbete. Många av de artiklar vi studerat lägger större fokus på tekniken bakom säkerheten än den mjuka aspekten som vi vill lyfta fram (Kim, Kim, Lee & Choi, 2005; Nayak, Rajendran, Phatak & Gulati, 2004; Scheuermann, 2002). Även om den tekniska utvecklingen underlättar och ökar det mobila arbetets tillväxt så kommer det att ställas högre säkerhetskrav på användarna. Tidningsartiklarna visar att området är aktuellt och påminner oss om att det finns ett ständigt behov av att identifiera nya säkerhetsrisker och lösningar för dessa.

När det gäller säkerhet kring användare har det forskats kring vikten av policys för organisationers informationssäkerhet (Patriciu & Bica, 2002), verktyg för hantering och klassificering av risker (Clear & Lee-Kelley, 2005) samt vikten av användares hantering av lösenord (Gehring, 2002).

1.2 Problem

Mobilt arbete växer i omfattning och det finns fortfarande brister i säkerheten. Verksamheter saknar rutiner för användning och skydd av mobila enheter (Brandel, 2007) vilket leder till att förlorade enheter blir en stor säkerhetsrisk [4]. Det är brist på medvetenhet i fråga om säkerhetsrisker (Kowalski & Swanson, 2005) vilket leder till att användare saknar kunskap i säker användning av mobila enheter (Dhamija, Tygar & Hearst, 2006).

Efter att ha studerat vetenskapliga artiklar inom området och jämfört dessa med problemen i tidningsartiklarna har vi fått bekräftat att den mänskliga faktorn påverkar säkerheten i mobilt arbete.

Hur kan IT-säkerhetsansvariga förstärka säkerheten för mobilt arbete utifrån den mänskliga faktorn som säkerhetsrisk?

1.3 Syfte

Vi vill undersöka och belysa den mänskliga faktorns betydelse för säkerhetsarbetet vid mobilt arbete. Vi vill även ge förslag på åtgärder som ett företags IT-säkerhetsansvariga kan tillämpa för att göra mobilt arbete säkrare.

1.4 Målgrupp

Vår undersökning riktar sig till IT-säkerhetsansvariga som har infört eller planerar att införa mobilt arbete.

1.5 Avgränsningar

Undersökningen fokuserar på användarna – ”den svagaste länken” och de IT-säkerhetsansvarigas åtgärder för att upprätthålla säkerheten vid mobilt arbete. Då människan står i centrum för vår undersökning kommer vi inte att behandla de tekniska problem och lösningar som finns inom säkerhetsområdet.

2. Teori

Detta kapitel innehåller resultatet av vår litteraturundersökning och är en teoretisk bakgrund till vårt problemområde. Här redogörs för de teman som vi identifierat - de faktorer som kretsar kring säkerhet inom mobilt arbete i organisationer. Dessa teman återkommer i hela uppsatsen.

2.1 Informationssäkerhet

Begreppet informationssäkerhet är en modernisering av datorsäkerhet. Säkerhet i sin ursprungliga form innebär att genom åtgärder minska sannolikheten för oönskade händelser eller att mildra konsekvenserna av dem (SIG Security). Behovet av datorsäkerhet uppkom under andra världskriget då stordatorerna förseddes med lager av säkerhet för att skydda den information som fanns på datorerna. Säkerhet på denna tiden bestod av fysiska nycklar och säkerhetsvakter. Det första kända säkerhetsproblemet som inte var av fysisk natur uppdagades i början av 1960-talet då en systemadministratör arbetade i en textfil samtidigt som en annan administratör editerade en lösenordsfil. Ett mjukvarufel blandade ihop de båda filerna och resultatet blev att lösenordsfilen skrevs i varje dokument (Whitman & Mattord, 2005). Enligt Whitman och Mattord (2005) består säkerhet av flera lager som organisationer måste tillgodose för att upprätthålla säkerheten. Dessa lager är fysisk säkerhet, personsäkerhet, kommunikationssäkerhet, nätverkssäkerhet och informationssäkerhet.

Lager	Innehåll
Fysisk säkerhet	Lås, vakter, övervakningskameror, ID-brickor och flera typer av larm. Syftar till att skydda organisationen från obehöriga.
Personsäkerhet	För att reducera mänskliga fel, stöld och bedrägeri genom exempelvis utbildning och policys.
Kommunikationssäkerhet	Skydda organisationens kommunikation med exempelvis kryptering.
Nätverkssäkerhet	Skydd av nätverkskomponenter och anslutningar som använder, lagrar och kommunicerar kritisk information.
Informationssäkerhet	Se nedan.

Tabell 2:1 Säkerhetslager enligt Whitman och Mattord (2005)

Informationssäkerhet är skydd av information och dess kritiska element vilket inkluderar de system och den hårdvara som använder, lagrar och överför informationen (Whitman & Mattord, 2005). Information är en tillgång som har ett värde för organisationer och behöver därför en anpassad säkerhet (Patriciu & Bica, 2002). Patriciu och Bica (2002) karakteriserar informationssäkerhet som bevarandet av konfidentialitet, integritet och tillgänglighet. Konfidentialitet uppnås när informationen är tillgänglig enbart av de som har behörighet till den. För att bevara informationen konfidentiell kan företag använda sig av informationsklassificering, säker dokumentförvaring, säkerhetspolicys och utbildning av användare. Informationens integritet avgörs i hur korrekt och fullständig den är. Integriteten hotas då informationens ursprungliga form modifieras av obehöriga personer. Tillgänglighet innebär att behöriga användare har tillgång till informationen när den behövs (Whitman & Mattord, 2005; Tipton & Krause, 2003).

Informationssäkerhet måste balansera skydd och tillgänglighet. Det är möjligt att öppna upp ett system så att alla har tillgång till det. Detta skulle dock innebära ett hot mot informationens integritet. Å andra sidan skulle fullständig informationssäkerhet av ett system

som inte tillåter någon access innebära ett hot mot tillgängligheten. Utmaningen ligger i att uppnå balans så att både användarna och säkerhetspersonalen känner sig nöjda. Säkerhetsnivån måste tillåta tillräcklig access samtidigt som systemet skyddas mot hot. I arbetet med att balansera tillgång och säkerhet är det viktigt att säkerhetspersonal och användare samarbetar och har förståelse för varandras synsätt. Säkerhetspersonalen anser att kryptering är nödvändigt för att skydda kritisk information medan användarna ser det som tidsödande och besvärligt att kryptera (Whitman & Mattord, 2005).

Informationssäkerhet involverar både teknologi och människor. Teknologiska framsteg förbättrar säkerhetsskyddet men det har blivit allt tydligare att den mänskliga faktorn är informationssäkerhetens akilleshäla (Gonzales & Sawicka, 2002). Att säkra informations-säkerheten är kritiskt vid mobilt arbete. Skyddet av informationssäkerheten ska motsvara de risker som finns inom mobilt arbete. Riskerna att arbeta i en oskyddad miljö ska beaktas och en lämplig säkerhet ska appliceras (Patriciu & Bica, 2002)

2.2 Mobilt arbete

Clear och Lee-Kelley (2005) använder termen *telework* och definierar begreppet som att arbeta utanför företaget. Detta kan vara hemma, hos en kund eller på resande fot. Carnahan och Guttman (1998) skriver om att arbeta utanför det fysiska kontoret som *telecommuting*.

Mobilt arbete ökar i omfattning och allt fler organisationer implementerar eller planerar att implementera. Detta medför att det blir nödvändigt att skapa riktlinjer för mobilt arbete. Det har ännu inte gjorts några studier eller rapporter med riktlinjer för mobilt arbete. För att vara konkurrenskraftig är implementering av mobilt arbete inte längre något val utan nödvändigt för de flesta organisationer (Kowalski & Swanson, 2005). Detta står dock i konflikt med Economist Intelligence Unit's [3] undersökning som visar att många företag väntar med att införa mobilt arbete då det anses finnas brister i säkerheten. Innan implementering av mobilt arbete sker är det viktigt att fundera om det överensstämmer med organisationens strategiska mål och konkurrensrioriteringar. Vidare bör organisationen analysera vilka fördelar mobilt arbete kan innebära (Harpaz, 2002).

Det finns många anledningar och fördelar för organisationer att arbeta mobilt. Det är inte bara organisationen som anses dra fördelar av mobilt arbete utan även de anställda. En stor fördel med mobilt arbete är den flexibilitet som erbjuds avseende plats och tid. Mobilt arbete gör det även möjligt för företag att anställa personal som inte bor i närheten av företagets fysiska kontor. Det ökar även företagets möjligheter att planera och schemalägga arbetet utifrån kundernas behov. Att arbeta mobilt har visat sig öka tillfredsställelsen bland de anställda. Ökad tillfredsställelse resulterar också i högre produktivitet, ökat samarbete, minskad frånvaro, minskad omsättning av personal och högre moral bland de anställda. Mobilt arbete innebär också en kostnadsminskning för organisationer, bland annat genom minskat behov av kontorsutrymmen (Manoochehri & Pinkerton, 2003). Walter et al. (2004) presenterar ett scenario om en mobilt arbetande säljare och vilka enheter denne använder i sitt dagliga arbete. För att läsa företagsmail använder säljaren sin mobiltelefon, för att planera kundbesök används en PDA och för att registrera en ny order använder säljaren en bärbar dator. Det finns även problem för organisationer som bedriver mobilt arbete. Då de anställda befinner sig på distans blir det svårare att kontrollera och påverka deras arbete samt att ingjuta motivation och engagemang. Att införa mobilt arbete kräver förändring av arbetsmetoder vilket innebär extra arbetsansträngningar och kostnader. Övervakning, rapportering och kommunikation blir svårare vid mobilt arbete. Att arbeta mobilt för den enskilda individen kan innebära att känslan av tillhörighet försämras. Enligt rapporter kan en känsla av isolering uppstå vid

mobilt arbete och användaren kan känna mindre tillhörighet då han besöker den fysiska arbetsplatsen. Förmågan att påverka andra människor och händelser i företaget försämras också. Detta blir mer påtagligt på människor som har ett starkt behov av social interaktion. Det är viktigt att individen som arbetar mobilt har självdisciplin då denne ofta får ett större ansvar för sitt eget schema. Brist på självdisciplin kan resultera dels i att den anställda arbetar för lite och dels i att den blir beroende av jobbet och inte vet när det är dags att sluta arbeta. Att arbeta mobilt innebär också att det blir svårare att tillgå professionell support när problem uppstår då denna vanligtvis finns på det fysiska kontoret (Harpaz, 2002).

För att få ut det bästa resultatet vid skapande av riktlinjer måste företag studera processerna, verktygen och tekniken som används, inte bara resultat och effekt av det mobila arbetet. Det är därför viktigt att inte bara titta på mättningsresultat som t.ex. produktivitet och kostnadsbesparingar, utan också undersöka själva processen för mobilt arbete. Eftersom området är relativt nytt och många organisationer saknar förståelse och medvetenhet, lär en del organisationer finna det svårt att identifiera stegen i början av implementeringsfasen för mobilt arbete (Kowalski & Swanson, 2005).

För att övertyga ledningen att införa mobilt arbete krävs det att de får kunskap om fördelarna med mobilt arbete. Detta har visat sig vara positivt vid införande av mobilt arbete i organisationer. IBM hade inte ledningens stöd vid införandet av mobilt arbete då rädslan var alltför stor. Det ansågs vara ett hinder vid införandet. IBM hanterade motståndet genom att involvera ledningen i utbildningen och erbjöd enkla redskap, tekniker och erfarenheter från mobilt arbete avseende tid- och jobbmanagement (Kowalski & Swanson, 2005).

2.3 Risker och hot inom mobilt arbete

Risker beskrivs som en negativ utkomst som har en känd förekomst eller beräknad chans att någonting kommer att inträffa baserat på erfarenheter eller teorier. Mobilt arbete orsakar utmaningar för säkerheten som är identiska med det konventionella kontoret men mobiliteten kan också innebära ytterligare risker. Förlorad eller förstörd information är en risk som ökar vid mobilt arbete. På kontoret anses datorer vara säkrare då informationen ofta filtreras genom en brandvägg innan den kommer in på nätverket (Clear & Lee-Kelley, 2005), på kontoret omges datorerna även av det fysiska skyddet (SIG Security, 1997). En annan risk med mobilt arbete enligt Whitman och Mattord (2005) är att obehöriga kan komma åt ett företags system utan att fysiskt vara i närheten av systemet. Detta kan ske genom *shoulder surfing* som innebär att obehöriga personer tillgodoser sig inloggningsuppgifter genom att läsa av tangentbord när uppgifterna matas in. Whitman och Mattord (2005) betonar vikten av att ha säkra anslutningar när arbete utförs mobilt. Med det ökade hotet mot bärbara datorer, mobiltelefoner och PDA's kräver mobilt arbete än mer säkerhet än de system som finns inom organisationers väggar. Många av dessa mobila enheter innehåller värdefull företagsdata och är konfigurerade för att underlätta åtkomst till organisationens system. Informationen är ofta fördelad på flera olika system och applikationer som kräver unika användarnamn och lösenord. Många användare utnyttjar därför bekvämligheten i att låta enheter komma ihåg användarnamn och lösenord eftersom det förenklar åtkomsten av information (Whitman & Mattord, 2005). Ett annat traditionellt exempel är användare som skriver sitt lösenord på en papperslapp och förvarar denna i närheten av datorn (Wood, 1997).

Stulna enheter är ett stort problem inom mobilt arbete då de är små, portabla och enkla att stjäla (Armstrong, Wynne & O'Shea, 2004). För att maximera en mobil enhets fysiska säkerhet ska den vara under besittning hela tiden, framför allt när användare befinner på offentliga platser (Whitman & Mattord, 2005). En användare som arbetar mobilt vet inte vilka

som är uppkopplade på det trådlösa nätet eller om någon har möjlighet att logga trafiken på den trådlösa anslutningen vilket innebär att trafik på nätverket registreras. Externa anslutningar innebär en potentiell risk för obehörig access till affärsinformation (Patriciu & Bica, 2002). Clear och Lee-Kelley (2005) skriver att virusangrepp är ett större hot vid mobilt arbete än i det fysiska kontoret eftersom nätverket ofta är försett med brandväggar och viruskontroller. Även om de mobila enheterna förses med anti-virusprogram är det svårt för företaget att försäkra sig om att medarbetarna uppdaterar programvaran och att de inte kör program som avaktiverar viruskontrollen.

De flesta företag har värdefull information som kontrolleras av människor som inte alltid är medvetna om informationens värde, vikten av att hantera dess skydd eller följderna om informationen kommer i fel händer. Människor begår misstag, de utför fel konfigurationer, öppnar skadliga filer, raderar fel filer och sprider information i tron om att de är hjälpsamma. Den mänskliga faktorn är orsaken till många säkerhetsincidenter (Orshesky, 2003). För att få människor att göra rätt krävs det planering och engagemang. Erfarenhet visar att det svåraste hotet mot informationssäkerheten finns inom den egna organisationen. Vanligt förekommande är fel, misstag och oavsiktligt slarv som en följd av brister i organisationen, exempelvis ansvarsfördelning eller kompetens- och kunskapsbrist. Mindre vanligt men ett desto farligare hot är avsiktliga internangrepp, kanske i konspiration med en eller flera personer inom eller utanför organisationen. Internangrepp kan uppstå utifrån missnöje över ett oväntat avsked, en utebliven förväntad löneförmån eller bristande lojalitet mot en arbetsgivare som betraktas som okänslig och anonym (SIG Security, 1997).

2.4 Ansvar för planering och uppdatering av säkerhet

Det finns flera olika sätt att placera ansvar för säkerhet. Informationssäkerhetsansvaret är ofta knutet till verksamhetsansvaret på olika nivåer. För att samordna informationssäkerhetsarbetet behövs det dock spetskompetens som ofta inte finns i de olika nivåerna. Ett första steg till ett aktivt säkerhetsarbete är att utse en person, informationssäkerhetschef eller liknande, som har huvudansvaret för samordningen av informationssäkerhetsarbetet. För att öka samordningen av säkerhetsarbetet är det lämpligt att informationssäkerhetschefen placeras som direkt underställd till den övergripande säkerhetschefen om sådan finns. Betydelsen av informationssäkerhet motiverar att den placeras direkt under verksamhetsledningen, tjänsten bör alltså inte placeras på IT-avdelningen. En av ledningens viktigaste uppgifter är att delegera samordningen av informationssäkerhetsarbetet till informationssäkerhetschefer eller motsvarande. Ledningen har dock fortfarande ansvaret att fatta de beslut som krävs på ledningsnivå. Exempel på beslut av dessa slag är fastställande av verksamhetens informationssäkerhetspolicy, beslut om hur säkerhetsarbetet ska utföras i det stora perspektivet och övergripande informationssäkerhetsbeslut (SIG Security, 1997).

En organisations säkerhetsavdelning måste ha tydligt definierade roller och en tydlig rapporteringsstruktur. Säkerhetsavdelningen ska rikta sitt fokus mot såväl anställda, kunder och leverantörer för att kunna ta hand om frågor och uppkomna hot. När en anställd tar emot ett e-mail som befaras vara infekterat av virus eller liknande ska han vara medveten om att det är ett ämne för säkerhetsavdelningen och inte börja informera sina kollegor på egen hand. Säkerhetschefen har ansvaret för utbildning och de anställdas medvetenhet så väl som att hålla sig uppdaterad om utvecklingen inom området avseende existerande hot och vilka åtgärder som finns att tillgå. Stora organisationer kan använda sig av en IT-kommité där varje affärsområde finns representerat för att diskutera och ta beslut om IT-satsningar (Tipton & Krause, 2003).

För att säkerhetsarbetet ska vara lyckosamt är det viktigt att de anställda tidigt involveras och aktivt deltar i ansträngningarna för att förbättra säkerheten. Säkerhetsansvar ska introduceras för användarna redan i anställningsfasen, inkluderas i kontrakt och kontrolleras under anställningstiden. Det är också viktigt att användare får nödvändig utbildning i gällande säkerhetspolicy, säkerhetskrav och regler samt utbildning i användningen av IT-resurserna innan han börjar anställningen. De anställda måste också ges möjlighet till fortlöpande utbildning under anställningstiden. Anställningskraven bör poängtera den anställdes ansvar avseende informationssäkerheten samt vilka åtgärder som tas om den anställde ignorerar säkerhetskraven. För att säkerställa att användarna är medvetna om hot mot informationssäkerheten och kan följa organisationens säkerhetspolicys i det vardagliga arbetet ska de utbildas i säkerhet och korrekt hantering av information. För att undvika brister i kontrollen av organisationens säkerhet bör anställdas förhållande till arbetsgivaren följas kontinuerligt, detta sker lämpligen genom personsamtal. Oavsett skälen till att en anställning upphör och oavsett uppsägningstidens längd bör den anställde omgående fräntas tilldelade behörigheter. Det kan också vara aktuellt att tilldela personen mindre känsliga arbetsuppgifter (SIG Security, 1997; Whitman & Mattord, 2005).

2.5 Policy som säkerhetsskydd

Ledningen bör vara medveten om säkerhetsskyddets betydelse. Detta innebär att det bör finnas ett övergripande dokument - en säkerhetspolicy - som återspeglar ledningens inriktning för säkerhetsskydd och informationssäkerhet. Säkerhetspolicy är ledningens direktiv för att skapa en skyddsnivå. En informationssäkerhetspolicy ska ha en anknytning till verksamheten och den eventuella IT-policy och IT-miljö som finns. Regelverken är det skelett som behövs för att veta vad som ur säkerhetssynpunkt gäller i verksamheten. En erfarenhet som ofta görs är att det är lättare att skriva reglerna än att praktiskt få den att fungera på ett sätt som inte upplevs som störande i arbetet (SIG Security). Organisationens policys är specifika element i arbetsmiljön som har direkt påverkan på de anställdas arbete. En organisation som värderar de anställdas produktivitet högt implementerar troligen policys som uppmuntrar till hög produktivitet där de anställdas arbete övervakas och belönas (Foote, Seipel, Johnson & Duffy, 2005). Det är viktigt att hålla säkerhetspolicyn uppdaterad eftersom det ständigt uppstår nya hot mot säkerheten. För att skydda företagets information bör målet vara att alltid försöka ha en policy som täcker in den existerande hotbilden (Danchev, 2003).

Fast många organisationer låter individen läsa policys som förklarar acceptabelt och oacceptabelt användande av datorutrustning fortsätter missbruket att växa. För att minska missbruk av en organisations informationssystem används skrivna policydokument som en hörnsten i säkerheten. Dessa förklarar vad som är rätt och fel användning av informationssystemen. Existensen av policys i en organisation garanterar dock inte att alla användare har läst dem. Även om de flesta säkert förstår att regler och begränsningar finns kan många vara obekanta med innebörden av policyn och dess regler och begränsningar. Många organisationer redogör policyn för sina anställda endast en gång och detta anses otillräckligt. Att en organisation har en policy innebär inte att policyn kommer att följas eller skötas av organisationen. För att minska kostnaderna och omfattningen av missbruk och datorbrott i dagens miljöer måste ledningen ständigt diskutera rätt och fel användande, åtgärder vid missbruk och moral med de anställda (Foltz, Cronan & Jones, 2005). Genom att involvera anställda i policyutveckling och uppdatering av policys ökar möjligheten att policyn blir begriplig. Människor som deltar i processen känner sig mer motiverade att följa den och uppmuntra andra att följa den än när de blir tilldelad en policy (Orshesky, 2003). Erfarenhet visar att utbildning och spridning av säkerhetspolicys ofta är en kritisk faktor vid införande av informationssäkerhet i en organisation (Patriciu & Bica, 2002).

Mobiliteten ökar i vårt samhälle och tilliten mellan anställda och organisation avtar, och sammanslagning och förvärv av nya företag fortsätter att registreras från och till. Att känna till allt om sitt företag kan för många anställda vara en avskräckande uppgift, särskilt på lägre nivå inom företaget. I en sådan miljö kan de anställda känna svårigheter att skapa något djupt engagemang till företaget. De förväntningar som policys skapar är beroende av förståelse för personalens motivation, eller den positiva eller negativa psykologiska kraft som påverkar deras beteende gentemot organisationens policys (Foote et al., 2005).

Att ha tillgång till konfidentiellt material utanför företagets byggnader orsakar en del säkerhetsproblem. På företaget är den anställda skyddad av företagets IT-infrastruktur. När företaget låter anställda arbeta mobilt försvinner detta skydd och nya utmaningar för säkerheten uppstår. Av denna anledning är det kritiskt för företag att instifta tydliga policys, procedurer och fortlöpande utbildningar som täcker säker hantering och kontroll av känslig information (Papmehl, 2001). En organisation måste försäkra sig om att de anställda är medvetna om de informationssäkerhetsrisker som föreligger samt se till att de anställda stödjer säkerhetspolicyn. Detta uppnås genom utbildning i hur de bör agera för att minimera säkerhetsrisker. Alla anställda bör få nödvändig utbildning och regelbunden uppdatering av policys och procedurer (Patriciu & Bica, 2002). Brandel (2007) skriver att många företag inte har upprättat någon mobilitetspolicy trots de många risker som är förknippat med mobilt arbete.

2.6 Den mänskliga faktorn som säkerhetsrisk

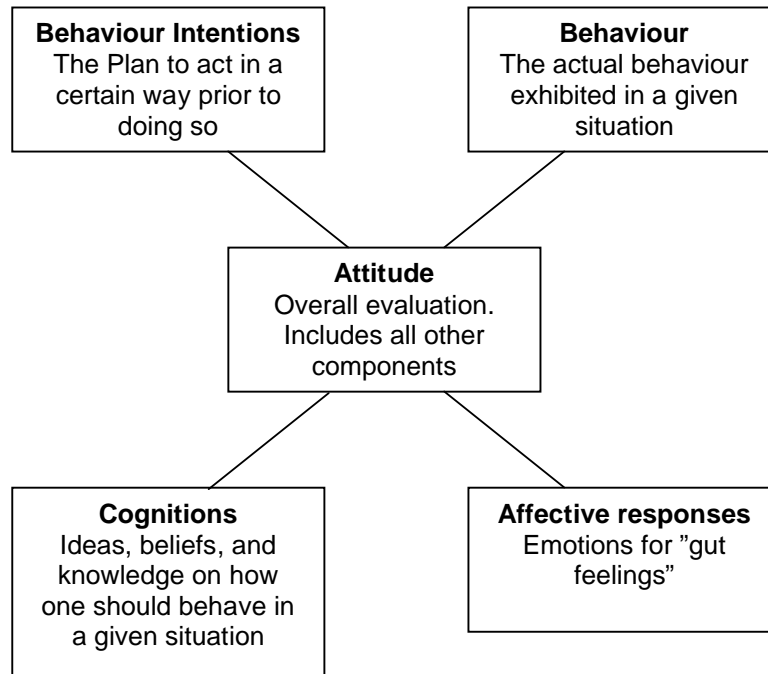
Vi nämnde i inledningen att användarna är den svagaste länken och att de är orsaken till 80-90% av alla säkerhetsrelaterade problem i organisationer (Gonzales & Sawicka, 2002). Även Clear och Lee-Kelley (2005) skriver att människan är den svagaste länken i kedjan, teknik kan anpassas medan mänsklig logik är svårare att hantera. Tipton och Krause (2003) skriver att människan även kan vara den starkaste tillgången i en organisations säkerhet. Datorer och policy har en tendens att vara statiska och begränsade medan människan handlar innovativt och emotionellt i nya situationer. På samma sätt som datorer inte kommer att utföra regler den inte förstår så kommer människor inte att ge stöd åt regler som de inte tror på. Enligt Orshesky (2003) ska teknik användas för att upprätthålla eller automatisera våra policys och processer, inte för att ersätta dem. Nyckeln för att förstärka effektiviteten inom säkerhet ligger i utbildning, flexibilitet, öppenhet och kontroll (Tipton & Krause, 2003).

Medvetenhet innebär utbildning och träning. Utbildning bör öka användarnas förståelse och svara på frågan ”varför”, medan träning skall öka användarnas färdighet inom området. Då ”varför” är väldigt viktigt, bör användarna inte nöja sig med svar som ”du behöver bara göra det”, ”så är reglerna”, ”det är vår policy”. På detta sätt ökar knappast användarnas motivation och attityd (Siponen, 2000).

Förändring av beteende och attityd genom utbildning

För att främja en säkerhetsmedveten företagskultur krävs det utbildning och medvetenhet om riskerna, hur de ser ut, var de kommer ifrån, hur vi exponeras och hur vi hanterar situationerna. Det är nödvändigt att förstå vilka åtgärder som finns om vi ska kunna reducera en risk (Orshesky, 2003). En människas attityd uppkommer som ett resultat utifrån dennes tidigare erfarenheter. Detta innebär att en anställds tidigare erfarenheter av policys har en betydelsefull roll i den anställdes nuvarande inställning till hur effektiv policyn är. Om de tidigare erfarenheterna är positiva kan det förväntas att den anställdes attityd mot policyn kommer att vara positiv även i framtiden (Foote et al., 2005).

Thomson och Solms (1998) skriver om effektiv utbildning av användare och fokuserar på deras attityd, beteende och medvetenhet inom säkerhetsområdet. Attitydkartan visar det typiska attitydsystemet som alla människor har. Attitydkartan hjälper till att förklara de faktorer som är avgörande för hur en person beter sig i en viss situation.



Figur 2:2 Attitydkarta (Thomson & Solms, 1998)

Centralt är den aktuella attityden vilken påverkas av ett antal andra faktorer:

- *Behaviour intentions* – Refererar till personens avsikter att bete sig på ett särskilt sätt vid en viss situation/visst tillstånd
- *Behaviour* – Det aktuella beteendet i en given situation, inte nödvändigtvis det samma som det avsiktliga sättet att bete sig i samma situation.
- *Cognitions* – detta hänvisar till en persons kunskap och övertygelse, om hur de ska bete sig i en viss situation.
- *Affective responses* – Dessa är som emotionella känslor som visas i en viss situation.

Figur 2:2 visar att faktorerna är relaterade och förändring i en av faktorerna kan påverka de andra. När det handlar om informationssäkerhet förväntas det att detta resulterar i en stor attitydförändring hos användarna. Det finns ett antal effektiva metoder som kan användas för att påverka en användares beteende:

Direkt ändra användarnas beteende

Denna metod syftar till att ändra användarnas beteende genom att ignorera deras tidigare kunskaper och attityder. Detta kan göras genom att belöning utdelas när personen visar det förväntade beteendet. De personer som belönas kan därigenom få sina kollegor att anta ett liknande beteende. Ett annat sätt är att skapa grupstryck, detta syftar till att få den grupp som antagit "rätt" beteende att försöka övertyga de som ännu inte visar "rätt" beteende. Lydnad för auktoriteter är ytterliggare ett tillvägagångssätt. Forskning har visat att det ofta är ofattbart hur långt människor är redo att gå för att lyda en ledargestalt (Thomson & Solms, 1998).

Förändra attityden genom att förändra beteendet

Detta syftar till att visa på hur olika sätt av omedvetna förändringar i beteendet kan leda till en förändrad attityd. Det är mer troligt att en attitydförändring också innebär en långsiktig förändring i beteendet. Detta kan göras genom att försöka få människor att skapa en anledning till att förändra sitt beteende genom exempelvis belöning. En annan teknik är att använda sig av rollspel för att försöka få personer att fränse sitt eget synsätt och därigenom komma på anledningar till att förändra sitt beteende (Thomson & Solms, 1998).

Förändra genom övertygelse

Denna metod består av några psykologiska tekniker som effektivt kan förändra attityder och beteenden hos personer. Det är viktigt att få personer att lyssna på budskapet. Budskap som inte stämmer överens med personens åsikt har en tendens att vara ointressant för mottagaren. För att behålla deltagarnas uppmärksamhet under en presentation hjälper det att regelbundet påminna deltagarna om att informationen är ny och användbar och att informationen inte skiljer sig så mycket från deras egen uppfattning. Vidare är det ingen mening med att ha deltagarnas uppmärksamhet om de inte förstår vad som presenteras. Mediet i sammanhanget är en kritisk faktor. Skriven media är mer effektiv när informationen är komplex då användaren på egen hand kan repetera och försäkra sig om att de har förstått budskapet. Är information mindre komplex är det mer effektivt att använda sig av enbart muntlig presentation. Det räcker inte med att uppnå deltagarnas uppmärksamhet och försäkra sig att de har förstått budskapet. Det är viktigt att individen accepterar budskapet för att uppnå en förändring i attityden. Budskapen som presenteras måste tåla granskning från deltagarna. Om deltagarna inte finner tvivel till budskapen blir det lättare att acceptera dem. Det är också viktigt att bibehålla rätt attityd. Detta kan göras genom att repetera viktig fakta under presentationen då detta ökar chanserna att deltagarna kommer ihåg det som presenterats (Thomson & Solms, 1998). Orshesky (2003) skriver att människor behöver kontinuerlig påminnelse för att handla ”rätt”. Påminnelser kan komma i flera former, exempelvis en säkerhetskolumn i företagets utskick, affischer som behandlar säkerhet och lunchmöte (*brown bag sessions*) för att diskutera nyligen inträffade incidenter. För att informationssäkerhet ska bli en del av företagskulturen måste den bli en del av våra dagliga aktiviteter.

3. Metod

Detta kapitel presenterar tillvägagångssättet i vår uppsats. Vi redogör här för våra metoder avseende litteraturinsamling, urval av intervjupersoner, konstruktion av intervjufrågor, intervjuteknik, undersökning samt analys av empirisk data. Vi avslutar detta kapitel med en metoddiskussion.

3.1 Angreppssätt

Det finns två övergripande sätt att bedriva forskning på. Det induktiva angreppssättet som är upptäckens väg och det deduktiva angreppssättet som är bevisandets väg (Holme & Solvang, 1997). Det induktiva angreppssättet bygger i stort på att observationer görs utan någon anknytning till teorin, ”från empiri till teori”. Deduktion bygger således på att befintlig teori är utgångspunkt för de empiriska studierna, ”från teori till empiri” (Johannessen & Tufte, 2003). Det deduktiva angreppssättet visar tydligare än det induktiva vilka konsekvenser som teorin leder till och om de överensstämmer med hypotesen. Holme och Solvang (1997) skriver att en kombination av dessa angreppssätt bidrar till ny, spännande kunskap. Vi kommer att använda oss av den deduktiva ansatsen som innebär att vi testar generella påståenden (teorier) med empiriska data. Teorin prövas med empiriska undersökningar och utifrån dessa kan vi stärka eller försvaga tilliten till teorin. Anledningen till att vi väljer den deduktiva ansatsen är att vi med semistrukturerade intervjuer vill testa hur den befintliga teorin är förankrad i verkligheten. Detta hade inte varit möjligt med den induktiva ansatsen då denna har sin utgångspunkt i empirin där insamlad data används för att hitta generella mönster som kan göras till teorier (Johannessen & Tufte, 2003).

3.2 Litteraturöversikt

Vi började vår studie med en litteraturöversikt som syftade till att visa medvetenhet om den tidigare forskning som redan har utförts inom området (Denscombe, 2000). Den hade också som syfte att identifiera de huvudsakliga problemområdena, de avgörande frågorna och de uppenbara luckorna i den nuvarande kunskapen inom området. Utifrån de sökningar som har gjorts har vi inhämtat den existerande kunskapen inom området. Utifrån denna teoretiska genomgång har vi identifierat vårt problemområde och preciserat vår problemformulering.

3.3 Sökmetod

Den teori som användes vid litteraturöversikten är hämtad från flera olika källor. Vi har använt oss av högskolebiblioteket i Halmstad där vi sökt böcker i databasen Hulda. Böcker och tidsskrifter innehåller den ackumulerade kunskap som forskningsprojektet bör bygga på (Denscombe, 2000). De vetenskapliga artiklarna är hämtade från databaserna IEEE, Emerald, ABI/Inform och Google Scholar. Vi använde följande sökord: *trustworthy computing, mobile work security, telework security, virtual office security, human factor security, telecommuting security*. Tidningsartiklarna som användes för att visa på ämnets aktualitet är till största del från Computer Sweden. Vi har kritiskt granskat all insamlad litteratur utifrån när de är utgivna och vem som har givit ut dem. Vi har i vissa fall, när det varit brist på alternativ, använt äldre litteratur. Denscombe (2000) skriver att tidsskrifter som har funnits länge är i regel användbara medan nyare tidsskrifter bör granskas mer kritiskt. Då vårt problemområde är i ständig utveckling har vi försökt hitta en balans mellan gammal och ny litteratur för att bevara trovärdigheten samtidigt som vi tvingats ta hänsyn till aktualiteten. Vetenskapliga artiklar som medverkat i konferenser anser vi vara pålitliga källor, detsamma gäller tidsskrifter och böcker som är utgivna av renommerade förlag och/eller myndigheter.

Resultatet av sökningen utgör den teoretiska referensram som finns presenterad i kapitel 2. Vi hittade många artiklar om mobilt arbete och säkerhet. Vi hittade inga artiklar som behandlar de risker som är förenat med den mänskliga faktorn inom mobilt arbete.

3.4 Undersökningsmetod

Det finns två typer av metoder, kvantitativ och kvalitativ ansats. I den kvantitativa ansatsen strävar forskaren efter att samla in numeriska data. Den kvalitativa ansatsen syftar till att omvandla det som rapporteras, registreras eller observeras till ord (Denscombe, 2000).

Vi valde att använda oss av den kvalitativa ansatsen. Utmaningen i denna ansats är att lyssna och se utan förutfattade meningar och att skriva ner detta utan att lägga till egna värderingar (Halvorsen, 1992). Intervjuer bör användas då forskaren tjänar på att erhålla material som ger mer djupgående insikt i ämnet (Denscombe, 2000). Utifrån detta valde vi att använda oss av intervjuer i vår undersökning. Anledningen till att vi inte valde enkätundersökning var att de kan innehålla många felkällor. Problemet med felkällor kan uppstå då respondenterna svarar för snabbt för att bli färdiga eller att respondenten inte satt sig in tillräckligt i ämnet (Ryen, 2004). För att besvara vår frågeställning ansåg vi att det krävdes detaljerad information från ett antal personer som arbetar med IT-säkerhet för mobilt arbete. Denscombe (2000) skriver att det avgörande valet står mellan att samla ytlig information från ett stort antal människor (kvantitet) eller att samla djupare information från ett mindre antal människor (kvalitet). Intervjuer kan struktureras på olika sätt beroende på vad som efterfrågas av intervjun. Semistrukturerade intervjuer innebär att intervjuaren har en färdig lista med ämnen som ska behandlas och frågor som ska besvaras. Intervjuaren är flexibel vad gäller frågornas/ämnenas ordningsföljd till skillnad mot strukturerade intervjuer som kan liknas vid frågeformulär. Det är vid semistrukturerade intervjuer viktigt att låta respondenten utveckla sina tankar och idéer inom det ämne som intervjuaren tar upp. Ostrukturerade intervjuer går ut på att forskaren ska ingripa så lite som möjligt. Här handlar det om att introducera ett ämne för intervjuobjektet och låta denne utveckla och fullfölja sina tankegångar och idéer. Ostrukturerade intervjuer är ett bra sätt för att upptäcka saker i komplexa frågor och syftar till att "upptäcka" mer än att kontrollera vilket är fallet i strukturerade intervjuer.

"Det som skiljer strukturerade intervjuer från semistrukturerade och ostrukturerade intervjuer är i hur hög grad forskaren bestämmer svarens karaktär och den längd respondentens svar tillåts ha" (Denscombe, 2000, s.136).

Vår undersökning består av semistrukturerade intervjuer. Med dessa har vi fått en helhetsbild av området samtidigt som vi inriktat oss på vårt fokus som är den mänskliga faktorns påverkan på säkerhet. Genom de semistrukturerade intervjuerna anser vi att vi fått en datainsamling som är tillräcklig för att besvara vår problemställning.

3.5 Rimlighet och trovärdighet

Målet är att samla in empirisk data som är relevanta för den problemställning som gäller för forskningen (Halvorsen, 1992). För att uppnå hög rimlighet finns det ett antal kriterier som bör beaktas. För att kontrollera resultatens rimlighet kommer vi att följa de punkter som Denscombe (2000) presenterar.

- Undersökningsenheterna ska väljas ut på rimliga och tydligt redovisade grunder utifrån forskningens syfte. Vi har varit noggranna i vårt urval och efterfrågat intervjupersoner med kunskap och erfarenhet inom problemområdet mobilt arbete.

- Eventuella alternativa lösningar och förklaringar ska undersökas. Detta visar att forskaren inte valt första bästa förklaring utan kritiskt granskat konkurrerande teorier. Det gäller även att undersöka om det finns dolda problem i resultatet.

Det finns författare som påstår att företag väntar med att införa mobilt arbete på grund av säkerhetsriskerna men vi har även hittat författare som skriver att företag måste införa mobilt arbete för att kunna vara konkurrenskraftiga. Vi har valt att presentera motsägande teorier för att öka rimligheten i vår studie. Utifrån resultatet av våra intervjuer har vi tagit ställning till de motsägande teorierna.

- Resultat och slutsatser bör jämföras med existerande kunskaper inom området för att kontrollera huruvida de överensstämmer. De resultat vi fick fram från intervjuerna har jämförts med befintlig teori, detta presenteras i analyskapitlet.

Med trovärdighet menas hur säkra mätinstrumenten och mätmetoderna är i det som mäts, oavsett vad forskaren syftar till att mäta (Winter, 1985). Mätinstrumentets trovärdighet anger med vilken precision forskaren mäter. Att uppnå hög trovärdighet syftar till att mätningarna ska bli oförändrade så långt som möjligt om mätningen upprepas en andra gång eller om någon annan utför mätningen (Carlsson, 1991). Vi anser att vårt mätinstrument i form av ljudupptagning och anteckningar vid intervjuerna uppnår hög trovärdighet då dessa tillsammans kompletterar varandra och undviker att någon information går förlorad. För att öka trovärdigheten ytterligare har vi haft för avsikt att vara opartiska och försökt bortse från våra åsikter inom problemområdet.

3.6 Urval av intervjupersoner

Syftet med kvalitativa intervjuer är att öka informationsvärdet och skapa en grund för djupare och mer fullständiga uppfattningar om det som studeras. För att få så stort informationsinnehåll som möjligt bör forskaren försäkra sig om största möjliga variationsbredd i urvalet. Vidare ökar informationsinnehållet om urvalet består av intervjupersoner som har rikligt med kunskap om de företeelser som undersöks (Holme & Solvang, 1997). Intervjupersonen måste även ha något motiv och något skäl för sin medverkan (Carlsson, 1991).

Urvalet för kvalitativa intervjuer baseras i allmänhet på medvetna val snarare än slumpmässigt urval. De personer som ingår i urvalet väljs för att de har något speciellt att bidra med, har en unik inblick eller en särskild position. Urvalet av intervjupersoner bör även spegla vad forskaren har för inriktning i sitt arbete. Forskning som syftar till att skapa resultat som går att generalisera bör ha ett representativt urval medan djupare forskning bör innehålla intervjuobjekt som är nyckelpersoner inom forskningsområdet (Denscombe, 2000). Ryen (2004) skriver att kvalitativa intervjuer bör ha en viss variation så att forskningen inte endast täcker in "vanliga" fall. Denna variation kan bland annat uppnås genom att välja intervjupersoner ur företag med varierande branscher och storlek.

Vi skickade e-mail till potentiella intervjupersoner där vi presenterade oss och beskrev vårt problemområde samt syftet med intervjun (se bilaga 1). För att säkerställa utskicketets kvalitet fick vi materialet granskat av andra studenter. Genom Dataföreningen fick vi kontakt med IT-säkerhetsansvariga på svenska företag som är stora aktörer på marknaden. Utöver intervjupersonerna från Dataföreningen kontaktade vi även ett företag i Halmstad.

Vi har genomfört tre djupare och längre intervjuer. Genom att följa upp intervjupersonernas svar och ställa relevanta följdfrågor resulterade intervjuerna i ett mer djupgående material.

Varje intervju pågick ca 60-80 minuter. Den första intervjun genomfördes med VDn på ett IT-företag. Den andra intervjun genomfördes med en säkerhetschef på ett stort energibolag. Den tredje intervjun genomfördes med en säkerhetskonsult på ett etablerat konsultföretag. Intervjuerna koncentrerades kring de teman som varit grunden för undersökningen. Vi har strävat efter att få detaljerad och riklig information inom problemområdet. De olika personerna som vi intervjuat har unik inblick i området och en särskild position i företaget. Denna bredd har bidragit till ett empiriskt material som motsvarar stora delar av branschens syn på mobilt arbete. Då vi har gjort djupgående intervjuer med personer vars position i företagen kräver mycket kunskap inom området anser vi att antalet intervjupersoner är tillräckligt för vår undersökning.

3.7 Intervjuteknik

Utifrån Ryen's (2004) och Denscombe's (2000) rekommendationer har vi tillämpat vad som anses vara god intervjuteknik. För att vara säkra på att få med allt från intervjuerna använde vi oss av ljudupptagning och anteckningar. Även om ljudupptagningen är ett mycket bra sätt att samla in data på, så är anteckningarna fortfarande viktiga då utrustningen kan krångla och materialet bli oanvändbart. Vi har varit medvetna om att intervjupersoner kan känna sig obekväma med teknisk utrustning vid intervjuer och tagit hänsyn till detta genom att fråga om tillstånd för ljudupptagning vid varje intervjutillfälle. Holme och Solvang (1997) skriver om vikten av att vi som intervjuare måste förstå och följa upp de problemområden som den intervjuade berättar om för att komma åt intressanta och viktiga fakta. För att kunna utveckla respondenternas svar har vi i våra semistrukturerade intervjuer gett utrymme för följdfrågor, detta gav oss ett detaljrikt material. Holme och Solvang (1997) skriver om vikten att notera icke-verbala reaktioner såsom kroppsspråk för att få ut så mycket som möjligt av intervjun. Genom att följa upp kommande frågor med det som intervjuobjektet svarat på tidigare frågor skapas en stämning där den intervjuade känner att forskaren lyssnar till denne vilket skapar en relation som präglas av tillit. Detta gör intervjun meningsfull för båda parter (Holme & Solvang, 1997).

3.8 Konstruktion av intervjufrågor

Vi har använt rubrikerna i teorin som tema vid konstruktion av intervjufrågor då dessa återspeglar vårt problemområde. Undantaget är "2.1 Informationssäkerhet" som är en inledande bakgrund till säkerhetsområdet. Varje intervjufråga motiveras med teori samt vad den tillför vår undersökning. Fullständig frågekonstruktion presenteras i bilaga 2. Följande frågor är exempel ur frågekonstruktionen:

- **10. Vilka säkerhetsproblem har ert företag stött på kring användarna vid mobilt arbete och hur hanterar ni dessa?**

Motivering: De förväntningar som policys skapar är beroende av att förståelse för personalens motivation, eller den positiva eller negativa psykologiska kraft som påverkar deras beteende gentemot organisationens policys (Foote et al., 2005) (kap 2.4.1). Vi vill identifiera vilka problem som är aktuella hos företagen som vi intervjuar. Detta för att få en tydligare bild av det existerande problemområdet.

- **15. Vi anser att användarna är en säkerhetsrisk. Tror du att det är så och i så fall varför?**

Motivering: Enligt Clear och Lee-Kelley (2005), är användarna den svagaste länken och utgör 80-90% av alla säkerhetsrelaterade problem i organisationer (kap 2.5). Vi undrar här på vilket sätt användarna är en risk för säkerheten.

Vi har konstruerat både inledande och uppföljande frågor. De inledande frågorna syftar till att säkerställa att intervjupersonerna är insatta i ämnet och har den kompetens som vi efterfrågar. De uppföljande frågorna används för att gå djupare in på området. Tabell 3.1 visar utifrån vilket tema/teoriområde frågorna är skapade.

Tema / Teoriområde	Tillhörande frågor
Informationssäkerhet	11
Mobilt arbete	3, 5, 7, 12
Risker och hot inom mobilt arbete	4, 14
Ansvar för planering och uppdatering av säkerhet	5.2
Policy som säkerhetsskydd	5.1, 9.1, 10, 13
Den mänskliga faktorn som säkerhetsrisk	8, 9, 9.2, 15

Tabell 3:1 Tematisering av intervjufrågor

3.9 Analysmetod

Vi analyserade vårt empiriska material med inspiration från Denscombe's (2000) *analytisk kodning*. Detta innebär att bryta ner data till analysenheter samt att kategorisera enheterna. Enheter kan vara speciella ord, idéer eller företeelser i datamaterialet (Denscombe, 2000). Vi har brutit ner materialet till analysenheter genom att identifiera nyckelord utifrån våra teman. Dessa nyckelord har därefter kategoriserats till våra teman.

Följande steg genomfördes i analysen:

1. Överföra ljudinspelning till textbaserad data
2. Tematisering av intervjumaterialet
3. Analytisk kodning

Det första steget i analysen var att överföra samtliga intervjuers ljudupptagningar till textbaserad data. Detta gjorde vi genom att ordagrant skriva ner de relevanta delarna av ljudupptagningarna från varje intervju samtidigt som vi validerade detta med anteckningar från intervjuerna. Då våra intervjufrågor redan var tematiserade utifrån vår teoretiska referensram placerades svaren under respektive tema. Efter tematiseringen gjorde vi analytisk kodning genom att identifiera nyckelord utifrån de teman som vi identifierat. Detta gjorde vi eftersom intervjupersonernas svar på frågorna ibland förekom i svaren under andra frågor. Detta gav oss en bättre översikt när vi skulle identifiera samband och motsättningar i materialet. Detta bidrog också till att våra olika teman endast innehåller relevanta svar.

3.10 Metoddiskussion

Den kvalitativa forskningsansatsen visade sig vara rätt för vår undersökning då vi fick djupgående information från ett antal intervjupersoner. Detta var av stor vikt för att skapa en detaljerad bild av problemområdet. Undersökningsprocessen startade då vi skickade ut intresseansökningar via e-mail till ett antal potentiella respondenter sett utifrån vårt problemområde (bilaga 1). De som svarade visade stort intresse i att delta i vår undersökning. Efter att datum och tid bokats träffades vi på respondenternas arbetsplats. Vi tror att vi hade

ringat in området på ett bättre sätt om vi hade genomfört en pilotintervju. Genom en pilotintervju hade vi också haft möjlighet att utveckla intervjufrågorna i ett tidigare skede.

I litteraturstudien var vi fast beslutna om att nypublicerade källor var av vikt för vårt problemområde. Vid intervjuerna insåg vi att även äldre litteratur var givande för vår undersökning då vårt problemområde inte kretsar kring aktuell teknik utan kring den mänskliga faktorn. Intervjupersonerna visade genom sin erfarenhet och position prov på rätt kompetens och hade unik inblick i ämnet. De av intervjupersonerna som planerar för ”Informationssäkerhetsnätverket” i Dataföreningen ser vi som nyckelpersoner inom problemområdet. ”Informationssäkerhetsnätverket” verkar för att sprida kunskap inom IT-säkerhet och är en mötesplats för säkerhetsintresserade medlemmar i Dataföreningen [5]. Urvalet gav oss bred variation av företag med tanke på deras storlek och arbetsområde inom IT.

Det visade sig under intervjuerna att det var lättare att identifiera problem kring mobilt arbete vid samtal med konsulter då företagsansvariga inte är lika öppna om vilka säkerhetsproblem och brister som finns i deras verksamhet. Våra intervjufrågor kunde konstruerats på ett sätt som riktade sig mindre till intervjupersonens egna arbetsplats. I efterhand insåg vi att vi borde diskutera mer generellt kring området och rikta mindre fokus mot det enskilda företaget. Detta hade gett en mer generell syn på mobilt arbete. Att intervjua ett antal användare hade bidragit till större trovärdighet av undersökningen. Genom intervjuer med användare hade vi kunnat jämföra deras syn på säkerheten, skillnader och motsättningar i förhållande till de ansvariga.

4. Empiri

I detta kapitel presenterar vi de personer vi har intervjuat och här redovisas resultatet i fråga om intervjuer som genomförts i tematiserad form. Frågorna som används som underlag för intervjuerna återfinns i bilaga 2.

4.1 Presentation av intervjupersoner och verksamheter

För att skydda intervjupersonernas identitet har vi valt att använda fingerade namn för samtliga intervjupersoner.

Niklas är VD på Datahalland som levererar behovsanpassade IT-lösningar till organisationer. Företaget startades 1972 som servicebyrå. När IBM PC kom i början på 80-talet bildades det som är Datahalland idag. De började då sälja hårdvara, installerade, lagade och höll datorerna i drift. Datahalland har 35 anställda och har sin kundgrupp inom en timmes bilfärd från företaget. Företaget verkar inom affärsområdena systemintegration, applikationsutveckling, Internet/webbutveckling, utbildning och varuförsäljning. Datahalland har Microsoft Gold certifiering och kan idag lösa mer och mer med fjärrstyrning.

Hanna arbetar som CISO (Chief Information Security Officer) på EON Market Union Nordic som ingår i EON Group. EON Group är tyskägt och är världens största privatägda energibolag med ca 70000 anställda. EON tillverkar och distribuerar el. I Sverige finns ca 15-20 dotterbolag. Varje bolag har en informationssäkerhetsansvarig och en IT-säkerhetsansvarig, ibland är det samma person, ibland olika. Det beror på hur stort bolaget är. Hanna är även en av de personer som står bakom planeringen av Dataföreningens informationssäkerhetsnätverk.

Lisa arbetar som informationssäkerhetskonsult på CapGemini i Malmö. CapGemini har mer än 75 000 anställda över hela världen, varav cirka 1 300 i Sverige. Aktien är noterad på Parisbörsen. Lisa har varit konsult inom området sedan 1998. Från början var det mer fokus mot IT-säkerhet men det har övergått till att bli mer informationssäkerhet. Lisa är också en av de personer som står bakom planeringen av Dataföreningens informationssäkerhetsnätverk.

4.2 Mobilt arbete

Niklas (VD) ser mobilt arbete som när arbete utförs utanför fast uppkoppling på nätverket. Han berättade att han är lika uppkopplad med sin mobiltelefon som med sin dator och påstår att mobilitet är transparent, det finns ingen början och inget slut. Enligt Hanna (CISO) innebär mobilt arbete att användarna tar enheter eller information med sig utanför företagets skalskydd. Lisa har ett liknande synsätt och berättade att mobilt arbete är när anställda tar med sig information ut från företaget till oskyddade miljöer, hon tar flygplatser, hotellrum och bostaden som exempel. Niklas, Hanna och Lisa berättade att de vanligaste enheterna som används vid mobilt arbete är bärbara datorer, smartphones och mobiltelefoner. Andra mobila enheter som framkom under intervjuerna var USB-minne och dosa som levererar engångslösenord. Niklas berättade att deras företag har arbetat mobilt i många år och anser att det har smugit sig på. Sedan 1,5-2 år tillbaka har de tagit greppet med ett större säkerhetsmässigt perspektiv då de har arbetat fram en säkerhetspolicy och en IT-säkerhetspolicy.

”Ska vi ligga i framkant när vi jobbar med våra kunder så måste vi själv arbeta med det” (Niklas)

Detta var en trigger till att börja arbeta mobilt. Niklas tror att användarna har en positiv inställning till mobilt arbete och påstod att de snarare vill ha mobil utrustning för att kunna vara mobila.

Hanna har arbetat på EON i 5 år och berättar att de bedrev mobilt arbete redan innan hon började arbeta på företaget. Anledningen till att företaget började arbeta mobilt tror Hanna är en kombination av att yngre personal tillträder, avståndet till arbetsplatsen växer och det är fler arbetsrelaterade resor idag än det var förr. Vad gäller företagets serviceenhet så var de tvingade till att börja arbeta mobilt eftersom kunderna finns där ute. Det finns inga begränsningar i vilka som får tillgång till de mobila enheterna på företaget. Hanna tror att användarna tycker det är väldigt bekvämt och är positiva till att arbeta mobilt. Hanna tror också att de anställda tycker det är positivt att kunna göra sitt jobb från olika ställen och anser att det känns som en frihet för de anställda att kunna välja var och när de vill jobba.

Lisa (konsult) förklarar att det inte finns några mobillösa konsulter och att hennes företag har arbetat mobilt i många år.

”Det ligger i affärsidén att man ska vara mobil” (Lisa)

Enligt Lisa tänker den anställda inte på att den arbetar mobilt eftersom det är så vanligt idag.

4.3 Risker och hot inom mobilt arbete

Intervjupersonerna är överens om att det finns risker och hot inom mobilt arbete. Några exempel på risker som Niklas (VD) tog upp var stöldrisken av mobila enheter, vikten av att stänga av alla konton och byta lösenord när en medarbetare slutar eller går till en konkurrent samt att bevaka dennes mailbox för att undvika förlorad företagsinformation. Det är också viktigt att samla in den anställdes enheter. Ett annat problem är det som sitter i huvudet på den anställda, det går inte att radera den mänskliga hårddisken.

Lisa (konsult) berättade om stulna och borttappade enheter som en risk och anser att det därmed hela tiden finns en risk vid mobilt arbete. Även om enheten tappas bort eller blir stulen ska den inte kunna tömmas på information, därför används hårddiskkryptering. Stöldbenägenheten minskar när enheten är försedd med hårddiskkryptering då den med detta skydd är obrukbar. Enligt Lisa är virus kopplat till mobilt arbete det största problemet för företag då virusen ofta bärs in via USB eller bärbara datorer, de kommer inte via företagets nät eller e-mail. Lisa anser att virus är jättefarligt och kostar jättemycket. Hon berättade vidare om risken med att anställda ser företagsdatorn som sin privata. Detta skapar problem då anställda tar hem datorn på kvällen och fildelar, installerar applikationer och låter barnen spela nätverksspel. Det är viktigt att poängtera att det faktiskt är företagets dator. Hanna (CISO) har stött på problem med medarbetare som försöker ta sig förbi brandväggar för att tillgodose sig fler rättigheter än vad de är berättigade till.

Det finns många anledningar till att företag väntar med att införa mobilt arbete. Niklas hävdar att företag väntar med införandet på grund av rädsla för tekniken då teknikutvecklingen är intensiv. Han anser att de som väntar saknar kunskap om vilka säkerhetslösningar som finns och därför är rädda för att bära runt på känslig information med tanke på stöldrisken av både enhet och information. De tror inte det finns några säkra system och hittar därför inte den rätta lösningen.

Anledningen till att företag inte vågar införa mobilt arbete är att de inte säkrar upp det tillräckligt mycket, enligt Hanna. Hon berättade att företag måste satsa på tekniska lösningar för att uppnå god säkerhet vilket är dyrt. Detta ska inte ses som ett hinder då säkerhet är som en försäkring för företaget.

”Man försäkrar sig i övrigt och då betalar man också pengar för ingenting om man säger så” (Hanna)

Hon anser att mindre företag inte känner till vilka möjligheter som finns då de inte riktigt förstår vad de är utsatta för.

Enligt Lisa har alla företag mobilitet på ett eller annat sätt, hon berättade att vi har passerat stadiet där företag har möjlighet att välja om de vill arbeta mobilt eller ej. Många företag har kommit så långt att det inte går att undvika det och företag klarar till viss del inte sig utan mobilt arbete. Lisa påstår att företag börjar arbeta mobilt utan att vara medvetna om att de därmed skapar säkerhetsproblem. Det är inte förrän säkerhetsproblem uppstår som företag börjar ta tag i säkerheten.

Huruvida nyttan med mobilt arbete är tillräcklig med tanke på säkerhetsriskerna berättade Niklas att det inte är en ekonomisk kalkyl som går att göra.

”Det är nytta med mobilt arbete men jag kan inte leda den i bevis med några tal” (Niklas)

Lisa påstår att eftersom säkerhet kostar är det svårare för mindre företag att upprätthålla säkerheten för mobilt arbete. Med tanke på de höga kostnaderna berättade även Hanna att det är svårt för mindre företag att motivera nyttan med mobilt arbete och de säkerhetsprodukter som måste investeras för att inte utsätta sig för riskerna som mobilt arbete innebär.

4.4 Ansvar för planering och uppdatering av säkerhet

Vad gäller planeringen vid införandet av mobilt arbete berättade Niklas (VD) att de kanske förutsätter att de hanterat planeringen på ett bra sätt eftersom dem själv arbetar med det. På frågan om de planerade och hur de planerade vid införandet fick vi svaret:

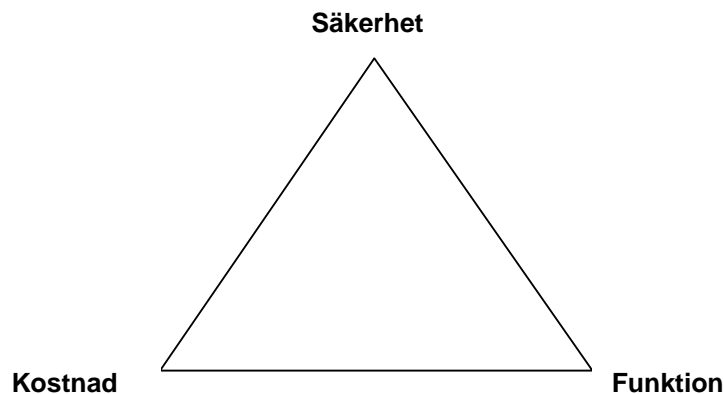
”Delvis har vi kanske, jag vet inte, det måste vi ta reda på. Vi förutsätter kanske eftersom vi jobbar med det här att vi hanterat det på ett bra sätt. Det tror jag man gör ganska långt” (Niklas)

Hannas (CISO) företag har vid planeringen av införandet av mobilt arbete ersatt det fysiska skyddet med tekniska lösningar för de mobila enheterna för att upprätthålla den skydds nivå som fysiskt motsvaras av väggar och lås. Dessa tekniska lösningar är väldigt kostsamma och används oftast av större företag. Genom att implementera tekniska lösningar såsom hårddiskkryptering blir enheterna också mindre stöldbegärliga.

”När man tar ut datorn så fattas skalskyddet, då måste vi ersätta det med något annat skydd” (Hanna)

Lisa (konsult) påpekar att målsättningen vid planeringen av säkerheten är att få den så transparent som möjligt. Allra helst ska användaren inte kunna göra fel och ska inte behöva bry sig om säkerhetsskyddet, det ska bara finnas. Då har vi lyckats. Tyvärr är verkligheten

inte så. Lisa presenterade en modell (figur 4:1) som behandlar tre viktiga variabler i säkerhetsarbetet.



Figur 4:1 Variabler i säkerhetsarbetet

Hon påstår att det endast går att kombinera två av variablerna och berättade att:

- Du kan få hög säkerhet och hög funktionalitet, då ökar kostnaderna.
- Du kan få hög funktionalitet till låg kostnad, då försämras säkerheten.
- Du kan få hög säkerhet till låg kostnad, då minskar funktionaliteten.

”När projektgrupper gör sin projektplan så tar de inte med toppen på triangeln, de lägger fokus på kostnad och funktion men glömmar säkerheten” (Lisa)

Hanna berättade att normalt sett placeras säkerhetschefen under IT-chefen. Hannas chef är medlem i koncernledningen vilket tyder på att hon som säkerhetschef har stort inflytande, detta visar på hur viktig säkerheten är. Hanna berättade att de även har en kommitté som består av en representant från varje affärsområde, ett tiotal personer, där de tar beslut om vad som ska göras inom säkerhetsområdet. De har även en grupp som arbetar med *risk management* och gör riskanalyser för de system som används.

Lisa berättade att de på CapGemini har en kontorschef som också är säkerhetsansvarig för kontoret. Nationellt har de en fysisk och en logisk säkerhetschef men hon vet inte om de har något folk under sig. Hon berättade att informationshantering och informationsklassificering ligger på individen, den som skapar eller tar emot information skall klassificera det. Säkerhetsavdelningen har inte möjlighet att klassificera allt.

Niklas berättar att han tillsammans med styrelsen en gång om året redogör för hur dem bedriver sitt säkerhetsarbete, hur de arbetar med att analysera och bedöma risker. Om riskerna bedöms som allvarliga tar de också upp hur de ska förhindra dem. Det kan vara allt från brand, inbrott och strömavbrott. Internt har de två personer som sköter säkerheten, de träffar Niklas kontinuerligt för att diskutera situationen. Han berättade att bara för att de är ett IT-företag kan de inte känna att allt är frid och fröjd, de kan aldrig slappna av med säkerhetsbiten.

”Det är viktigt att få in säkerheten som en naturlig del, det är inte något som ska ske en gång om året, det ska finnas dagligen.”

Hanna berättade att de uppdaterar och ser över säkerheten konstant och att de på EON har en avdelning som hanterar säkerhetsfrågor och som kan uppdatera policyn när nya hot identifieras. De har även samarbete med säkerhetsleverantörer som kan förse dem med uppdateringar när nya hot uppstår.

4.5 Policy som säkerhetsskydd

Samtliga företag som vi intervjuat har idag policys som behandlar mobilt arbete, dock har inte alla en separat policy för mobilt arbete. Inget av de intervjuade företagen hade policys som behandlade mobilitet innan år 2004. Lisa (konsult) hävdar att policybiten är relativt sen.

”För 5 år sedan pratade man inte om detta, det fanns inte och existerade inte på agendan. Informationssäkerhet kunde man knappt stava till och IT-säkerhet visste man att det fanns och att det behövdes...man har kanske haft något papper lite generellt som säger att vi ska ha en god säkerhet” (Lisa)

Det är absolut nödvändigt med policys för att kunna tala om för användare att de har gjort fel. Finns det inte specificerat vad de får göra och hur de ska göra kan de inte anklagas för att ha gjort fel. Det är dessutom ett lagkrav enligt PUL när det gäller exempelvis e-post och Internet. Använder företaget dessutom loggning eller surffilter måste det också stå i policyn. Användarna måste veta att det de gör på sina företagsdatorer kan bli loggat.

Hanna (CISO) berättade att de har skapat en särskild mobilpolicy för mobilt arbete. Detta har de gjort som ett steg för att uppnå ISO-standarden 17799-127 som är en internationell standard för IT-säkerhet. De har fastslagit att uppfylla standarden till 75% vilket de gör idag.

Niklas (VD) tror att de flesta företag idag arbetar med policys men att det ofta inte görs på ett strukturerat sätt. Är inte policyarbetet strukturerat så följs inte standarden, snarare blir det så att företagen går emot den. Han påstår att policyn i sig är inte det viktiga, det viktiga är att företagen lyckas efterleva den och berättar vidare att ett dokument är den enkla biten att skapa, det svåra är att följa den. Niklas tar lösenordshantering som exempel, ofta är det bara att titta runt på skrivbordet så finns lösenordet där. Det är många gånger det ser ut så.

”Vi har snart policy för allting. Bilpolicy, mobilpolicy, drogpolicy, jämställdhetspolicy, arbetsmiljöpolicy...det är snart ett skämt” (Niklas)

4.6 Den mänskliga faktorn som säkerhetsrisk

Hanna (CISO) är övertygad om att den mänskliga faktorn är en säkerhetsrisk och hävdar att användarna är för dåligt utbildade.

”De är för dåligt utbildade, de förstår inte. Så enkelt är det” (Hanna)

Niklas (VD) tror att användarna är en större säkerhetsrisk än tekniken och berättade att han har sett fruktansvärt många exempel på detta. Han tror att det beror på att de ansvariga inte jobbar tillräckligt med att få användarna att förstå säkerhetsproblem.

Hanna anser också att användaren är en större säkerhetsrisk än tekniken. Hon berättade att det gäller att försöka begränsa riskerna med hjälp av tekniska lösningar för att hindra användarna att göra fel när de arbetar mobilt. Hanna poängterar dock att det inte räcker med tekniska lösningar, det krävs även utbildning av användarna. Tekniken är en del av åtgärden men det är

inte den brinnande punkten för det är informationen. Detta åtgärdas genom utbildning. Det är viktigt att få nivån mellan utbildning och teknik att stämma överens så bra som möjligt.

Enligt Hanna kommer användarna inte att följa reglerna fullt ut oavsett utbildning. Allt som användarna lär sig är en tolkning utifrån deras egen referensram. Användarna har inte förståelsen och det är oavsett om de är 60 eller 22 år. Det är olika frågeställningar beroende på åldern. 22-åringen vet mycket väl vad man kan göra eftersom de är uppväxta med datorer. De chattar, använder skype och fildelar hemma. Med denna kunskap och erfarenhet försöker de med kreativa idéer att få tillgång till dessa funktioner även på jobbet vilket är en stor säkerhetsrisk. Även den äldre generationen utgör en risk, anser Hanna. De förstår inte att det som syns på skärmen inte finns i datorn, det är svårt att förklara att det finns ett nätverk. Lisa håller med om att åldern spelar roll i hur säkerhetsmedveten användaren är. De som är under 50 år har teknisk förståelse. Det är relativt vana användare som vet att det finns olika sätt att arbeta på.

Hanna tycker att det är för liten kunskap och för mycket godtrogenhet och tror att detta fenomen är väldigt svenskt. Hon hävdar att användarna är väldigt godtrogna och knappast tror att någon är intresserad av deras arbete. Om man som företag inte är beredd eller inte har pengar att satsa på tekniken måste de lita på användarna, det tror inte Hanna fungerar.

”Det där kommer aldrig att fungera. Inte för att de är oärliga utan det är för att de har olika referensramar” (Hanna)

Vidare berättar Hanna att om de inte hade satsat på tekniska lösningar hade användarna varit en ännu större säkerhetsrisk. Användarna tänker att det som inte kontrolleras är nog tillåtet. Det går inte att lita på det sunda förnuftet då det är olika från person till person. Användarna gör inte medvetet fel utan gör det av oförstånd. För att hjälpa användarna att göra så rätt som möjligt så måste vi använda de hjälpmedel som faktiskt finns.

”Det kan ju inte vara den enskilda människans ansvar att se till att vi har det säkert här” (Hanna)

Enligt Lisa (konsult) är användarna en säkerhetsrisk på grund av brist i medvetandet och på grund av bristande kunskap. Mobilt arbete innebär att företaget utsätter sig för en annan och högre risk. Användarna förstår inte vilka risker det faktiskt innebär att arbeta mobilt. Hon anser att policy och utbildning är bra men att de har sina begränsningar. De kan vara ett rättesnöre och kan kanske förhindra det mesta. Det finns dock fortfarande de som har läst men inte förstått dem, det finns de som inte har läst och det finns de som har läst och förstått men inte bryr sig. Sen finns det dem som vill göra en illa eller vill vara elaka, men det anser Lisa är en minoritet. Reglerna behövs, men de hjälper inte helt och hållet. För att täcka hela komplexiteten är det viktigt att integrera logiskt, administrativt och fysiskt skydd. Fysiskt skydd har funnits länge, exempelvis genom att låsa in saker. Det måste vi börja lära oss att göra logiskt också. Vi kan inte tro att hela världen och alla är ärliga och vill oss väl. Det är den blåögheten vi måste bort ifrån, enligt Lisa.

När det gäller att ha en öppen dialog med användarna om säkerhetsproblem som uppkommit tror Niklas att de har bra förhållande till sina användare, han tror att folk vågar träda fram och erkänna misstag och olyckor som har med säkerheten att göra.

”Jag skulle nog vilja tro men jag kan inte garantera, att det kommer fram”
(Niklas)

Hanna berättade att på EON är det aldrig användaren som blir anklagad när säkerhetsproblem uppstår, det är en dator som är med i någonting och det är datorn som beslagtas för att undersökas. Även om kontrollerna i företagets system identifierar ett säkerhetsproblem så ses inte användaren som skyldig. Det enda de konstaterar är att datorn varit med om något. För att ta tillvara på användarnas erfarenheter används helpdesk. Det som kommer till helpdesk vidarebefordras till den lokala informations- eller IT-säkerhetspersonalen, därefter tas frågorna upp centralt. De har idag ingen typ av forum där användarna kan diskutera erfarenheter sinsemellan. De har incidentrapportering men inte den typen av forum.

När det gäller att göra användarna uppmärksamma på risker och hot inom mobilt arbete påstår Niklas att det gäller att lyfta fram och påminna om risker och hot vid olika sammanhang. Det gör de idag när de träffas gruppmissigt men han berättade också att de skulle kunna göra det på ett bättre sätt. Idag sker utbildning internt, de har inte någon standardutbildning. De kommunicerar sina egna policys, instruktioner, erfarenheter och ”tänk på detta”. Vid nyanställning har de ett introduktionsprogram som innehåller företagets verksamhetsbeskrivning, arbetsrutiner och policys. Den nyanställde måste kvittera att de har mottagit, läst och förstått de olika policys som finns.

Hanna berättade att det användarna uppmärksammas på inte är specifikt för mobilt arbete utan är rent etiskt vad de får och inte får göra. Exempel på sådana uppmaningar är vad medarbetarna inte får ladda hem, vad de inte får koppla in själv, vad de inte får installera på deras datorer, att de inte får surfa var som helst och att de inte får uttrycka sig hur som helst i e-mail som lämnar företaget. Hanna försöker poängtera för användarna att de aldrig är anonyma när de befinner sig på företaget. De lägger fokus på utbildning och samtliga anställda har gått en obligatorisk standardutbildning som ligger på deras intranät. De anställda får inte sina enheter förrän de klarat den tenta som ingår i utbildningen vilken kräver 75% rätt. Det svåra är att få den personal som varit anställda på företaget en längre tid att genomgå samma utbildning som de nyanställda. Det gäller att motivera dem och få med sig alla VDar så att de går ut och pushar på det och säger hur viktigt det är.

Genom att konstant upplysa användarna och försöka skapa en känsla om att säkerhetsarbetet är viktigt så ökar medvetenheten, anser Lisa. På CapGemini finns e-learningutbildningar som både är på användarnivå och mer avancerade nivåer för konsulter. Personalen blir också informerade av sin chef om säkerheten och har en 3-dagars introduktionsutbildning som gäller alla. Alla får också en fadder som hjälper till med praktiska saker och informerar om allt som de nyanställda behöver veta. Lisa berättar att de inte har någon tenta på utbildningen och att det märks väldigt snabbt när en konsult gör fel. De anställda har även möjlighet att genomföra så kallade *brown bag sessions* som går ut på att ta tillvara på varandras kunskaper inom företaget. Företaget bjuder då på lunch och en timmes utbildning.

5. Analys

I detta kapitel analyseras resultatet från intervjuerna utifrån vår litteraturundersökning. Här kopplas teorin till vårt empiriska material.

5.1 Mobilt arbete

Hur intervjupersonerna definierade mobilt arbete skiljer sig till viss del åt men har ändå en liknande riktning. Som exempel säger intervjupersonerna att mobilt arbete är när användaren är utanför fast uppkoppling i nätverket, utanför företagets skalskydd och när de tar med sig information ut från företaget till oskyddade miljöer som flygplatser, hotellrum eller till hemmet. Intervjupersonernas syn på mobilt arbete stämmer överens med Clear och Lee-Kelley (2005) som använder termen *telework* och Carnahan och Guttman (1998) som använder *telecommuting* för att beskriva arbete som utförs utanför företaget. Detta kan innebära att arbeta hemma, hos en kund eller på resande fot.

De företag vi har intervjuat arbetar mobilt och under intervjun med Lisa framkom att företag idag till viss del inte klarar sig utan mobilt arbete. Detta får stöd av Kowalski och Swanson (2005) som skriver att implementering av mobilt arbete är nödvändigt för de flesta organisationer för att vara konkurrenskraftiga. Det finns flera anledningar till att företag börjar arbeta mobilt. Intervjuerna har visat att anledningarna skiljer sig åt beroende på företagets verksamhetsområde. Ett företag började arbeta mobilt för att underlätta serviceenhetens arbete som befinner sig ute hos kunderna. Ett annat företag började arbeta mobilt för att utvecklas med de mobila tjänster och produkter de säljer. Vad gäller konsultfirmor ligger det i affärsidén att vara mobil då arbetet till största del görs i anslutning till kunden vilket Manoochehri och Pinkerton (2003) anser är en fördel då det ökar företagets möjligheter att schemalägga och planera utifrån kundernas behov. Ytterliggare anledningar som kom fram under intervjuerna är en kombinationen av att yngre personal tillträder, avståndet till arbetsplatsen växer och att det är fler arbetsrelaterade resor idag än förr. Dessa anledningar till att börja arbeta mobilt bekräftas av Manoochehri och Pinkerton (2003) som anser att mobilt arbete möjliggör för företag att anställa personal som inte bor i närheten av företagets fysiska kontor samt den flexibilitet som erbjuds avseende plats och tid. Intervjupersonerna tror att de anställda är positiva till att arbeta mobilt då de har möjlighet att kunna välja var och när de vill jobba. Detta visade sig stämma överens med Manoochehri och Pinkerton (2003) som påstår att mobilt arbete har visat sig öka tillfredsställelsen bland de anställda.

5.2 Risker och hot inom mobilt arbete

Enligt Economist Intelligence Unit's [3] undersökning väntar många företag att införa mobilt arbete på grund av brister i säkerheten. Intervjupersonerna är oeniga om det verkligen är så. Niklas (VD) tror att företag väntar med införandet då de saknar kunskap om vilka säkerhetslösningar som finns till skillnad från Lisa (konsult) som tror att företag inför mobilt arbete utan att vara medvetna om de säkerhetsproblem mobilt arbete skapar. Kowalski och Swanson (2005) skriver att eftersom området är relativt nytt saknar många organisationer förståelse och medvetenhet vilket försvårar implementeringsfasen för mobilt arbete. Lisa hävdar att mobilt arbete innebär att företaget utsätter sig för en annan och högre risk och tar som exempel att anställda ser de mobila enheterna som sina privata och använder de till annat än arbetsrelaterade uppgifter. Hon tar som exempel att användarna tar hem den bärbara företagsdatorn och fildelar, installerar applikationer och spelar nätverksspel. Hon berättade att det är viktigt att poängtera att det faktiskt är företagets dator. Detta hävdar också Clear och Lee-Kelley (2005) som skriver att mobilt arbete orsakar utmaningar för säkerheten som är

identiska med det konventionella kontoret men kan även innebära ytterliggare risker. För att uppnå så hög säkerhet som möjligt berättade Lisa att det är viktigt att integrera logiskt, administrativt och fysiskt skydd vilket kan kopplas till Whitman och Mattord (2005) som skriver att organisationers säkerhet måste bestå av flera lager.

De risker och hot som intervjupersonerna tar upp överensstämmer med de vi identifierade vid litteraturstudien och som finns presenterade i teorin. Exempel på risker och hot från intervjuerna är stöldrisk av såväl mobila enheter (Armstrong, Wynne & O'Shea, 2004) som information (Clear & Lee-Kelley, 2005), virusangrepp mot mobila enheter (Clear & Lee-Kelley (2005) och lösenordshantering (Wood, 1997)

Samtliga intervjupersoner berättade under intervjuerna om internangrepp som hotar säkerheten. Niklas tar exemplet när anställda slutar och vikten av att stänga av deras konton och byta lösenord till deras behörigheter. Om den anställda ska börja arbeta hos en konkurrent kan det även vara lämpligt att bevaka dennes mailbox. Whitman och Mattord (2005) skriver att oavsett skälen till att en anställning upphör bör den anställdes tilldelade behörigheter fräntas vid uppsägning. Det kan även vara befogat att tilldela den anställda mindre känsliga arbetsuppgifter under uppsägningstiden. Niklas fortsätter och berättar att det som sitter i huvudet på den anställda inte går att radera och är därför ett problem. Lisa tar upp exemplet med anställda som gör avsiktliga internangrepp, de som vill göra en illa eller vara elaka, men tillägger också att det är en minoritet. SIG Security (1997) skriver att sådana fall kan uppstå vid exempelvis missnöje, oväntat besked och utebliven förväntad löneförmån. Under denna kategori placeras även det problem som Hanna (CISO) beskriver där användare försöker ta sig förbi brandväggar för att tillgodose sig fler rättigheter än vad de är berättigade till.

5.3 Ansvar för planering och uppdatering av säkerhet

Intervjupersonerna är överens om att det är företagets VD som är övergripande ansvarig för säkerheten men att säkerhetsansvaret kan delegeras till underordnade. Detta innebär, som SIG Security (1997) skriver, att tjänsten som säkerhetsansvarig inte bör placeras på IT-avdelningen utan direkt under verksamhetsledningen. En av ledningens viktigaste funktioner är vidare att delegera samordningen av informationssäkerhetsarbetet till underordnade chefer eller motsvarande. Tipton och Krause (2003) skriver att stora organisationer kan använda sig av en IT-kommitté för att ta beslut rörande IT-satsningar. Detta fick en klar koppling till intervjun med Hanna (CISO) då EON, som är ett stort företag, använder sig av en IT-kommitté.

Kowalski och Swanson (2005) hävdar att det är viktigt att inte bara titta på produktivitet och kostnadsbesparingar för att få ett lyckat resultat, utan också undersöka själva processen för mobilt arbete. Detta berättade Lisa (konsult) är alltför vanligt vid planering av IT-projekt i allmänhet där fokus läggs på kostnad och funktion medan säkerheten glöms bort.

5.4 Policy som säkerhetsskydd

Brandel (2007) påstår att många företag inte har upprättat någon mobilitetspolicy trots de många risker som är förknippat med mobilt arbete. Detta visade sig stämma bland intervjupersonerna. Lisa (konsult) hävdar att policybiten är relativt sen och inga av de intervjuade företagen har någon policy som behandlade mobilitet innan år 2004. Lisa fortsätter att berätta att det är absolut nödvändigt med policy för att kunna tala om för användare att de har gjort fel. Finns det inte specificerat vad de får göra och hur de ska göra kan de inte anklagas för att ha gjort fel. För detta ändamål bör det finnas en säkerhetspolicy som återspeglar ledningens inriktning för säkerhetsskydd och informationssäkerhet (SIG

Security, 1997). Målet bör vara att alltid försöka ha en policy som täcker in den existerande hotbilden (Danchev, 2003). Hanna (CISO) berättar att de på EON har en avdelning som ansvarar för att uppdatera säkerhetspolicys när nya hot identifieras. Niklas (VD) berättar att han kontinuerligt träffar de som sköter den interna säkerheten för att diskutera säkerhetssituationen. Det räcker dock inte med en policy. Niklas berättade att policyn i sig inte är det viktiga, det viktiga är att företagen lyckas efterleva den. En policy är enkel att skapa, det svåra är att följa den. Detta har även SIG Security (1997) uppmärksammat, de skriver att det är lättare att skapa reglerna än att praktiskt få den att fungera. Foltz et al. (2005) skriver att existensen av policys i en organisation garanterar inte att alla användare har läst dem. Även om de flesta förstår att regler och begränsningar finns kan många vara obekanta med innebörden av policyn, dess regler och begränsningar.

5.5 Den mänskliga faktorn som säkerhetsrisk

Samtliga intervjupersoner är överens om att den mänskliga faktorn är en säkerhetsrisk. Gonzales och Sawicka (2002) påstår att användarna är den svagaste länken och att de orsakar 80-90% av alla säkerhetsrelaterade problem i organisationer. Detta anser intervjupersonerna beror på att användarna är för dåligt utbildade. SIG Security (1997) och Whitman och Mattord (2005) skriver att användarna ska utbildas i säkerhet och korrekt hantering av information för att minimera potentiella risker. Tipton och Krause (2003) skriver att utbildning är nyckeln för att förstärka effektiviteten inom säkerhet.

Hanna (CISO) tror dock inte att det räcker med utbildning. Oavsett utbildning kommer användarna inte att följa reglerna fullt ut då allt de lär sig kommer att tolkas utifrån deras egen referensram. Hon berättade att de måste använda de tekniska hjälpmedel som finns för att hjälpa användarna att göra så rätt som möjligt och påstår att de hade varit en ännu större säkerhetsrisk om de inte hade satsat på tekniska lösningar. Thomson och Solms (1998) skriver om belöningar i utbildningssammanhang och anser att de ska delas ut när det förväntade resultatet uppnås. I EONs utbildningsprogram ingår en tenta vilken måste klaras till 75% för att få tillgång till enheterna vilket kan ses som en belöning. Hanna berättade också att det gäller att motivera användarna genom att engagera högsta ledningen så att de går ut och berättar hur viktig säkerheten är. Detta ska enligt Thomson och Solms (1998) underlätta då lydnad för auktoriteter är en självklarhet i samhället. Om detta tillämpas på rätt sätt kommer användarna att acceptera de budskap som auktoriteterna förmedlar. Det är ofta ofattbart hur långt människor är redo att gå för att lyda en ledargestalt enligt Thomson och Solms (1998).

Lisa (konsult) berättade under intervjun att policy och utbildning kan vara ett rättesnöre och kanske förhindra det mesta. Det finns dock fortfarande de som har läst men inte förstått dem, det finns de som inte har läst och det finns de som har läst och förstått men inte bryr sig. När dessa problem är aktuella är det ingen mening med att ha deltagarnas uppmärksamhet om de inte förstår vad som presenteras. För att nå ut till deltagarna under utbildningen är mediet som används en kritisk faktor. När komplex information ska förmedlas är skriven media att föredra då deltagarna i egen takt kan repetera in och försäkra sig om att de förstår budskapen. När mindre komplex information förmedlas är muntlig presentation att föredra (Thomson & Solms, 1998). För att öka säkerheten ytterligare bland de anställda kan användare lära av varandra. Thomson och Solms (1998) skriver att användare kan se deras kollegor utföra uppgifter som upprätthåller informationssäkerheten och på så vis anta ett liknande beteende. Lisa berättar att de tillämpar detta genom att de anställda har möjlighet att anordna *brown bag sessions* som är en form av utbildning som går ut på att ta tillvara på varandras kunskaper inom företaget. Hanna berättar att de på EON inte har någon anpassad lösning där användarna kan diskutera erfarenheter sinsemellan. Användare hänvisas till företagets helpdesk när

problem uppstår eller ombeds att göra en incidentrapportering. När det gäller att göra användarna uppmärksamma och medvetna om de risker och hot som finns inom mobilt arbete berättade Niklas (VD) och Lisa att det är nödvändigt att konstant upplysa användarna och försöka skapa en känsla om att säkerhetsarbetet är viktigt. Thomson och Solms (1998) skriver att detta kan göras genom repetition av viktiga fakta under utbildningstillfällen. Det ökar chanserna att deltagarna kommer ihåg det som presenteras. Detta får stöd av Foltz et al. (2005) som hävdar att ledningen ständigt måste diskutera rätt och fel användande, åtgärder vid missbruk och moral med användarna i organisationen.

6. Diskussion

Detta kapitel redogör för vad vi har kommit fram till utifrån vårt syfte och sammanfattar vårt arbete. Diskussionen utgår från analysen av det empiriska materialet. Här presenteras också vårt förslag till fortsatt forskning inom området.

Som vi nämnde i inledningen räcker det inte med policys och hårdvara för att upprätthålla en hög säkerhet då dessa enheter är statiska. Till skillnad från hårdvara handlar människan innovativt och emotionellt i nya situationer och anpassar sig till den verklighet som råder. Människan är den svagaste länken och står för 80-90% av säkerhetsrelaterade problem i organisationer. Med denna utgångspunkt har vi undersökt och belyst den mänskliga faktorns betydelse för säkerhetsarbetet kring mobilt arbete.

Vår inledande föreställning var att företag väntar med att införa mobilt arbete på grund av brister i säkerheten, detta grundade sig på de tidningsartiklar vi använde som inspiration till området. I såväl litteraturstudien som i den kvalitativa undersökningen påträffade vi åsikter som skiljde sig åt i fråga om företag väntar med införandet. Största delen av vårt insamlade material visar att konkurrenssituationen är en stor anledning till att företag idag måste införa mobilt arbete. Detta görs ofta utan att företagen är medvetna om vilka säkerhetsproblem de därmed utsätter sig för. De som anser att företag väntar med införandet har som argument att det saknas medvetenhet om vilka risker och åtgärder som finns inom området. Vi instämmer i åsikten om att företag saknar medvetenhet om vilka säkerhetsproblem de utsätter sig för och anser att företag idag tvingas införa mobilt arbete för att vara konkurrenskraftiga. Då ledningen har det yttersta ansvaret för att upprätthålla säkerheten och exempelvis måste fastställa policys som täcker den nuvarande hotbilden anser vi att de måste hålla sig uppdaterade inom området. Ledningen har även möjlighet att delegera detta ansvar till säkerhetschefer eller motsvarande. Oavsett vem som tilldelas ansvaret måste de utbildas för att kunna upprätthålla säkerheten.

Även om de säkerhetsansvariga är medvetna om vilka risker och lösningar som finns inom området så är den mänskliga faktorn fortfarande den största säkerhetsrisken. För att kunna tala om för användarna vad som är rätt och fel måste de ha läst och förstått företagets policys. Existensen av policys garanterar inte att användarna har läst dem eller förstått innebörden, dess regler och begränsningar. Ledningen måste därför ständigt diskutera rätt och fel användande, åtgärder vid missbruk och moral med de anställda. Många företag redogör policyn endast en gång för användarna. Vi anser att policyn kan synas oftare om den presenteras på ett mer intressant sätt. Genom att involvera användarna i policyutvecklingen ser vi möjligheten att uppmuntra användarna till att följa reglerna. På detta sätt förankras policyn och blir en del av det dagliga arbetet. Det är ändå nödvändigt att de anställda utbildas och regelbundet uppdateras om företagets policys.

Anledningen till att den mänskliga faktorn är den största säkerhetsrisken beror på att användarna är för dåligt utbildade, enligt samtliga intervjupersoner. Då ledningen har det övergripande säkerhetsansvaret anser vi att de bör försäkra sig om att samtliga användare blir utbildade. Utbildning av användare är nödvändigt men har sina begränsningar. Det är viktigt för företag att även investera i de tekniska hjälpmedel som finns då dessa hjälper användarna att göra så rätt som möjligt. Tekniken kompletterar dock inte alltid användarnas brister, därför måste utbildning ske kontinuerligt och anpassas efter användaren. Detta är viktigt då allt användaren lär sig kommer att tolkas utifrån dennes referensram. Vi tror att det är viktigt att rikta utbildningen till användarnas ålder och tidigare erfarenheter då detta är betydelsefullt för

användarnas beteende och attityd. Utbildning kan även ske genom intern kommunikation på företaget. Detta kan höja säkerheten genom att erfarenheter som visat sig upprätthålla säkerheten sprids kollegor emellan.

Många av de risker och hot som presenterades under intervjuerna har sitt ursprung redan innan mobilt arbete infördes. Ett nytt problem som uppstått med mobilt arbete är att användare ser de mobila enheterna som sina egna, detta skapar problem när de använder enheterna till annat än arbetsrelaterade uppgifter som motstrider de regler som finns. Detta tyder på att policys inte följs. Detta problem tas inte upp i den litteratur vi har studerat men vi anser att det är ett allvarligt problem som ställer nya och högre krav på säkerheten. Detta kan också vara en av anledningarna till att virus ofta bärs in på företag.

Vi har i vår undersökning sett prov på områdets enorma komplexitet avseende säkerhet. Det är svårt att urskilja de olika problem som är förknippat med mobilt arbete då de ofta är beroende av varandra. Har ledningen inte tillräckligt med kunskap inom området påverkas policyutveckling och utbildning. Detta leder till att användarna inte blir tillräckligt säkerhetsmedvetna för att arbeta mobilt på ett säkert sätt. Vi tolkar resultatet av vår undersökning som att stora företag har mindre förtroende för sina användare vad gäller mobilt arbete. De begränsar riskerna som den mänskliga faktorn utgör genom att investera i tekniska lösningar. Mindre företag som inte investerar tekniska lösningar måste lägga mer fokus på att utbilda användarna och förlita sig till att användarna är säkerhetsmedvetna.

6.1 Förslag till fortsatt forskning

Resultatet av undersökningen visar att säkerhetsutbildningarna innehåller brister. Vi anser att vidare forskning inom detta område ska fokusera på knowledge management och beteendevetenskap. Genom att kombinera lärande, medvetenhet och kunskapsspridning tillsammans med beteende, motivation och attityd skapas förutsättningar för bättre utbildning inom säkerhet.

7. Slutsats

Detta avslutande avsnitt besvarar vår fråga genom att ge förslag på åtgärder.

Följande punkter besvarar frågan *Hur kan IT-säkerhetsansvariga förstärka säkerheten för mobilt arbete utifrån den mänskliga faktorn som säkerhetsrisk?:*

- Företag inför mobilt arbete utan att vara fullt medvetna om vilka risker de utsätter sig för. Detta kan förebyggas genom att företag och dess ledning blir mer medvetna om riskerna samt vilka tekniska hjälpmedel och lösningar som finns att tillgå.
- Användare har ofta svårt att efterleva företagets policys, dess regler och begränsningar. Detta kan förebyggas genom att policys presenteras oftare och på ett mer intressant sätt. Genom att involvera användarna i policyutvecklingen ser vi möjligheten att uppmuntra användarna till att följa reglerna. Detta leder till att policys förankras i det dagliga arbetet och påminner användarna om de regler som finns.
- Användare som inte är säkerhetsmedvetna är den största säkerhetsrisken inom mobilt arbete. Detta kan förebyggas genom att ledningen tar ett större ansvar i att utbilda användarna.
- Användarna får inte alltid den utbildning de behöver inom säkerhetsområdet. Detta kan förebyggas genom att utbildning sker kontinuerligt och formas utifrån användarnas referensramar i fråga om erfarenhet och ålder.

8. Referenser

- Arce, I., & Levy, E. (2003) *The Weakest Link Revisited*. IEEE Security & Privacy.
- Armstrong, H., Wynne, M., & O'Shea, T. (2004). *Who has the keys to the vault? Protecting secrets on Laptops*. Submitted to IEEE Information Assurance Workshop June 2004.
- Badamas, M. (2001). *Mobile computer systems – security considerations*. Information Management & Computer Security. Vol. 9. No. 3. s. 134-136.
- Brandel, M. (2007, 02, 26). *Strategies & Tactics - Home office lockdown*. Computerworld. Vol. 41. No. 9. s. 26.
- Carlsson, B. (1991). *Kvalitativa forskningsmetoder för medicin och beteendevetenskap*. Almqvist & Wiksell.
- Carnahan, L., & Guttman, B. (1998). *Security Issues for Telecommuting*. Information Technology Laboratory. National Institutes of Standards and Technology.
- Clear, F., & Lee-Kelley, L. (2005). *Risks to data security for small firms raised by telework*. IACIS Pacific 2005 Conference Proceedings.
- Dhamija, R., Tygar, J., & Hearst, M. (2006). *Why phishing works*. Proceedings of the SIGCHI conference on Human Factors in computing systems.
- Danchev, D. (2003). *Building and Implementing a Successful Information Security Policy*. WindowSecurity.com - Windows Security resource for IT admins.
- Denscombe, M. (2000). *Forskningshandboken – för småskaliga forskningsprojekt inom samhällsvetenskaperna*. Studentlitteratur.
- Foltz, C., Cronan, T., & Jones, T. (2005). *Have you met your organization's computer usage policy?* Industrial Management & Data Systems. Vol. 105. No.2. s. 137-146.
- Foote, D., Seipel, S., Johnson, N., & Duffy, M. (2005). *Employee commitment and organizational policies*. Management Decision. Vol. 43. No. 2. s. 203-219.
- Gehringer, E. (2002). *Choosing Passwords: Security and Human Factors*. Department of Electrical Computer Engineering, Department of Computer Science. North Carolina State University.
- Gonzales, J., & Sawicka, A. (2002). *A framework for Human Factors in Information Security*. Grimstad: Agder University College, Department of Information and Communication Technology.
- Halvorsen, K. (1992). *Samhällsvetenskaplig metod*. Studentlitteratur: Lund.
- Harpaz, I. (2002). *Advantages and disadvantages of telecommuting for the individual, organization and society*. Work Study. Vol. 51. No. 2. s. 74-80.

- Holme, I., & Solvang, B. (1997). *Forskningsmetodik – Om kvalitativa och kvantitativa metoder*. Studentlitteratur: Lund
- Johannessen, A., & Tufte, P. (2003). *Introduktion till samhällsvetenskaplig metod*. Liber AB.
- Kelly, G., & Locke, K. (1999). *The Telecommuting Life: Managing Issues of Work, Home and Technology*. Pennsylvania: Hershey: Idea Group Inc.
- Kim, I., Kim, H., Lee, J., & Choi, J. (2005). *Analysis and Modification of ASK Mobile Security Protocol*. Dept. of Computer Science and Engineering, Korea University, Seoul.
- Kowalski, K., & Swanson, J. (2005). *Critical success factors in developing teleworking programs*. Benchmarking: An International Journal. Vol. 12. No.3. s. 236-249.
- Manoochehri, G., & Pinkerton, T. (2003). *Managing Telecommuters: Opportunities and Challenges*. American Business Review. Jan 2003. s.9-16.
- Nayak, D., Rajendran, N., Phatak, D., & Gulati, V. (2004). *Security Issues in Mobile Data Networks*. IEEE.
- Orshesky, C. (2003). *Beyond technology – The human factor in business systems*. Journal of business strategy. Vol.24. No.4. s.43-47.
- Papmehl, A. (2001, 05, 11). *Remote Access – Adapting business to the home-based worker*. CMA Management. Vol.75. No.3. s.11.
- Patriciu, V., & Bica, I. (2002). *Organization Information Security Management*. Bucharest: Military Technical Academy.
- Ryen, A. (2004). *Kvalitativ Intervju – Från vetenskapsteori till fältstudier*. Liber AB
- Scheuermann, D. (2002). *The smartcard as a mobile security device*. Electronics & Communication Engineering Journal. October 2002
- SIG Security. (1997). *Riktlinjer för god informationssäkerhet – SSR97ETT*. Studentlitteratur: Lund.
- Siponen, M. (2000). *A conceptual foundation for organizational information security awareness*. Information Management & Computer Security. Vol.8. No.1. s.31-41.
- Sturgeon, A. (1996). *Telework: threats, risks and solutions*. Information Management & Security, 4/2 (s. 27-38).
- Thomson, M., & Solms, R. (1998). *Information security awareness: educating your users effectively*. Information Management & Computer Security. Vol.6 No.4. s. 167-173.
- Tipton, H., & Krause, M. (2003). *Information Security Management Handbook*. Boca Ration, Florida: Auerbach.

Walter, T., Bussard, L., Roudier, Y., Haller, J., Kilian-Kehr, R., Posegga, J., & Robinson, P. (2004). *Secure Mobile Business Applications – Framework, Architecture and Implementation*. Information Security Technical Report. Vol. 9. No. 4. s. 6-21.

Whitman, M., & Mattord, H. (2005). *Principles of Information Security*. Boston: Thomson Course Technology

Winter, J. (1985). *Problemformulering, undersökning och rapport*. Liber Förlag

Carnahan, L., Guttman, B. (1998). *Security Issues for Telecommuting*. Information Technology Laboratory. National Institute of Standards and Technology.

Wood, C. (1997). *A secure password storage policy*. Information Management & Computer Security. Vol. 5. No.2. s.79-80.

Elektroniska källor

[1] <http://www.idg.se/2.1085/1.82892> (2007-02-02 11:20)

[2] <http://www.idg.se/2.1085/1.88782> (2007-02-02 10:45)

[3] http://www.symantec.com/sv/se/about/news/release/article.jsp?prid=20060406_01
(2007-01-28 14:30)

[4] <http://www.idg.se/2.1085/1.51854> (2007-04-23 14:10)

[5] <http://www.dfs.se/kretsar/sodra/natverken/it-saekerhet/>

Bilagor

Bilaga 1: Förfrågan till intervjupersoner

Hej!

Vi är två studenter som läser sista året Informatik på Högskolan i Halmstad. Vi skriver just nu en c-uppsats där vi försöker identifiera säkerhetsrisker i företag/organisationer som använder sig av mobila enheter (mobiltelefoner, bärbara datorer, USB-minnen osv.) i det vardagliga arbetet. Vår uppsats fokuserar på användare av dessa enheter och vilken säkerhetsrisk de kan innebära för organisationen vid mobilt arbete. Vi vill identifiera säkerhetsrisker inom detta område och ge förslag på hur företag kan förstärka sin säkerhet vid mobilt arbete utifrån den mänskliga faktorn.

Vi undrar om Ni har anställda som arbetar mobilt, dvs med bärbara datorer, mobiltelefoner, USB-minnen eller andra mobila enheter? Om ni bedriver denna typ av verksamhet skulle vi gärna vilja komma i kontakt med er för att göra en intervju med de som ansvarar för IT-säkerheten. Intervjun skulle i stort handla om vilka säkerhetsrisker ni identifierat vid införandet/användandet av mobila enheter (kring användaren), vilka säkerhetsrutiner/policys ni använder er av och hur ni gör användarna medvetna om säkerhetsriskerna.

Vi har planerat att genomföra våra intervjuer under Mars månad. Vi skulle gärna vilja träffa er på plats för att genomföra intervjun, vid undantag kan även telefonintervjuer tillämpas. För att maximera resultatet av intervjun skulle vi vilja använda oss av ljudupptagning, hoppas att detta inte ska vara några problem för er.

Om ni är intresserade av att delta i en intervju kommer vi att förbereda er genom att skicka ut material med övergripande samtalsämnen.

Dennis Möller och Axel Nordin-Svensson

Bilaga 2: Intervjufrågor

1. Vad innebär mobilt arbete för Dig?

Motivering: Denna fråga skapades för att kontrollera om vår bild av mobilt arbete stämmer överens. Detta bidrar till att vi genom hela intervjun förstår varandra i fråga om begreppet mobilt arbete.

2. Bedriver ert företag mobilt arbete och i så fall sedan hur lång tid tillbaka?

Motivering: Inledande fråga för att kontrollera hur väl insatt intervjupersonen är inom området mobilt arbete och för att få en bakgrund till deras erfarenhet av det.

3. Vad var det som fick företaget att börja med mobilt arbete och hur har arbetet utvecklats?

Motivering: Manoochehri & Pinkerton (2003) visar vad mobilt arbete kan innebära för både företag och anställda (kap 2.2). Vi vill undersöka de olika företagens anledningar till att de började med mobilt arbete.

4. Vilka får tillgång till mobila enheter för att kunna arbeta mobilt och vilka enheter får dem tillgång till?

Motivering: Denna fråga tar reda på hur modern infrastruktur företaget har för mobilt arbete och är av vikt när vi diskuterar deras säkerhet. Enligt Whitman & Mattord (2005) kräver de mobila enheterna mer säkerhet än de system som finns inom företagets väggar (kap 2.3).

5. Hur planerade ert företag kring säkerheten vid införandet av mobilt arbete?

Motivering: För att få ut det bästa resultatet vid skapande av riktlinjer för mobilt arbete måste företag studera processerna, verktygen och tekniken som används, inte bara resultat och effekt av det mobila arbetet. (Kowalski & Swanson, 2005) (kap 2.2). Denna fråga visar på företagets medvetenhet om säkerhet vid införandet av mobilt arbete.

5.1 Hade ert företag tidigare policys som ni kunde vidareutveckla för att de skulle passa för mobilt arbete eller var ni tvungna att arbeta fram helt nya policys?

Motivering: Det bör finnas ett övergripande dokument - en säkerhetspolicy - som återspeglar ledningens inriktning för säkerhetsskydd och informationssäkerhet (SIG Security) (kap 2.5). Denna fråga visar på hur stor vikt företaget har lagt på att skapa specifika policys för mobilt arbete.

5.2 Vilken nivå på företaget planerar och ansvarar för säkerheten och hur många är involverade i arbetet?

Motivering: SIG Security (1997) skriver att betydelsen av informationssäkerhetsfunktionen motiverar att ansvaret placeras direkt under verksamhetsledningen. Tjänsten bör alltså inte placeras på IT-avdelningen (kap 2.4). Denna fråga visar i vilket omfattning företaget arbetar med säkerhet och om/hur det förankras i hela organisationen.

6. Vi anser att företag väntar med att införa mobilt arbete på grund av brister i säkerheten. Stämmer detta och vilka risker är det som hindrar utbredningen?

Motivering: Enligt Economist Intelligence Unit's undersökning [1] väntar företag med att införa mobilt arbete då de anser att det finns brister i säkerheten (kap 1.2). Denna fråga ger dels en indikation på hur trovärdig Symantecs undersökning är och vi vill här även se om intervjupersonen lyfter fram den mänskliga faktorn som en brist i säkerheten.

7. Vi anser att ett problem kring mobilt arbete är bristen på policys och riktlinjer, hur ser Du på detta?

Motivering: Kowalski & Swanson (2002) skriver att det ännu inte har gjorts några studier eller rapporter med riktlinjer för mobilt arbete (kap 2.2). Denna fråga undersöker om intervjupersonens åsikter stämmer överens med denna åsikt som vi också uppmärksammat i branschtidningar.

8. Hur har ert företag gjort användarna uppmärksamma på vilka hot och risker som föreligger kring mobilt arbete?

Motivering: För att användarna ska vara medvetna om de befintliga hoten i det vardagliga arbetet ska de utbildas i säkerhet och korrekt hantering av information. (SIG Security, 1997; Whitman & Mattord, 2005) (kap 2.6). Med denna fråga vill vi indirekt ta reda på om företaget erbjuder sina anställda utbildning i säkerhet.

9. Får användarna någon utbildning kring säkerhet och vad är det för utbildning?

Motivering: SIG Security (1997) och Whitman & Mattord (2005) skriver om vikten av att användare får nödvändig utbildning i gällande säkerhetspolicy, säkerhetskrav och regler samt erforderlig utbildning i användningen av IT-resurserna (kap 2.6). Denna fråga bygger vidare på föregående och vill mer detaljerat ta reda på vad det är för utbildningar som erbjuds.

9.1 Hur försäkrar ert företag sig om att användarna har tagit åt sig och följer säkerhetsreglerna?

Motivering: Foltz et al. (2005) anser att ledningen måste diskutera rätt och fel användande, åtgärder vid missbruk och moral med de anställda i organisationen (kap 2.5). Denna fråga syftar till att förtydliga huruvida användarna är en säkerhetsrisk.

9.2 Hur gör ert företag för att användarna ska vara uppdaterade om vad som händer i det interna säkerhetsarbetet?

Motivering: Enligt SIG Security (1997) är det viktigt att användarna involveras och aktivt deltar i ansträngningarna för att förbättra säkerheten (kap 2.6). Med denna frågan vill vi ta reda på hur företag gör för att fortlöpande involvera användarna i det dagliga säkerhetsarbetet.

10. Vilka säkerhetsproblem har ert företag stött på kring användarna vid mobilt arbete och hur hanterar ni dessa?

Motivering: De förväntningar som policys skapar är beroende av förståelse för personalens motivation, eller den positiva eller negativa psykologiska kraft som påverkar deras beteende gentemot organisationens policys (Foote et al., 2005) (kap 2.5). Vi vill identifiera vilka problem som är aktuella hos företagen som vi intervjuar. Detta för att få en tydligare bild av det existerande problemområdet.

11. Hur gör ert företag för att ha en öppen dialog med användarna om säkerhetsproblem som uppkommit?

Motivering: I arbetet med att balansera tillgång och säkerhet är det viktigt att säkerhetspersonal och användare samarbetar och har förståelse för varandras synsätt (Whitman & Mattord, 2005) (kap 2.1). För att uppnå förståelse mellan användare och säkerhetspersonal anser vi att det är viktigt att ha en öppen dialog. Vi vill med denna fråga ta reda på om företag beaktar detta faktum och hur de går tillväga.

12. Vad har användarna för inställning kring mobilt arbete på ert företag?

Motivering: Harpaz (2002) skriver att det är svårt för företaget att ingjuta motivation och engagemang för de anställda när de arbetar mobilt (kap 2.2). Denna fråga undersöker hur användarna ställer sig till mobilt arbete vilket kan påverka hur väl de följer säkerhetsreglerna.

13. Hur ofta ser ert företag över och uppdaterar säkerhetsskyddet och hur går ni tillväga?

Motivering: Danchev (2003) påtalar vikten av att ha en uppdaterad säkerhetspolicy som täcker in den existerande hotbilden (kap 2.5). Vi vill ta reda på vilka rutiner företag har för att uppdatera sina säkerhetsskydd då nya hot uppstår.

14. Är nyttan med mobilt arbete tillräcklig med tanke på säkerhetsriskerna och varför är det så?

Motivering: Mobilt arbete orsakar utmaningar för säkerheten som är identiska med det konventionella kontoret men mobiliteten kan också innebära ytterliggare risker (Clear & Lee-Kelley, 2005) (kap 2.3). Här är vi ute efter en diskussion om huruvida mobilt arbete är tillräckligt säkert.

15. Vi anser att användarna är en säkerhetsrisk. Tror du att det är så och i så fall varför?

Motivering: Enligt Clear & Lee-Kelley (2005), är användarna den svagaste länken och utgör 80-90% av alla säkerhetsrelaterade problem i organisationer (kap 2.6). Vi undrar här på vilket sätt användarna är en risk för säkerheten.

16. Vilken är den största säkerhetsrisken, användare eller tekniken? Varför är det så?

Motivering: Arce & Levy (2003) skriver att datorbaserade säkerhetsapplikationer inte kan ersätta eventuella brister i organisationens säkerhetsstrategi vad gäller användarna (kap 1.1). Vi vill med denna fråga ytterliggare utveckla företagets syn på användarna kontra tekniken.