LUNDS UNIVERSITET

Ekonomihögskolan

Institutionen för informatik

Policy och dess efterlevnad

IS-ansvarigas perspektiv

Kandidatuppsats 15 hp, kurs SYSK02 i informationssystem

Författare: Erik Hallkvist
Philip Sköld

Handledare: Anders Svensson

Examinatorer: Odd Steen
Styliani Zafieroupolou

Policy och dess efterlevnad: IS-ansvarigas perspektiv

Författare: Erik Hallkvist och Philip Sköld

Utgivare: Inst. för informatik, Ekonomihögskolan, Lund universitet

Dokumenttyp: Kandidatuppsats

Antal sidor: 68

Nyckelord: informationssäkerhet, informationssäkerhetspolicy, efterlevnad, informationssäkerhetsansvarig

Sammanfattning (Max. 200 ord):
Arbetet med informationssäkerhet har på senare tid flyttat fokus från tekniska åtgärder till att i större utsträckning fokusera på administrativa och strategiska åtgärder. Det har konstaterats att anställda i organisationer utgör det största hotet mot informationssäkerheten. Organisationer har bemött hotet med att upprätta informationssäkerhetspolicys som dikterar hur anställda ska interagera med informationsresurser, dock är det vanligt förekommande att anställda inte följer dessa policys. Orsaken kan vara att policyn är svårförståelig och dåligt förankrad inom organisationen.

Det är den informationssäkerhetsansvariges arbete att framställa policy och förmedla ut den. Vidare innefattar dennes ansvar också de anställdas efterlevnad av dem. Flera tillvägagångssätt och metoder kan användas för att öka efterlevnadsgraden. Denna undersökning ämnar ta reda på hur informationssäkerhetsansvariga arbetar med policys och dess efterlevnad. Genom att intervjua tre stycken informationssäkerhetsansvariga har vi kunnat beskriva hur de arbetar med dessa frågor. Vi fann att de arbetar med policyutformning, förankring och revidering på ett snarlikt sätt. Gällande efterlevnad används utbildning, mätning, övervakning och sanktioner i varierande omfattning.

Innehåll

Figurer

Tabeller

Begreppsförklaring

IS: Informationssäkerhet

ISP: Informationssäkerhetspolicy

ISA: Informationssäkerhetsmedvetenhet (Information Security Awareness)

1 Introduktion

I detta kapitel presenterar vi undersökningens ämnesområde följt av vårt problemområde, syfte och frågeställning. Slutligen beskriver vi vilka avgränsningar undersökningen förhållit sig till. Då policy är ett brett begrepp kommer policy i denna uppsats syfta till både policy som behandlar informationssäkerhet och riktlinjer som rör informationssäkerhet.

1.1 Bakgrund

Informationssäkerhet har historiskt sett gått från att fysiskt skydda information från stöld, till mer tekniska lösningar när digitala informationssystem började tas i bruk (Gollmann, 2011; Whitman & Mattord, 2011). Idag ligger, framförallt akademiskt, återigen ett stort fokus även på den mänskliga faktorn. För att uppnå god säkerhet idag för både IT-system och information krävs ett beaktande av en kombination mellan människor, teknik och arbetsprocesser (Kearney, 2010). Tekniska säkerhetsåtgärder måste samspela med administrativa säkerhetsåtgärder för att vara verkningsfulla (Gollmann, 2011).

Det nämns ofta att orsaken till informationssäkerhetsproblem i organisationer kan härledas till anställda (Kearney, 2010). I datasäkerhetssammanhang har den mänskliga faktorn historiskt sett lämnats obeaktad. Men människor har alltid varit en risk i informationssäkerhetssammanhang, och idag anses anställda i organisationer vara en av de största informationssäkerhetsriskerna (Whitman & Mattord, 2011). Genom policys som behandlar säkerhetsfrågor kan organisationer definiera vad anställda får och inte får göra när de arbetar med organisationens teknik- och informationsresurser (Bulgurcu et al., 2010; Leveque, 2006).

Men anställdas tillkortakommande med att efterleva policys i organisationer utgör ett betydande hot (Siponen et al., 2010). Uppskattningsvis beror över hälften av dem fall där information kompromitterats på att anställda inte följt policy, och organisationer råkar vanligtvis ut för minst ett fall om året där anställda inte efterlever den antagna informationssäkerhetspolicyn. Detta har lett till att efterlevnad av policys i organisationer är ett omfattande problem (Vance et al., 2012). I en analys av 589 säkerhetsincidenter mellan åren 1980 och 2006, där persondata blivit kompromitterad, kunde 60% av fallen härledas till felaktigt handhavande i organisationer. Av de undersökta incidenterna så inträffade fler under 2005 och 2006 än det sammanlagda antalet mellan åren 1980 och 2004. Handhavandefelen omfattade fall där information av misstag hamnat för allmän beskådning eller åtkomst, där hårdvara eller backuper kommit bort, eller andra administrativa fel begåtts (Erickson & Howard, 2007).

1.2 Problemområde

När anställda i organisationer bryter mot policys beror det oftast på vårdslöshet, oaktsamhet, misstag eller att man avsiktligt avslöjar information (Kearney, 2010; Peltier, 2005a). An-

ställda bryter sällan avsiktligt mot policys och säkerhetsrutiner utan när det sker beror det oftast på dålig utformning av förfarandet eller bristande utbildning. Policys som är krångliga eller svårförståeliga riskeras att kringgås av anställda för att underlätta deras arbete (Kearney, 2010). Fastslagna säkerhetsrutiner kan i vissa fall upplevas som ett hinder i arbetet för den anställde när syftet med tillvägagångssättet inte känns väl definierat (Leveque, 2006).

Att öka efterlevnaden av informationssäkerhetspolicys handlar i grunden om att förändra individers beteenden. Tidigare forskning har främst fokuserat på hur olika beteendefaktorer påverkar den enskilde individens motivation att följa informationssäkerhetspolicys och att dessa beteendefaktorer influeras av organisatoriska åtgärder, exempelvis säkerhetsträning (Bulgurcu et al., 2010; Talib, 2015; D'arcy et al., 2009). Det verkar råda konsensus bland forskare att medvetenhets- och träningsprogram inom informationssäkerhet är absolut nödvändigt för att öka efterlevnadsgraden (Puhakainen & Siponen, 2010; Talib, 2015; Bulgurcu et al., 2010). Detsamma gäller övervakning och uppföljning av anställdas beteenden (Von Solms & Von Solms, 2004; Whitman & Mattord, 2011). Dock visar en undersökning av PwC (2015a) att bara 52% av de 9700 respondenterna hade någon form av aktiv övervakning av sin informationssäkerhet.

En annan undersökning av PwC (2015b) visar att 72% av de större tillfrågade organisationerna hade verksamma medvetenhets- och träningsprogram. Dock visar samma undersökning att 75% av organisationerna under samma tid haft informationssäkerhetsincidenter som kunnat härledas till de anställda. Medvetenhets- och träningsprogram måste uppfylla flera krav för att vara framgångsrika (Peltier, 2005b; Puhakainen & Siponen, 2010) samtidigt som övervakning medför både för- och nackdelar som måste balanseras (Spitzmüller & Stanton, 2006).

1.3 Syfte

Vi ämnar undersöka hur informationssäkerhetsansvariga arbetar för att öka efterlevnaden av informationssäkerhetspolicys. Målet är att identifiera dem förutsättningar hos policyn som möjliggör god efterlevnad, samt att kartlägga dem verktyg som bistår efterlevnadsarbetet.

1.4 Frågeställning

Hur arbetar informationssäkerhetsansvariga med informationssäkerhetspolicys och dess efterlevnad?

1.5 Avgränsningar

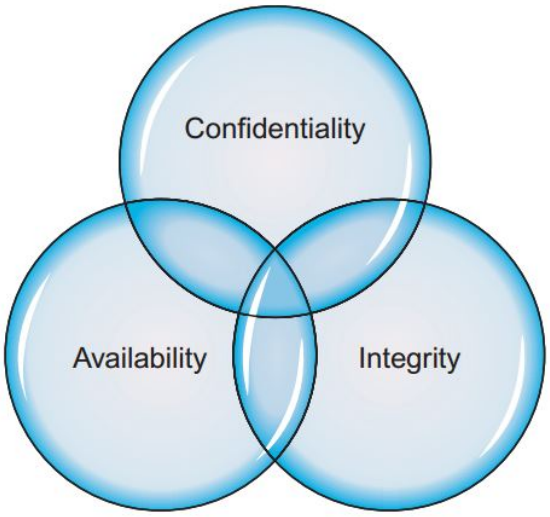
Huvudsakligen kommer undersökningen beröra informationssäkerhetspolicy i relation till IT-säkerhet. Undersökningen kommer inte behandla någon annans perspektiv än den ytterst informationssäkerhetsansvarige i organisationer. Fokus kommer inte heller läggas på informationssäkerhetspolicys vars efterlevnad är helt garanterad av tekniska eller fysiska åtgärder.

2 Teori

I detta kapitel presenteras tidigare forskning relaterat till vårt problemområde och frågeställning. Först beskrivs Informationssäkerhet då det är uppsatsens domän. Kapitlet Mänskliga faktorn ämnar ge en bakgrund till varför anställda ibland bryter mot policys. Resten av litteraturgenomgången mynnar ut i ett teoretiskt ramverk avsett att ligga till grund för vår empiriska undersökning.

2.1 Informationssäkerhet

Informationssäkerhet handlar i grunden om att hantera de risker som berör känslig data och kritiska resurser (Wheeler, 2010). Inom organisationer är information en värdefull resurs. För att skydda denna resurs syftar informationssäkerhet till att förhindra att information modifieras, förstörs eller avslöjas, och samtidigt säkerställa dess tillgänglighet till behöriga. (Leveque, 2006; Peltier, 2005a; Wheeler 2010; Whitman & Mattord. 2011). En vedertagen modell för att uppnå god informationssäkerhet är att säkerställa följande karaktärsdrag och krav på informationen:



Figur 2.1: CIA-Triaden (Andress, 2011, s. 171)

- Konfidentialitet – skyddad från obehörig åtkomst.
- Integritet – skyddad från obehörig modifiering, korrumperande eller förstörelse.
- Tillgänglighet – tillgänglig för behöriga.

(Gollmann 2011; Leveque, 2006; Peltier, 2005a; Wheeler, 2010; Whitman & Mattord, 2011)

Dessa tre karaktärsdrag utgör CIA-Triaden (se figur 2.1), som sedan dess introduktion blivit industristandard inom informationssäkerhet (Whitman & Mattord, 2011). Whitman & Mattord (2011) menar på att dessa karaktärsdrag fortfarande är högst relevanta i dagsläget, men att de inte är fullständigt tillräckliga i den ständigt föränderliga omvärld vi lever i. Då det ställs allt högre krav på säkerheten så är ytterligare ett viktigt krav på informationen spårbarhet (Wheeler, 2010). Spårbarhet innebär att hanteringen av information ska kunna härledas till en individ, plats och tid (Gollmann, 2011; Wheeler, 2010; Whitman & Mattord, 2011).

Det finns tre typer av säkerhetsåtgärder en organisation kan vidta för att minska risken för att information komprometteras. Dessa tre är fysiska-, logiska- och administrativa säkerhetsåtgärder. (Andress, 2011; Leveque, 2006) Fysiska åtgärder handlar om att skydda IT-tillgångar, såsom servers och datorer från icke-auktoriserade individer. Utan fysiska säkerhetssåtgärder kan övriga åtgärder tappa verkan. Det inkluderar exempelvis staket, lås, portar, kameror, alarmsystem.

Enligt Andress (2011) är tekniska åtgärder de mest välbekanta inom informationssäkerhet. De inkluderar bland annat brandväggar, lösenord och kryptering. Målet med dessa är precis som fysiska åtgärder att förhindra obehöriga individer åtkomst till känslig information.

Administrativa åtgärder definierar hur en organisations informationssäkerhetsarbete ska styras. Det utgörs av policys, procedurer, standarder och övriga riktlinjer ämnade att informera anställda hur verksamheten ska skötas på en daglig basis ur ett informationssäkerhetsperspektiv. Det utgör även grunden som fysiska och tekniska åtgärder baseras på. Enligt Andress (2011) är det oerhört viktigt att upprätthålla efterlevnaden av administrativa åtgärder.

Ansvaret för informationssäkerhetsarbete ligger hos den yttersta ledningen i organisationer. Organisationsledningen har ett styrningsansvar i arbetet med att säkerställa att åtgärder som krävs har vidtagits för att skydda informationen i verksamheten. I vissa fall kan styrelse eller ledning komma att hållas ansvarsskyldiga om någon obehörig kommer över organisationens informationsresurser. (Von Solms & Von Solms, 2004) Ansvaret innebär att styra informationssäkerhetsarbetet i linje med verksamhetens övriga affärsmål och se till att det finns tillräckliga resurser för att uppnå god säkerhet. Det är ledningens ansvar att involvera och engagera sig i arbetet med att upprätta säkerhetspolicys samt definiera ansvarsroller i verksamheten som säkerställer efterlevnad. (Leveque, 2006)

2.2 Policy

Majoriteten av standarder och internationella ”best-practices” understryker faktumet att en informationssäkerhetspolicy (ISP) är hjärtat och grunden i samtliga organisationers informationssäkerhetsarbete. Den policyn utgör grunden som kommande sub-policys, procedurer och standarder måste baseras på. Von Solms & Von Solms (2004) menar att den policyn ska undertecknas av den verkställande direktören för att visa organisationens engagemang mot informationssäkerhet. (Von Solms & Von Solms, 2004)

En ISP utgör en verksamhets säkerhetsprogram och är ett eller flera styrdokument med riktlinjer för säker informationshantering i en organisation. Dokumentet beskriver vad användaren i organisationen är beviljad att göra och inte göra med en viss informationsresurs (Leveque, 2006; Bulgurcu et al., 2010). Riktlinjerna är tänkta att skydda resurser i form av information

genom att förhindra oberättigat användande (Gollmann, 2011). Enligt Whitman & Mattord (2011) är en ISP baserad på en organisations mål och vision, samt har i uppgift att stödja dessa, men också vara vägledande och ligga till grund för en organisations omfattning och strategiska inriktning av informationssäkerhetsarbete.

En ISP bidrar väsentligt till en organisations informationssäkerhetsarbete men processen att framställa samt implementera en ISP är oftast komplicerad. Flertalet aspekter behöver tas i hänsyn vid utformande av ISP. Aspekter att ta i beaktning är bland annat teknikutveckling, externa lagar, och interna samt externa hot (Flowerday & Tuyikeze, 2016). En organisation bör undvika att upprätta en ISP som i lösa begrepp endast förespråkar vikten av informationssäkerhetsarbete (Leveque, 2006). Bristande förståelse för hur policyn ska utformas riskerar ge resultat i form av en ogenomtänkt, ofärdig och bristfällig slutprodukt. Utöver att ISP:n är undermålig i sig riskerar då även graden av efterlevnad att påverkas negativt (Flowerday & Tuyikeze, 2016).

ISP är dokumentation från ledningsnivå som oftast upprättas av organisationens CIO eller i samarbete mellan denne och antingen extern eller intern hjälp. Policyns utformning varierar beroende på verksamheten men bör innehålla en översikt av organisationens säkerhetsstrategi, information om strukturen i informationssäkerhetsarbetet, nyckelpersoner som har betydelse för informationssäkerhetsarbetet, tydligt definierade ansvarsområden för personer som verkar i organisationen och tydligt definierade ansvarsområden för nyckelpersoner i arbetet (Whitman & Mattord, 2011; Leveque, 2006). För att policyn sedan ska vara verksam måste den distribueras i organisationen till dem som kommer att beröras av den. En bra förmedling innebär att anställda läser och förstår policyn. (Whitman & Mattord, 2011) Som andra viktiga dokument så måste organisationen säkerställa att policyn är aktuell (Leveque, 2006). Policydokument är något som måste granskas och ses över under hela dess livslängd för att säkerställa att policyn lever upp till externa och interna krav. Detta gäller såväl offentliga som privata organisationer. En översyn och revidering av policyn bör ske årligen. Den som är ansvarig för policyarbetet bör vid revision lyssna till anställdas åsikter om policyn och dess innehåll. (Whitman & Mattord, 2011)

För att säkerställa att anställda efterlever policyn kan en organisation i anställningsfasen kräva att den nyanställde skriver under ett dokument som intygar att denne har tagit del av, förstått och samtycker till att efterleva policyn. Det är dock svårare för en organisation att hantera fall där en befintligt anställd motsätter sig policy och vägrar ge ett skriftligt samtycke. (Whitman & Mattord, 2011) Vidare är det kritiskt för en organisation att deras anställda upplever policyn som legitim. Upplevd legitimitet syftar till den grad anställda ser ISP’s som lämplig, önskvärd och rättvis. Son (2011) menar att en ISP’s upplevda legitimitet har ett positivt inflytande på efterlevnaden. Sådan legitimitet uppnås när en organisation lyckas kommunicera vikten av att följa den.

2.3 Mänskliga faktorn

Till skillnad från människor så utför datorer arbetsuppgifter konsekvent utifrån de anvsiningar de är tilldelade. Människor begår misstag, lämnar större utrymme för att tolka anvisningar, kan ta genvägar och kan rationalisera bort moment som den enskilde individen inte bedömer vara nödvändiga för uppgiften. På grund av detta uppstår ofta en säkerhetsrisk gällande informationshantering när människor interagerar med datorer (Kearney, 2010). Den mänskliga

faktorn är idag en av de största säkerhetsriskerna när det kommer till en organisations informationshantering (Whitman & Mattord, 2011).

För en organisations information kan människor både ses som hot och risk. Peltier (2005a) skriver att den mänskliga faktorn bör delas upp i två undergrupper av ”illvilliga” och ”icke illvilliga”. Undergruppen av illvilliga är oftast externa hot i form av människor som med ont uppsåt medvetet utgör ett säkerhetshot för organisationens information. Hotet behöver inte vara externt, det kan även vara en illvillig anställd i organisationen (Peltier, 2005a). Den andra gruppen av icke illvilliga består oftast av de egna anställda i organisationen och som utan ont uppsåt kan vara en säkerhetsrisk.

Peltier (2005a) skriver att en medveten attack av ont uppsåt kan vara ett försök att komma åt information i ett system denne inte har beviljats tillgång till genom att gissa sig till ett lösenord eller forcera en inloggning. En illvillig attack av ont uppsåt behöver inte vara av teknisk karaktär, utan kan också innebära ett försök till att få obehörig åtkomst till information genom att medvetet använda någon annan på arbetsplatsens lösenord. En illvillig person som med ont uppsåt försöker kompromettera informationssäkerheten i en organisation i syfte att få tillgång till information utan att ha behörig åtkomst, kommer enligt Kearney (2010) försöka ta den enklaste vägen. Det enklaste tillvägagångssättet är att utnyttja den mänskliga faktorn hos anställda i organisationen och genom manipulation eller utnyttjande av anställdas misstag få behörighet till system och dess information. Anledningen till att anställda begår misstag och kan manipuleras beror oftast på avsaknad av utbildning eller brister i utformandet av antingen arbetsrutiner eller tekniken i sig (Kearney, 2010).

Den mänskliga faktorn innebär att anställda kan begå misstag eller vara oaktsamma på grund av bristande förståelse för vad deras handlingar har för påföljder för organisationens informationshantering. Oaktsamt agerande vid hantering av information kan bland annat resultera i att felaktig data registreras, information lagras felaktigt, information felaktigt modifieras eller raderas och att sekretessbelagd information avslöjas. Om sekretessbelagd information hanteras felaktigt genom att exempelvis förvaras oskyddat på en anställds skrivbord så utgör det en minst lika stor säkerhetsrisk som den personen med ont uppsåt som försöker komma över och utnyttja informationen. Eftersom att anställda dagligen arbetar med organisationens information utgör de en av de större säkerhetsriskerna. En icke illvillig anställds oaktsamhet ger en illvillig person ett tillfälle att exploatera informationen (Whitman & Mattord, 2011).

Att anställda skriver ner sina lösenord på lappar, glömmer hårddiskar på offentliga ställen och pratar om känsliga uppgifter publikt beror enligt Kearney (2010) på naivitet. Allt som oftast finns inget ont uppsåt hos en anställd som oaktsamt begår ett misstag. Oaktsamheten beror vanligtvis på dåligt säkerhetsmedvetande, dåligt prioriterande, oförståelse eller ren okunskap om vilka konsekvenser handlingarna innebär för organisationen. Likaså skriver Leveque (2006) att följandet av säkerhetsrutiner kan försvåra eller komplicera arbetet för den anställde samtidigt som fördelarna med att följa rutinerna är svårförståeliga. Bra styrning från ledningsnivå hjälper till att säkerställa att säkerhetsrutiner följs och att säker informationshantering prioriteras över arbetsrutinernas enkelhet.

2.4 Informationssäkerhetsmedvetenhet

Informationssäkerhetsmedvetenhet (Information Security Awareness, ISA) syftar till ett tillstånd där anställda i en organisation är medvetna om deras säkerhetsansvar (Siponen, 2000). Siponen (2000) anser att ISA är oerhört viktigt eftersom säkerhetslösningar och procedurer kan misstolkas, missbrukas eller ignoreras, vilket resulterar i att lösningarna förlorar sin funktionalitet.

Bulgurcu et al. (2010) beskriver ISA som en anställds allmänna kunskap och förståelse gällande informationssäkerhetsprogem och dess komplikationer. Informationssäkerhetspolicy medvetenhet (ISPA) kan ses som en underkategori till ISA, och ISPA beskrivs som en anställds kunskap och förståelse kring innehållet i organisationens ISP. Nödvändigtvis behöver det ej finnas en relation mellan ISA och ISPA, och de kan därför ses enskilt. Till exempel, en anställd kan vara medveten om att organisationen har en ”clean desk” policy utan att förstå varför. Vice versa kan en anställd förstå syftet med en sådan policy utan att ha medvetenhet om att en sådan policy inrättats.

Anställdas medvetenhet skapas av tidigare erfarenheter, till exempel att man skadas av virus, eller genom att ha orsakat en säkerhetsincident på arbetsplatsen som uppmärksammades. Det bildas också från externa kunskapskällor som nyhetsartiklar, policydokument och utbildningsprogram (Bulgurcu et al., 2010).

Ökad ISA bör minska användarfel och samtidigt förbättra effektiviteten av säkerhetslösningar. För att lyckas med detta måste orsakerna till användarfelen identifieras och kvantifieras (Siponen, 2000). Vidare rekommenderar Bulgurcu et al. (2010) att organisationer skapar säkerhetsträning och medvetenhetsprogram för att säkerställa att anställda följer ISP.

2.5 Informationssäkerhetsprogram

Det är vanligt förekommande att organisationer implementerar ett gediget informationssäkerhetsprogram som senare misslyckas. För att lyckas måste organisationen hitta ett sätt att sälja in informationssäkerhet hos de anställda. Ett informationssäkerhetsprogram måste ta hänsyn till organisationens mål och säkerställa att de målen kan uppnås på ett så säkert sätt som möjligt. Lärande består av tre element, medvetenhet, träning och utbildning, och ett säkerhetsprogram bör inkorporera dessa (se figur 2.2). Ett informationssäkerhetsprogram grundas på organisationens policys, standarder och procedurer, och Peltier (2005b) menar att de flesta anställda varken har tid eller viljan att läsa igenom de dokumenten. Syftet med ett ISA-program är att leverera den informationen direkt till de anställda (Peltier, 2005b).

2.5.1 ISA-program

Anställdas beteende bör formas så att de kan utföra sitt dagliga arbete på ett sätt som ligger i linje med informationssäkerheten. Det är viktigt att detta beteende blir en del av anställdas undermedvetna. Till exempel, att de instinktivt loggar ur sitt användarkonto när de går från jobbet. För att åstadkomma detta kan ett ISA-program hjälpa. Ett ISA-program utbildar användare om informationssäkerhetsproblem. Programmet bör också påminna användarna kontinuerligt om dessa problem och nya problem som uppkommit. Målet med ett ISA-program är

att förändra anställdas tankar och beteende. Därför måste ISA-programmet vara strukturerad på ett sådant sätt att anställdas beteende och attityder kan förändras. (Thomson & Von Solms, 1998)

Ett ISA-program kan omöjligen passa en organisations samtliga avdelningar. Detta kräver att programmet anpassas utefter deras olika behov. Genom att kommunicera med respektive avdelningschefer och anställda kan deras specifika behov kartläggas. Det är också viktigt att betona hur programmet kommer hjälpa avdelningen att uppnå sina mål på ett säkert tillvägagångssätt. Nya policys och säkerhetsåtgärder bör inte heller implementeras utan deras vetskap. Sådana förändringar bör diskuteras så att samtliga förstår dess innebörd och varför de är nödvändiga (Peltier, 2005b). Sedermera bör ett ISA program differentiera mellan olika grupper och individer för att endast tillhandahålla information som är relevant för den publiken. Alla behöver inte samma typ av ISA för att kunna uträtta sitt jobb på ett säkert sätt (Awawdeh & Tubaishat, 2014).

Aktiviteter i ett ISA-program kan inkludera föreläsningar, informationsblad, säkerhetsposters, videos, och diskussionsforum. Informationsbladet är den mest kostnadseffektiva metoden för att sprida ISA. Dessa kan delas ut, mailas eller uppvisas på intranätet. Själva innehållet kan inkludera information om nya hot och schema för uppkommande träningsworkshops (Whitman & Mattord, 2011; Peltier, 2005b).

2.5.2 Träningsprogram

Säkerhetsträning är en process där anställda lär sig olika färdigheter och att använda verktyg nödvändiga för deras arbete (Peltier, 2005b). Utav samtliga åtgärder för efterlevnad av ISP är säkerhetsträning en av de mest förekommande rekommendationerna. Puhakainen & Siponen (2010) menar att säkerhetsträning är till för att aktivera och förändra anställdas tankegång, vilket leder till att anställda förstår anledningarna till varför de ska följa ISP. Säkerhetsträning bör ta hänsyn till anställdas tidigare kunskaper om efterlevnad av ISP, och under träningssessionerna bör anställda delas in i träningsgrupper utefter deras kunskap. Vidare är det viktigt att träningen inkorporerar träningsuppgifter som är relevanta för de anställdas arbete eftersom det hjälper till att synliggöra konsekvenserna av deras handlingar (Puhakainen & Siponen, 2010).

Träning kan ske på flera sätt; genom att läsa böcker om ämnet, titta på träningsvideor eller ha någon som demonstrerar hur det ska göras. Fördelen med det sistnämnda är att en närvarande demonstratör finns tillgänglig för att svara på eventuella frågor (Peltier, 2005b). Awawdeh & Tubaishat (2014) rekommenderar att organisationer anordnar träningsworkshops internt snarare än att säkerhetsträningen outsourcas. Internt medför fler fördelar än outsourcing, det är billigare och underlättar för personalen då träningssessionerna kan ta plats i organisationens egna lokaler.

2.5.3 Vidareutbildning

Utbildning är en mer specialiserad och djupgående kunskap som krävs för att vägleda informationssäkerhetsarbetet och för att stödja träningsverktygen. Utbildning innebär formella utbildningar på universitet och relevanta certifikat inom informationssäkerhet, snarare än workshops vilket används för träning. Det är viktigt att informationssäkerhetspersonal utvecklar sin kompetens kontinuerligt (Whitman & Mattord, 2011; Peltier, 2005b).

	Education	Training	Awareness
Attribute	Why	How	What
Level	Insight	Knowledge	Information
Objective	Understanding	Skill	Exposure
Teaching	Theoretical instruction	Practical instruction	Media
method	• Discussion seminar	• Lecture	• Videos
	• Background reading	• Case study workshop	• Newsletters
	• Hands-on practice	• Posters	
Test measure	Essay (interpret learning)	Problem solving (apply learning)	• True or false • Multiple choice (identify learning)
Impact timeframe	Long term	Intermediate	Short term

Figur 2.2: Comparative Framework of SETA från NIST SP 800-12 (Whitman & Mattord, 2011, s. 209)

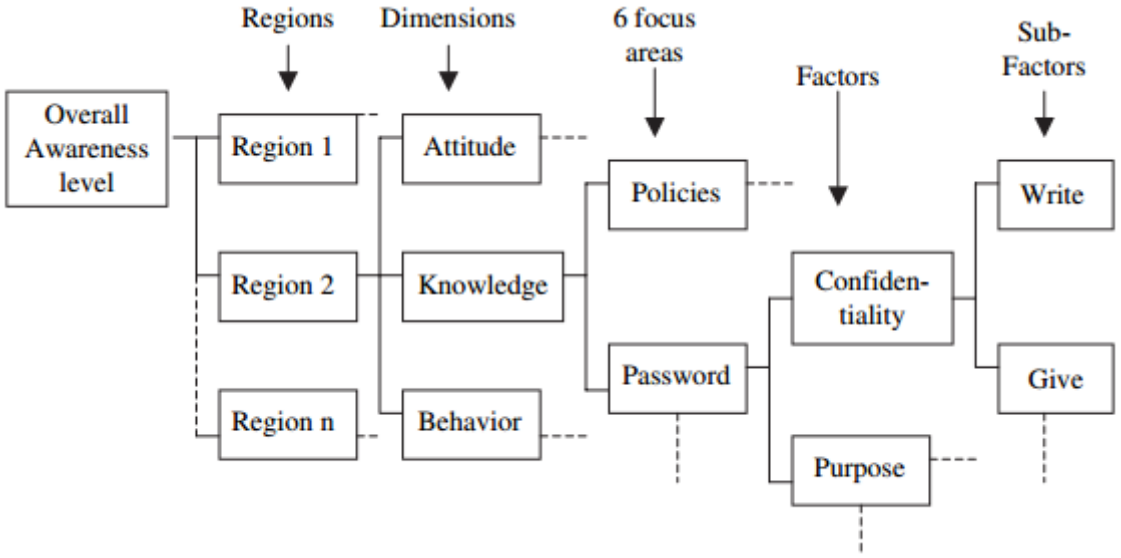
2.6 Mätning

Ett omfattande ISA-program behöver nödvändigtvis inte innebära att medvetenhetsnivån ökar (Kruger & Kearney, 2006; Bulgurcu et al., 2010). Genom att mäta anställdas ISA går det att utvärdera om ISA-programmet faktiskt bidrar med nytta (Sherif et al., 2015; Kruger & Kearney, 2006). Utöver det ger mätning en fingervisning om vilka avdelningar eller informationssäkerhetsområden som är i behov av extra uppmärksamhet. Mätningsdata kan även vara underlag till förbättringsinsatser av ISA-programmet (Kruger & Kearney, 2006).

Kruger och Kearney (2006) har framställt en metod för att mäta ISA-nivån inom en organisation. Det som mäts grundas i tre mänskliga aspekter; kunskap, attityd och beteende. Tillsammans utgör dessa en individs förutsättning att antingen agera positivt eller negativt gällande ett objekt.

- Kunskap – Vad individen vet.
- Attityd – Vad individen tänker.
- Beteende – Vad individen gör.

Initialt behövs det identifieras vilka nyckelfaktorer och fokusområden som kan ligga till underlag för utvärderingen. De rekommenderar att skapa ett värde-träd (se figur 2.3) eftersom det underlättar identifiering av nyckelfaktorer, fokusområden, och deras hierarkiska kartläggning. Exempelvis kan lösenord vara ett fokusområde; det kan delas upp i ”konfidentialitet av lösenord” och ”syfte med lösenord”. Dessa kan i sin tur delas upp ytterligare. I detta steg är det också viktigt att bedöma varje faktors enskilda inflytande på medvetenheten (Kruger & Kearney, 2006).



Figur 2.3: Värde-träd Mätning (Kruger & Kearney, 2006, s. 292)

Själva mätningen kan genomföras med hjälp av enkäter bestående av öppna frågor och flervalsfrågor. Det är viktigt att inse att mätningen nödvändigtvis inte är korrekt, då enkätrespondenter kan ljuga. Den risken är större gällande beteende frågorna. Oavsett ger resultatet en fingervisning om anställdas ISA och beteende. Metoden bör digitaliseras, programmet kan då automatiskt sammanställa data och det underlättar jämförelser med tidigare mätningar. På så sätt kan en organisation se ISA utvecklingen över tid. De rekommenderar också att en frågebank skapas, på så sätt kan programmet variera vilka frågor som ställs vid olika mätningar. Dessutom försvårar det för anställda att memorera frågorna och deras ”korrekta” svar. Mätningresultatet kan även hjälpa ledningen att sätta och följa upp informationssäkerhetsstrategiska mål (Kruger & Kearney, 2006).

2.7 Övervakning och utvärdering

2.7.1 Övervakning

Enligt Von Solms & Von Solms (2004) finns det ingen anledning att ha välformulerad ISP om det inte är möjligt att övervaka efterlevnaden av dem. Säkerhetschefer behöver både tekniska och icke tekniska verktyg för att mäta och övervaka efterlevnaden av ISP, så att de kan agera om en policy överträtts. Övervakningsverktygen måste ge information i realtid då information om en policyöverträdelse som inträffade för flera månader sedan inte alls är lika relevant. Utan övervakning finns det risk för att en organisation bildar en känsla av falsk trygghet (Von solms & Von solms, 2004). Övervakningstekniker omfattar bland annat elektronisk övervakning av e-post, internetanvändning och nätverksaktivitet. Det har visats att övervakning kan avskräcka anställda från att kringgå regler eftersom det ökar sannolikheten att gärningen upptäcks (D’arcy et al., 2009). Övervakningsresultatet behövs sedan utvärderas (Von solms & Von solms, 2004).

Spitzmüller & Stanton (2006) menar att övervakningsinsatser kan möta motstånd och ge motsatt effekt. Motreaktioner kan vara att anställda går över till otillåtna epostsystem, undviker eller modifierar arbetsutrustning och struntar i att rapportera regelöverträdelser. Deras studie fann att anställda som är hängivna till organisationen är mindre motståndsfulla till övervakning. Dock är det de individer som är i minst behov av övervakning eftersom deras värderingar i större grad redan ligger i linje med organisationens. Det är rekommenderbart att bemöta motståndet med träning och kommunikation som förmedlar varför övervakning är nödvändigt (Spitzmüller & Stanton, 2006).

Övervakning medför flera utmaningar som ledningen måste ta hänsyn till, de måste bestämma hur den insamlade informationen ska dokumenteras och lagras, samt analysera hur övervakningen kan komma att påverka organisationens övergripande produktivitet. Dessutom är det dyrt, framförallt för stora organisationer. Det innebär ökade utgifter för hårdvara, mjukvara, installation, och för den personal som har i uppgift att upprätthålla systemet. (Young, 2010) Young (2010) nämner att organisationer allt för ofta väljer en billig och underlägsen övervakningslösning som inte tillfredsställer övervakningsbehovet, vilket i slutändan resulterar i kostsamma uppgraderingar. Det är viktigt att välja den övervakningslösning som ger mest nytta för pengarna. Samtidigt hävdar D'arcy et al. (2009) att organisationens generösa hängivenhet av resurser till övervakning kan uppfattas som en varning.

2.7.2 Utvärdering

Utvärdering handlar i grunden om att leta igenom och granska insamlad data i syfte att bedöma en individs efterlevnad av de riktlinjer som existerar (Boss et al., 2008). Whitman & Mattord (2011) menar att sådan utvärdering bidrar till ökad ISA och minimerar riskfyllt beteende. Därför bör organisationer inkorporera informationssäkerhetsaspekter i anställdas generella utvärderingssamtal. Exempelvis, om en anställd har observerats bryta mot en ISP bör denne bli varnad, och om beteendet fortsätter bör det diskuteras under vederbörandes utvärderingssamtal. Överlag tenderar anställda att ta sådana samtal seriöst, och de blir mer motiverade att ändra sitt beteende om det icke-sanktionerade beteendet finns dokumenterat i utvärderingen. Talib (2015) beskriver utvärderingar som ett socialt tryck som influerar anställda att anpassa sig till organisationens önskvärda beteende.

2.7.3 Sanktioner

En sanktion beskrivs som en negativ stimulans eller incitament för att motverka individer från att genomföra särskilda handlingar eller fatta beslut som inte ligger i linje med organisatoriska mål. En sanktion delas upp i två underkategorier: övertygelse och allvarlighet. Övertygelse refererar till sannolikheten att en anställd åker fast, och allvarlighet refererar till straffets stränghet om den anställde åker fast. Sanktioner förutsätter att människor är rationella, och därav är det mindre troligt att anställda bryter mot ISPs om de vet att sannolikheten att åka fast är stor och att straffet är strängt (Talib, 2015).

2.7.4 Belöningar

En belöning är en positiv stimulans vars mål är att uppmuntra samstämmighet med de beteenden en organisation ser som önskvärda. Belöningar delas upp i två underkategorier, greppbara och ogreppbara. Greppbara omfattar belöningar som bonus, priser och diplom, medan

ogreppbara omfattar beröm, utökat förtroende och befordringar. Undersökningen av Bulgurcu et al. (2010) visar att anställda uppmuntras att följa ISP om de är tillräckligt motiverade av belöningar. Belöningar signalerar till anställda att efterlevnad av ISP är viktigt. Utan belöningar finns det en risk att ISPs ses som oviktigt (Talib, 2015).

2.8 Teoretiskt ramverk

Utifrån litteraturgenomgången identifierade vi flera åtgärder som kan understödja arbetet för ökad efterlevnad av ISP. Dessa presenteras i tabellen nedan tillsammans med en motivering om varför det är relevant. Kapitlet Informationssäkerhet och Mänskliga faktorn är ej inkluderat då deras syfte var att bidra med nödvändig bakgrundsförståelse om vårt problemområde. Detta teoretiska ramverk kommer ligga till grund för vår empiriinsamling.

Tabell 2.1: Teoretiskt ramverk

Område	**Åtgärder**	**Varför**	**Stycke**	**Referenser**
Policy	Skapa och underhålla policyn under dess livscykel. Förankra policyn i organisationen.	Policyn måste vara lättförståelig och relevant för att upplevas som legitim.	2.2	Flowerday & Tuyikeze, 2016 Leveque, 2006 Son, 2011 Von Solms & Von Solms, 2004 Whitman & Mattord, 2011
Informationssäkerhetprogram	Etablera ett informationssäkerhetsprogram som tillförser anställda med relevant kunskap.	Ökar ISA och förbättrar anställdas färdigheter att hantera informationssäkerhet och ISP. Utökar IS-ansvariges kompetens.	2.6	Awawdeh & Tubaishat, 2014 Peltier, 2005b Puhakainen & Siponen, 2010 Thomson & Von Solms, 1998 Whitman & Mattord, 2011
Mätning	Mäta anställdas kunskap, attityd och beteende gällande informationssäkerhetsfrågor.	Mätningsunderlaget ger en indikation om både säkerhetsprogrammets effektivitet och anställdas ISA.	2.7	Kruger & Kearney, 2006

Övervakning	Implementera övervakningsverktyg.	Gör det möjligt att granska efterlevnaden och utvärdera anställdas beteenden. Kan ha en avskräckande effekt.	2.8.1 2.8.2	D'Arcy et al., 2009 Spitzmüller & Stanton, 2006 Talib, 2015 Von Solms & Von Solms, 2004 Whitman & Mattord, 2011 Young, 2010
Utvärdering	Inrätta regelbunden utvärdering av anställdas säkerhetsbeteende och ISP efterlevnad.	Influerar anställdas beteenden.	2.7.2	Boss et al., 2008 Talib, 2015 Whitman & Mattord, 2011
Sanktioner	Inrätta sanktioner för anställda vid ISP överträdelser.	Anställda tenderar att undvika ett beteende om straffet för det beteendet är stort, eller om chansen att åka fast är stor.	2.8.3	Talib, 2015
Belöningar	Upprätta ett belöningssystem för gott säkerhetsbeteende och efterlevnad av ISP	Anställda tenderar att arbeta enligt organisationens riktlinjer om det resulterar i belöningar	2.8.4	Bulgurcu et al., 2010 Talib, 2015

3 Metod

I detta kapitel presenterar vi vårt metodval och tillvägagångssätt för insamling och bearbetning av empiri. Vi resonerar även kring uppsatsen validitet och reliabilitet för att slutligen beskriva de etiska aspekter vi beaktat under empiriinsamlingen.

3.1 Metodval

Utifrån vår frågeställning med tillhörande avgränsning inleddes en litteraturstudie som ämnade belysa tidigare forskning på området ISP och de åtgärder som influerar dess efterlevnad. Litteraturstudien baserades på publicerade artiklar och böcker som behandlar detta ämne. Utifrån litteraturstudien skapade vi ett teoretiskt ramverk avsett att ligga till grund för den kommande empiriinsamlingen. Eftersom vi inte besatt några tidigare kunskaper inom området fanns det också ett behov av flexibilitet. Med det menar vi en möjlighet att uppdatera litteraturstudien och vårt teoretiska ramverk i takt med att vi lär oss mer från insamlad empiri. Kvalitativa metoder kännetecknas av sådan flexibilitet (Jacobsen, 2002).

För att besvara vår forskningsfråga ”Hur arbetar IS-ansvarige med policys och dess efterlevnad?” så krävs det ett samtal med en IS-ansvarig. Jacobsen (2002) menar att kvantitativa metoder riskerar att endast mäta frågor som undersökaren själv anser vara relevanta. En enkätundersökning hade låst våra respondenter till fasta svarsalternativ utifrån vår litteraturstudie. Besvarandet av forskningsfrågan kräver detaljrik och djup information som ej går att bryta ned till fasta svarsalternativ. Vi behöver sådan information för att kunna beskriva hur de faktiskt arbetar. Vidare hoppas vi kunna identifiera nya tillvägagångssätt och metoder, både gällande policyarbete och åtgärder för att öka dess efterlevnad, som tidigare forskning ej belyst. Båda dessa punkter förutsätter att vi sätter så få begränsningar som möjligt över de svar vi samlar in. Enligt Jacobsen (2002) är en kvalitativ metod mer öppen för oförväntade svar.

Med vår forskningsfråga i åtanke beslöt vi oss för en kvalitativ undersökningsmetod där empirin kom att insamlas via öppna individuella intervjuer. Enligt Jacobsen (2002) är denna typ av intervju passande när forskare är intresserade av vad en specifik individ säger. Vi anser att denna typ av undersökning lämpar sig väl för att undersöka hur IS-ansvariga arbetar med ISP och dess efterlevnad.

3.2 Urval av organisationer och informanter

Urvalsprocessen för val av organisationer och informanter utgick ifrån vår frågeställning. Det yttersta kravet var att den blivande informantens arbetsroll omfattade ett övergripande informationssäkerhetsansvar. Idealt vore om informanten primärt arbetade med informationssäkerhet och efterlevnad av policys. Tidigt i urvalsprocessen insåg vi att få organisationer har en sådan anställd, och att det ansvarsområdet ofta faller på IT-chefen.

Ännu ett krav var att informantens organisationsstorlek skulle vara medelstor till stor. Vi misstänkte att små organisationer sällan har resurser eller behov att arbeta lika aktivt med dessa frågor. Då organisationer ofta förlitar sig på extern kompetens för att vägleda informationssäkerhetsarbetet valde vi att göra ett undantag för mindre konsultfirmor verksamma inom IT och informationssäkerhet. Bortsett från konsultfirmor hade vi ingen preferens om organisationens bransch och kärnverksamhet, förutsatt att de passade in på det ovanstående kriteriet. Det valet grundade sig i antagandet att samtliga organisationer som hanterar information bör ha åtgärder för att skydda den. Vi är medvetna om att olika organisationstyper har olika externa krav att leva upp till och att det kan förklara varför de arbetar som de gör. Men vi anser att en inkludering av olika organisationstyper kan ge upphov till att fler synvinklar belyses.

Två av de tre informanterna blev vi hänvisade till av personer i vårt kontaktnät. Den övriga informanten blev vi hänvisade till av dennes organisations växel. Vi ansåg att samtliga informanters befattning och organisation föll inom urvalsprocessens kriterier. I vår initiala kontakt med informanterna uppgav vi jämlik information om undersökningens ändamål. Detta för att säkerställa att informanternas val att delta utgick från samma information.

Informanterna ställde olika krav på anonymitet. För att försvåra deras identifiering fann vi det nödvändigt att anonymisera samtligas uppgifter. Nedan presenteras informanterna och deras organisation.

Tabell 3.1: Urval av organisationer och informanter

Organisation	**Organisations beskrivning**	**Antal anställda**	**Informant**	**Arbetsroll**
Organisation A	Nationell koncern inom media och journalistik	700–1000	INF1	IT-chef med informationssäkerhetsansvar.
Organisation B	Kommun bestående av ett stadskontor och ett flertal förvaltningar	15000–30000	INF2	Informationssäkerhetssamordnare.
Organisation C	Konsultfirma med fokus på strategisk rådgivning inom IT	5–15	INF3	Delägare. IT-chefs-konsult med övergripande ansvarsområde.

3.3 Intervju

En intervju skedde ansikte mot ansikte, och de resterande över telefon. Initialt planerade vi att genomföra samtliga intervjuer i person då de är mer lämpade för kvalitativa undersökningar (Jacobsen, 2002). Men till följd av de andra informanternas olika geografiska befinnande blev vi tvungna att förlita oss på telefoni för att på kort varsel få kontakt med dem.

Den personliga intervjun genomfördes i informantens kontor på dennes önskemål. Enligt Jacobsen (2002) har personer lättare att öppna upp i intervjuer som sker ansikte mot ansikte. Det skapar en förtrolig stämning som är svår att uppnå i en telefonintervju. Under en telefonintervju förlorar intervjuaren också möjligheten att observera informantens kroppsspråk. Sådan observation kan ge en indikation ifall informanten känner sig besvärad av ämnet, eller om ämnet ifråga bör utforskas mer (Jacobsen, 2002).

Under intervjuerna deltog vi båda aktivt genom att ställa frågor och följdfrågor till informanten. Om en av oss mot förmodan skulle missa ett tillfälle att ställa en relevant följdfråga kunde den andra snabbt flika in. Vi spelade in samtliga intervjuer istället för att förlita oss på anteckningar under samtalets gång. På så sätt kunde vi få med all information som informanten delade med sig utav. Det fick också samtalet att flyta mer naturligt eftersom vi kunde fokusera på samtalets utveckling och atmosfär snarare än att anteckna det som sades. Enligt Jacobsen (2002) är det ofta är problematiskt att anteckna under samtalets gång.

Vi utformade en semistrukturerad intervjuguide med tydliga teman som innehöll en blandning av både öppna och mer direkta frågor (se bilaga 1). Enligt Jacobsen (2002) bör en intervju inte vara så strukturerad att den består av i förväg bestämda frågor, och inte heller vara öppen utan någon form av struktur. Intervjuguiden baserades på vårt teoretiska ramverk och den hjälpte oss säkerställa att alla undersökningsfrågor faktiskt behandlades under intervjun. Genom att ställa öppna frågor kunde informanten belysa de områden denne ansåg viktigast ur ett efterlevnads perspektiv. Beroende på informantens svar anpassade vi oss till det temat. Intervjufrågorna ställdes således inte i en kronologisk ordning. Somliga frågeformuleringar möjliggjorde det för informanten att bidra med övriga tillvägagångssätt och metoder utanför vårt teoretiska ramverk. Intervjuguiden var ett levande dokument som uppdaterades i takt med att vi lärde oss mer om ämnet.

Innan intervjun påbörjades presenterade vi oss själva och förklarade undersökningens syfte. I detta stadie bad vi om tillstånd att spela in samtalet och förklarade att ljudinspelningen kommer raderas efter att transkriberingen färdigställts. Intervjun inleddes med allmänna frågor om informantens befattning och ansvarsområde, och gick därefter in på frågor rörande vårt problemområde. Under samtalet försökte vi skapa en god atmosfär genom att visa intresse både verbalt och fysiskt. Avslutningsvis frågades det om informanten hade något mer att tillägga. Intervjuguiden följdes inte exakt och frågorna omformulerades för att passa in i sammanhanget.

3.4 Bearbetning av data

Direkt efter att intervjun var genomförd transkriberade vi samtalet samtidigt som vi antecknade nyckelord i kommentarsfältet. Varje kommentar refererade till ett ämnesområde i vårt teoretiska ramverk. Transkriberingarna fångade upp allting informanten nämnde vilket gjorde

det möjligt för oss att lyfta in ordagranna citat i resultatpresentationen. Dessa två faktorer kom att underlätta kategoriseringen och presentationen av vår insamlade empiri. Jacobsen (2002) anser att transkribering är mödosamt. Med tanke på vårt begränsade antal intervjupersoner ansåg vi att transkribering var optimalt framför anteckningar. I transkriberingen har information som eventuellt kan härleda till informantens identitet eller organisation korrigerats.

Samtliga transkriberingar finns tillgängliga som bilagor.

- INF1 transkribering finnes i bilaga 2
- INF2 transkribering finnes i bilaga 3
- INF3 transkribering finnes i bilaga 4

3.5 Kvalitetsaspekter

3.5.1 Validitet

I vår strävan att uppnå god intern validitet har vi jämfört vår slutsats mot tidigare forskning. Jacobsen (2002) skriver att det närmsta vi kan komma sanningen är om flera personer är ense om hur något ska beskrivas. Det har varit svårt att hitta publicerad forskning som behandlat samma ämne ur vårt perspektiv, men det finns liknande forskning som kunnat ge en indikation på vår slutsats validitet.

För att säkerställa att vår insamlade empiri möter kravet på validitet har vi endast intervjuat informanter som antingen är informationssäkerhetsansvariga eller IT-ansvariga vars ansvarsområde också omfattar informationssäkerhet. Innan intervjugenomförandet beskrev vi intervjuns tema så informanterna kunde ta ställning till om de besatt rätt kunskaper. Genom att ha semistrukturerade intervjuer med intervjufrågor baserade på vårt teoretiska ramverk kunde vi kontrollera att vi faktiskt samlade in data som var relevant för vår forskningsfråga.

Vår empiri samlades in under olika tidpunkter. Det medförde att vi mot slutet av undersökningsprocessen hade en tydligare bild om vårt problemområde och en klarare uppfattning om vad för information vi sökte från informanterna. Jacobsen (2002) menar att data som samlas in mot slutet ofta är den bästa, och att detta kan ha en betydelse för undersökningens validitet.

Gällande extern validitet understryker Jacobsen (2002) att avsikten med kvalitativa metoder överlag inte är att överföra eller generalisera insamlad empiri till en större grupp. Jacobsen (2002) tillägger att om en synpunkt återkommer från flera informanter, så kan den synpunkten vara generaliserbar (Jacobsen, 2002). Dock anser vi att undersökningen har för få intervjuobjekt för att resultatet ska kunna vara överförbart. Därav är det svårt för undersökningen att uppnå god extern validitet.

3.5.2 Tillförlitlighet

Jacobsen (2002) beskriver att undersökningsmetoden influerar datainsamlingen. Vid intervjuer och analysarbetet finns det flera faktorer att beakta för att säkerställa god tillförlitlighet. Under besöksintervjun försökte vi minska intervjuareffekten genom att vara neutralt klädda, inta lyssnar ställning och visa intresse och engagemang under samtalets gång. Telefonintervjuer minimerar intervjuareffekten, dock påverkar andra faktorer dess tillförlitlighet (Jacobsen, 2002). Jacobsen (2002) menar att det är lättare för intervjuobjekt att ljuga under en telefonintervju.

Utöver det kan kontexteffekten påverka datainsamlingen. Vi försökte motverka detta genom att låta intervjupersonerna själva bestämma intervjuplats. Vid besöksintervjun genomfördes intervjun på informantens arbetsplats. Vid telefonintervjuerna hade vi dock ingen kontroll över informanternas val av plats. En informant körde bil samtidigt som intervjun ägde rum, det kan ha varit en konstlad miljö för denne.

Slarv vid nedteckning och analys av data beskriver Jacobsen (2002) som det sista hotet mot tillförlitligheten. Som tidigare nämnt spelades samtalet in och transkriberades, detta gav oss en komplett återgivning av samtalet som säkerställde att ingen data gick oregistrerad vid insamlandet. Transkriberingarna finns tillgängliga i form av bilagor, vilket ger läsaren möjlighet att granska vår presentation av empiri.

3.6 Etik

Jacobsen (2002) nämner tre etiska krav som bör beaktas av forskare. Kraven är informerat samtycke, rätt till privatliv och kravet på riktig presentation av data. Under undersökningens gång har vi strävat att uppnå dessa krav.

Informerat samtycke förutsätter att undersökningspersonen frivilligt ställer upp på en undersökning, samt att personen är medveten och förstår vilka risker eller vinster som ett undersökningsdeltagande eventuellt kan medföra (Jacobsen, 2002). I vår strävan att uppnå informerat samtycke beaktade vi kravet på full information. I vår inledande kontakt med informanterna berättade vi om uppsatsens syfte och vilka ämneskategorier som frågorna skulle behandla. Innan intervjun genomfördes bad vi om tillstånd att spela in samtalet på en ljudfil, och förklarade att ljudfilen skulle komma att raderas efter den transkriberats. I detta stadie berättade vi även att transkriberingen skulle finnas med som en bilaga i uppsatsen, och att uppsatsen kommer publiceras online av Lunds Universitet.

Undersökningspersoner har rätt till ett privatliv och därför är det viktig att ha i åtanke att informanten eventuellt kan identifieras utifrån insamlad data (Jacobsen, 2002). I samband med intervjuerna frågade vi informanterna hur deras och organisations identitet ska presenteras i uppsatsen. På grund utav varierande svar hos informanterna ansåg vi det bäst att anonymisera bådadera för samtliga.

Tabell 3.1 har medvetet en låg detaljeringsgrad, t.ex. antal anställda presenteras i ett sifferspann. Transkriberingen har redigerats för att försvåra identifieringen av informanten och dennes arbetsgivare. Transkriberingarna skickades också till respektive informant för deras

godkännande. Detta gav dem ett tillfälle att kontrollera att transkriberingen inte innehöll känslig, privat eller missvisande information.

Gällande kravet på riktig presentation av data har vi försökt i den mån det går att återge data korrekt och i rätt sammanhang. Jacobsen (2002) menar att all dataanalys leder till mindre mångfald och detaljrikhet, samt att utbrutna citat kan få en helt annan betydelse om de används i en annan kontext. Därför har vi valt att inkludera transkriberingarna som bilagor.

4 Empiri

I detta kapitel presenteras resultatet av den insamlade empirin. Resultatet presenteras i följande kategorier: policy, informationssäkerhetsprogam, mätning, kontroll och utvärdering samt sanktioner och belöningar. Ett intervjuresultat redogörs åt gången.

4.1 Resultat av intervju 1

Informant 1 (INF1) arbetar som IT-chef och har ansvaret för informationssäkerhet i organisation A. Organisationen är en mediekoncern med 700–1000 anställda som verkar på nationell nivå. Organisationens anställda är främst journalister.

4.1.1 Policy

Företaget har ett flertal policys däribland ISP's som en anställd måste förhålla sig till. Samtliga policys publiceras på deras intranät för de anställda att ta del av. INF1 berättar att *"det är varje anställds skyldighet att känna till vilken IT-policy som gäller"* (bilaga 2, rad 22). Numera har de ett krav att varje anställd ska underteckna ett dokument som kräver efterlevnad av samtliga policys. Det initiativet bemöttes av motstånd och flertalet vägrade att skriva under det. INF1's respons var att *"det spelar ingen roll om du skriver på eller inte, den gäller i alla fall"* (bilaga 2, rad 22).

INF1 och en kollega har ansvaret att utforma IT-policys tillsammans med personalchefsgruppen, som i sin tur ansvarar för hela koncernens personalfrågor. Tillsammans analyserar och diskuterar de policyn för att sedan godkänna den, därefter skickas policyn till koncernledningen för godkännande. INF1 menar att det är nödvändigt *"För att få lite tyngd bakom sig"* (bilaga 2, rad 4).

Förankring av policys sker på ett semi-decentraliserat tillvägagångssätt. Det är upp till varje avdelningschef hur policyn ska förankras i deras avdelningar samt vilka konsekvenser en eventuell policy överträdelse ska resultera i, INF1 säger att IT-avdelningen inte ger några som helst direktiv kring hur de mindre avdelningarna ska sköta policys. INF1 beskriver arbetssättet som *"vi jobbar uppifrån och ner. Vi lämnar över det till någon relativt högt uppe och så får de trycka ut det och gå ut med informationen"* (bilaga 2, rad 81).

4.1.2 Informationssäkerhetsprogram

Företaget har inget övergripande informationssäkerhetsprogram. Anställda säkerhetstränas inte, och företaget lägger ej ned större resurser på att sprida medvetenhet om informationssäkerhetsrisker och om deras ISP. Dock publiceras företagets samtliga policys på deras intranät (bilaga 2, rad 24). INF1 anser att Organisation A överlag blivit mer och mer medveten om både informationssäkerhet och deras policys, trots att inga åtgärder har tagits för att öka med-

vetenheten. De försöker se till att anställda förstår faktumet att lösenord är personligt, samt vikten av att ha lås både på telefon och dator (bilaga 2, rad 34). Om ett visst beteende tyder på okunskap kan det generera en informell utbildningsinsats. Ingen på IT-avdelningen utbildar sig kontinuerligt inom informationssäkerhet, utan de förlitar sig på tidigare utbildning och erfarenheter. INF1 menar att om extra kunskap behövs tar man hjälp utav någon utomstående (bilaga 2, rad 28).

4.1.3 Mätning

Företaget granskas internt av revisorer på en årlig basis. Exempelvis har de en lösenordspolicy innehållandes riktlinjer om hur ofta lösenordet ska bytas samt tecken- och längdkrav. Revisorerna kontrollerar alla konton för att säkerställa att de lever upp till kraven i lösenordspolicyn (bilaga 2, rad 18).

4.1.4 Övervakning och utvärdering

Företaget förlitar sig inte på övervakning i speciellt stor utsträckning, och de har inga övriga kontrollåtgärder för att se om en ISP efterlevs. INF1 säger att *”Vi skulle kunna ha det om vi velat, men nej”* (bilaga 2, rad 52). INF1 ser det som en integritetsfråga. Dock övervakar företaget i viss mån efterlevnaden av IT-policys, exempelvis dataanvändning för företagets telefoner. Endast mängden data övervakas, inte informationen i sig. Det görs ur ett ekonomiskt perspektiv snarare än ett säkerhetsperspektiv (bilaga 2, rad 48).

Rent generellt efterlevs företagets policys, men det förekommer ibland att anställda bryter mot ISP’s. Om en anställd bryter mot policy, omedvetet eller på grund av dålig förståelse så informeras denne av vederbörandes chef. Företaget utvärderar endast anställdas beteende om en incident uppmärksammas. Det har förekommit att de behövt göra efterforskningar när det funnits misstanke om missbruk eller brott (bilaga 2, rad 56).

4.1.5 Sanktioner och belöningar

Det finns inga tydliga sanktioner för anställda som överträder en policy. I deras kommande IT-policy som är under utveckling kommer anställda att hållas ekonomiskt ansvarsskyldiga vid vårdslös hantering av företagstillgångar, exempelvis telefon och datorer. Företaget erbjuder heller inga incitament för att motivera följsamt beteende (bilaga 2, rad 40).

Ur ett datasäkerhetsmässigt perspektiv anser INF1 att motivationstekniker och utbildningsprogram är överflödigt (bilaga 2, rad 75), då INF1 upplever att deras säkerhetsåtgärder är tillräckliga för att hålla informationen säker (bilaga 2, rad 73).

4.2 Resultat intervju 2

Informant 2 (INF2) arbetar som informationssäkerhetssamordnare i en större kommun och arbetar med att styra samt leda samordnare i organisationens informationssäkerhetsarbete. I organisationen kallas chefer för samordnare.

4.2.1 Policy

Organisationen har en säkerhetspolicy som reglerar allting gällande säkerhet. Direkt underställt säkerhetspolicyn finns ett dokument som heter ”Riktlinjer och Anvisningar för informationssäkerhet”, och INF2 menar att *”Det kan man tolka som en policy”* (bilaga 3, rad 6). Dessa riktlinjer är lika bindande som policyn. Policyn är ett politiskt beslut som behandlas i kommunfullmäktige, medan riktlinjerna och anvisningarna behandlas i kommunalstyrelsen.

INF2 har det yttersta ansvaret för dokumentet och dess innehåll. Däremot involveras flera aktörer vid dess utformning. Vid behov får INF2 stöd från jurister, IT-drifts personal, HR och kommunikationsavdelningen. Dock involveras inte vanliga anställda vid utformningen av riktlinjerna.

Gällande förankringen av styrdokumenten berättar INF2 att *”Främst så har vi sett till att få ett politiskt beslut, det ger ett mandat till riktlinjerna. Efter det kommuniceras de till varje enskild förvaltning”* (bilaga 3, rad 14). Organisationen består av ett flertal förvaltningar, de har alla har en direktör och en informationssäkerhetssamordnare som agerar som INF2’s högra hand. Policyn kommuniceras ut till förvaltningarna och publiceras på organisationens intranät. Förvaltningarnas informationssäkerhetssamordnare har både ansvaret att informera de anställda om förändringarna och för efterlevnadsgraden. Eftersom varje förvaltning hanterar dessa frågor på olika tillvägagångssätt ges det inga direktiv från INF2’s sida om hur samordnarna ska informera medarbetarna om riktlinjerna. INF2 berättar att *”Det vi istället gör är att vara tydliga med vad som behöver kommuniceras ut”* (bilaga 3, rad 16). Vid nyanställning behöver inte anställda skriva på ett dokument för att samtycka till att policyn och intyga att de ämnar efterleva den. Dock uppmanar INF2 genom policyn att förvaltningarna låter nyanställda skriva på en sekretessförbindelse. Det ser lite olika ut beroende på förvaltning, inom vård och omsorg finns exempelvis en klausul gällande sekretessbestämmelser i anställningskontraktet. (bilaga 3, rad 46)

Angående ISP medvetenhet berättar INF2 att *”I den nyskapande processen när vi tar fram nya styrdokument eller metoder så innebär det också att ta fram en kommunikationsplan. Den kommunikationsplanen ska vara ett stöd i genomförandet, i implementationsfasen”* (bilaga 3, rad 40). Kommunikationsplanen innefattar vad som bör tänkas på ur ett kommunikationsperspektiv under dokumentets livscykel. INF2 är ansvarig att formulera kommunikationsplanen, och kommunikationsavdelning finns som stöd. INF2 poängterar att *”Om vi ska förmedla ett budskap så ska vi vara tydliga och konkreta, och inte formulera vår text så att den skapar fler frågor än svar. Det måste vara väl och noga genomtänkt när man publicerar det”* (bilaga 3, rad 40).

Riktlinjerna revideras en gång om året. INF2 menar att det *”främst handlar det om att förtydliga riktlinjerna, anvisningarna”* (bilaga 3, rad 44). Dels behöver de också revideras på grund utav nya eller förändrade lagar, eller om något nytt behöver tilläggas. Gällande riktlinjerna understryker INF2 vikten av att *”de ska inte vara uppsatser. För då läser folk inte dem. Utan det ska vara enkelt, lättillgänglig text som förklarar väldigt tydligt för dig vad som gäller”* (bilaga 3, rad 44), dock ”är det inte busenkelt att formulera sig” (bilaga 3, rad 44).

4.2.2 Informationssäkerhetsprogram

INF2's avdelning har också till uppgift att tillhandahålla utbildning till förvaltningarna i den mån det går. Utöver det finns det en central utbildning som samtliga har tillgång till på organisationens intranät (bilaga 3, rad 18). Utbildningen kallas DISA (Datorstödd Informations-Säkerhetsutbildning för Anställda) och berör hur anställda ska tänka generellt kring hantering av information i olika förpackningar, med fokus på digital informationshantering (bilaga 3, rad 22).

För nyanställda på INF2's avdelning är utbildningen numera obligatorisk och utgör en del av introduktionsprogrammet som varje nyanställd ska genomföra. Genomförandet av utbildningen måste därefter undertecknas av respektives chef. I övriga fall ger stadskontoret förvaltningarna möjlighet att själva bestämma om utbildningen ska vara obligatorisk eller ej.

INF2 försöker uppmana de olika förvaltningarna att göra utbildningen obligatoriskt. I dagsläget tycker INF2 att medarbetarna är väl insatta och har en bra medvetenhet (bilaga 3, rad 38).

INF2 och hans informationssäkerhetskollegor utökar sin kompetens genom att delta i nätverk. Det finns ett informationssäkerhetsnätverk för Sveriges kommuner där alla som arbetar med dessa frågor kan dela med sig av styrningsdokument, utbildningsmaterial, beslut och allmänna råd på ett forum. De medverkar även i ett internationellt nätverk för europeiska städer som anordnar träffar regelbundet. Utöver det förekommer det utbildningar och konferenser inom informationssäkerhet (bilaga 3, rad 48).

4.2.3 Mätning

Organisationen använder sig av enkäter för att mäta efterlevnaden och medvetenheten. Enkätfrågorna baseras på styrdokumentets riktlinjer och frågorna riktas till olika målgrupper. Enkäterna skickas både till medarbetare och chefer. En av frågorna till medarbetargruppen var *"Har ni genomfört utbildningen som finns på vårt intranät?"* (bilaga 3, rad 26). INF2 menar att *"det är ett sätt att följa upp efterlevnad", "även om det inte var en vetenskaplig studie, så ger det en fingervisning på hur det ligger till"* (bilaga 3, rad 26). Resultatet i detta fall ledde till åtgärder på kommunal ledningsnivå, och låg till grund för att utbildningen blev obligatoriskt inom INF2's avdelning.

4.2.4 Övervakning och utvärdering

Övervakning av anställda sker i den mån de ser behov. För att tydliggöra för medarbetarna har INF2 skrivit i riktlinjerna att organisationen har rätt att göra det och kan göra det. Dock menar INF2 att *"Vi vill inte styra det [beteenden] genom övervakning, men vi tycker det är viktigt att möjligheten finns", "hur kan man annars kontrollera efterlevnad"* (bilaga 3, rad 60).

Övervakningen sker främst via stickprov. Om ett stickprov visar på ett särskilt beteende eller tyder på okunskap kan det generera en utbildnings eller informationsinsats. Då på ett brett perspektiv, snarare än på individnivå. Övervakningen omfattar bland annat nätverkstrafik och kontroll av lagring, så att inget lagras privat. De har även restriktioner på hur anställda får använda sin tjänsteutrustning, till exempel telefon och dator. Ingen övervakning sker i realtid (bilaga 3, rad 54).

4.2.5 Sanktioner och belöningar

Gällande sanktioner berättar INF2 att de har *”varit tydliga med att om du tar ett aktivt beslut som exempelvis går emot våra riktlinjer så finns det ett avsnitt i riktlinjerna som reglerar påföljder om man inte följer riktlinjerna. Det kan bli arbetsrättsliga, civilrättsliga åtgärder om det visar sig att det var jätteallvarligt. Det kan också bara bli någon form av reprimand eller att man får förklara sig om det uppdagas”* (bilaga 3, rad 28). Organisationen erbjuder inga incitament för god efterlevnad. INF2 beskriver att *”Det finns ingen morot mer än att se till att göra rätt, och vi ska kunna stå rakryggat ifall något av det vi gör ifrågasätts. Att vi har gjort det som kan förväntas göras av oss. Det är den moroten vi har”* (bilaga 3, rad 58)

4.3 Resultat intervju 3

Informant 3 (INF3) är anställd och delägare i Organisation C som är ett mindre företag verksamt i västra Sverige med ca 5–15 medarbetare. Organisationen erbjuder oberoende rådgivning, främst inom IT, till både små och stora organisationer. Ett typiskt uppdrag för anställda i organisation C är att arbeta som deltidsanställda IT-chefer eller IT-rådgivare.

4.3.1 Policy

INF3 berättar att *”Vi som ansvariga rådgivare på IT-sidan jobbar ganska mycket med att det finns en genomtänkt policy att efterleva. Det är en första nivå, att det faktiskt finns en policy. Nästa nivå är efterlevnaden. Där jobbar vi på det viset att vi försöker implementera policyn i andra rutiner. Tar vi personalfrågor så handlar det om att när någon ska börja på ett företag, nyanställning, så behöver man ha en process där man hanterar nycklar, datorer, telefoner och så vidare”* (bilaga 4, rad 6).

Överlag inom organisationer är det vanligtvis den IT-ansvarige som har i uppgift att skapa policyn. Dock anser INF3 att *”det är en ledningsfråga, det är en fråga för ett ledningsrum och en ledningsgrupp”*, men i praktiken ser det sällan ut så (bilaga 4, rad 8). Att få högsta ledningen engagerad i frågor kring policy och efterlevnad är i vissa organisationer en av dem största svårigheterna (bilaga 4, rad 46). Skapandet av en policy behöver input från en verksamhets alla avdelningar, då det berör samtliga i företaget. HR avdelningen är särskilt viktigt eftersom de hanterar personalfrågor och sköter kommunikationen mot fackliga organisationer. Policyn bestämmer vilket ansvar anställda har gällande specifika frågor, och vissa punkter kan uppfattas som hårda. Därför understryker INF3 att den behöver synkas med samtliga avdelningar (bilaga 4, rad 10).

INF3 och hans kollegor har utvecklat en metod för policy utformning. Den är baserad på tidigare erfarenheter och best-practices snarare än formella standarder. Metoden grundar sig i tomma mallar och innehåller ingen färdig information. INF3 menar att det är processen att framställa policyn tillsammans med de berörda som skapar förutsättningar för efterlevnad. INF3 säger att *”Det handlar om delaktighet”, och ”att de kan känna att det här är något jag vill skriva under på. Om alla har varit med och tyckt till om policyn är det mycket lättare att få det att efterlevas.”* (bilaga 4, rad 44)

Policyförankring sker i flera steg. Det första steget beskriver INF3 *”är att ha ett dokument som man får ta del av i samband med att man startar sin anställning”, ”gärna att man i det*

läget har både fått läsa och signera det” (bilaga 4, rad 12). Detta skapar en överensstämmelse mellan arbetsgivaren och arbetstagaren om vilka regler som gäller. Sedan måste policyn göras tillgänglig för medarbetarna, exempelvis genom intranätet. Det förutsätter att intranätet är ett *”levande ställe där många är inne och tittar”*, dock är det sällan så i verkligheten (bilaga 4, rad 14). INF3 berättar att *”om jag går in och skriver en uppdatering på min IT-policy och lägger upp version två på intranätet, så innebär det inte att det är implementerat i min värld. Utan, nu finns det ett nytt dokument, men det har inte medarbetare köpt”, ”Alltså accepterat vad som står där i, utan som alltid måste det vara någonting som man presenterar ut, när det är så pass viktiga saker”* (bilaga 4, rad 14).

För att kunna implementera policyn ordentligt krävs det stöd från ledningen. Vid en revidering bör ledningen kommunicera ut att policyn är uppdaterad tillsammans med vilka förändringar som gjorts. INF3 säger att policys idealt sett ska revideras på en årlig basis, till följd av den ständigt föränderliga omvärlden (bilaga 4, rad 12; bilaga 4, rad 34). I sitt arbete ser INF3 ofta föråldrade policys som inkluderar riktlinjer om faxanvändning och som samtidigt ignorerar mobiltelefoni (bilaga 4, rad 12).

Samtidigt så menar INF3 på att utvecklingen inom IT går otroligt fort, *“Det innebär att IT-policys alltid ligger steget efter”* (bilaga 4, rad 52). Att uppdatera och förmedla policy i den takt som krävs för att tillfredsställa behovet av säkerhet kan vara svårt, då är vidareutbildning av personal en mindre tidskrävande och mer effektiv metod. Policyn är inget man läser på regelbunden basis, fokus ligger på att anställda gör rätt och har rätt kunskap. *“Då är utbildning mycket viktigare än att man kan rabbla innehållet i IT-policyn. Det ger mycket större effekt”* (bilaga 4, rad 54).

4.3.2 Informationssäkerhetsprogram

INF3 säger *”Det är medarbetarna vi måste utbilda, löpande. Det är det som är lösningen på våra säkerhetsproblem. Inte en bättre brandvägg eller bättre lås till porten. Utan det blir väldigt mycket fokus på att utbilda medarbetare så att de förstår vad dem gör när dem surfar eller klickar på en länk i ett mail”*.

Utbildning kan ske genom E-learnings programvara. Det finns flera aktörer som säljer sådana tjänster. Utbildningsprogrammet INF3 förespråkar inkluderar frågor och information om informationssäkerhetsrisker och vad som bör tänkas på vid hantering av känslig information. Utöver det ingår det en epost-prenumeration, där informations-epost skickas ut på en veckolig basis innehållandes påminnelser eller information om nya hot. Det är även effektivt att utbilda anställda löpande under vardagsarbetet. Varje måndagsmöte kan behandla en kort fråga eller generella tips. Utbildning kan även ske på arbetsplatsträffar eller avdelningsmöten.

INF3 rekommenderar att alla tjänstemän som hanterar information behöver få utbildning, men att det exempelvis är lätt att glömma lagerpersonal. Även de har tillgång till lager- och logistiksystem, transportadministration, såväl som internet och epost.

Gällande vidareutveckling av sin egen kompetens berättar INF3 att *”Dels så jobbar vi inom företaget med vad vi kallar kompetensgrupper. Det betyder egentligen att vi ser till att ha ansvariga personer och små grupper som driver kompetensen i respektive område. Det kan vara allt från säkerhet till affärssystem till driftansvar och så vidare. I de grupperna så ingår dels att köpa utbildningar och gå utbildningar inom respektive område. Det andra är att*

träffa leverantörer, vi har ett väldigt stort kontaktnätverk på leverantörssidan. Det vill säga IT-företag som är duktiga på olika saker. Det kan vara allt från PUL, eller numera GDPR, till alla andra kompetensområdena. Man kan säga att vi dels lyssnar på leverantörsföretagen, på vad de är duktiga på och hur de arbetar med frågorna. Och dels går vi kurser och utbildningar för att skaffa oss den kunskapen löpande".

4.3.3 Mätning

Ett sätt att mäta säkerhetsmedvetenheten i en organisation är att använda sig av resultatet från E-Learning. Genom att bearbeta svaren som anställda givit under programmet så kan man identifiera områden där man anser att personalens säkerhetsmedvetenhet är otillräcklig och arbeta aktivt med åtgärder. (bilaga 4, rad 26) Det finns även andra verktyg och metoder för att mäta efterlevnadsgraden i organisationer men enligt vår informant så används inte dessa i så stor utsträckning. Ett sätt att mäta efterlevnad och medvetenhet är att utnyttja medarbetarenkäter som vanligtvis fokuserar på anställdas trivsel, hälsa och förbättringsförslag i organisationen. *"Men där har man ett tillfälle att ställa ett gäng frågor till medarbetare. Där skulle man kunna nyttja chansen att prata medvetenhet kring IT-säkerhet"* (bilaga 4, rad 30).

4.3.4 Övervakning och utvärdering

Det finns idag allt fler möjligheter till att övervaka dem anställda i organisationen och då framförallt vad det gäller hur organisationens mobiltelefoner används. Men det är väldigt sällan en organisation vill övervaka sina anställda. Detta för att övervakning i sin förlängning kan ses som ett ifrågasättande huruvida man har tillit och förtroende för sin personal eller inte. (bilaga 4, rad 36)

INF3 berättar att större organisationer ofta administrerar företagets mobiltelefoner centralt idag. *"Det vill säga att de har programvara som kan styra innehållet. När du får din telefon kan vi skicka ut appar som måste finnas på telefonen. Man kan se dataförbrukning och sådana där saker."* Dataförbrukning är vanligt att man övervakar, men detta gör man oftast ur ett kostnadsperspektiv snarare än för att kontrollera om användandet av enheten sker enligt policy. (bilaga 4, rad 36) Om det är vanligt förekommande att anställda felaktigt hanterar organisationens mobiltelefoner på ett obegåvat eller riskfyllt sätt så är det vanligtvis IT-avdelningen i organisationen som upptäcker det. Utredningen av händelsen kan vara en IT-fråga då man försöker ta reda på fakta om vad som har hänt, vilken typ av information som felhanterats och hur information har felhanterats (bilaga 4, rad 38). Anställdas säkerhetsbeteende utvärderas endast när en incident uppdagas.

4.3.5 Sanktioner och belöningar

Vid mindre förseelser och brott mot policy så för man en dialog med medarbetaren för att informera om vad som gäller i organisationen. *"Om man upptäcker någon typ av slarv eller misstag, då kan vi påminna den personen om att det är fel."* (bilaga 4, rad 40) Om en anställd felaktigt skulle hantera organisationens information så beror konsekvenserna helt och hållet på vad det är för sorts information. INF3 berättar att det är *"en jätteallvarlig fråga, om det är någon som till exempel tar ut ett kundregister och sparar ner det någonstans, och tar med det utanför företaget"*. Men vad för konsekvenser som kan vara aktuella för ett felaktigt handhavande anser INF3 snarare är en personal- och ledningsfråga. (bilaga 4, rad 38)

Det är enligt INF3 sällan organisationer arbetar med att motivera anställda till att följa policys. I de flesta fall får den anställde bara förklarat för sig att *”du är anställd här, därmed gäller ett antal ramar som vi faktiskt har bestämt inom verksamheten”*. (bilaga 4, rad 34)

5 Diskussion

I detta kapitel ställer vi vårt resultat mot tidigare litteratur som vårt teoretiska ramverk baserades på. Utifrån det för vi en diskussion.

5.1 Policy

Informanterna har ansvar över policyn och dess innehåll i deras roll som IT och informationssäkerhetsansvarig. Vilket Whitman & Mattord (2011) säger är viktigt. Samtliga involverar övriga avdelningar, grupper och ledningen vid utformandet. De samtycker att det skapar goda förutsättningar för efterlevnaden om alla berörda parter involveras. Sådan delaktighet kan bidra till att policyn upplevs som lämplig och rättvis, vilket Son (2011) menar bidrar till en högre efterlevnadsgrad.

Samtliga får stöd och godkännande från ledningsnivå vid utformandet och under implementationsfasen då de anser att det ökar policyns legitimitet. Detta ligger i linje med Son (2011) som hävdar att det är viktigt att anställda upplever policyn som legitim. Ledningen bör även vara delaktig vid revidering och förmedla ut att policyn har uppdaterats och vilka förändringar som gjorts. Von Solms & Von Solms (2004) menar att ledningsstöd demonstrerar organisationens engagemang i frågan. Dock upplever INF3 att en av de största svårigheterna ibland kan vara att få ledningen involverad i arbetet.

För att förmedla en antagen policy har informanterna ett liknande semi-decentraliserat tillvägagångssätt där avdelningschefer tilldelas ansvaret att vidareförmedla policyn ut i respektive avdelning. En tydlig skillnad är att INF2 upprättar en kommunikationsplan som beskriver vad avdelningscheferna behöver kommunicera ut. Dock framgår det inte i planen hur tillvägagångssättet kan se ut. Att det är viktigt att förmedla policyn och säkerställa att anställda tar del av, läser, samt förstår den är enligt Whitman & Mattord (2011) viktigt. Men det finns inget konkret tillvägagångssätt beskrivet. Utöver att ta fram en plan för vad som ska förmedlas, så tror vi det skulle kunna gynna efterlevnadsgraden av policys om IS-ansvarig tar fram en plan för hur förmedlingen ska gå till. Detta bör göras i samarbete med dem som får i ansvar att förmedla policyn för att kunna beakta skillnader i olika avdelningar och uppnå samstämmighet över hur man förmedlar policyn på bästa sätt. Utöver det publicerar samtliga sina policys på respektives organisations intranät så att de anställda kan ta del av dem. Enligt INF3 förutsätter det att intranätet är aktivt och en central del av organisationen. Genom att göra policys tillgängliga misstänker vi att det också blir lättare att hålla anställda ansvarsskyldiga. De kan då inte hävda att policyn inte tillgängliggjorts på ett smidigt sätt. I Organisation A och C behöver nyanställda läsa och skriva under en överenskommelse där denne går med på att efterleva policys, vilket är i linje med vad Whitman & Mattord (2011) förespråkar.

Enligt Leveque (2006) är det viktigt att säkerställa att policys i organisationer är aktuella. Samtliga informanter reviderar sina policys med varierande mellanrum för att hålla sig uppdaterade med nya lagar, nya hot och ny teknik men även för att förtydliga innehållet. INF3 anser

att utvecklingen på IT-sidan går så snabbt att det kan vara svårt att hålla policyn aktuell. Det kan då vara en effektivare strategi att skapa medvetenhet och utbilda sina anställda i säkerhetsfrågor.

5.2 Informationssäkerhetsprogram

Det råder delade meningar om hur nödvändig IS-utbildning är. Organisation A har till skillnad från de andra inget utbildningsprogram, INF1 menar att det vore överflödigt. Istället har de en stark organisationskultur som präglas av kritiskt tänkande, och personal utbildas informellt vid behov. De övriga två har ett utbildningsprogram, men de är inte tillräckligt omfattande och kontinuerliga för att klassas som ett fullskaligt etablerat informationssäkerhetsprogram. Enligt Peltier (2005b) ska ett informationssäkerhetsprogram inkludera följande aspekter: medvetenhet, träning och utbildning. Något som tydligt saknades var säkerhetsträning i form av workshops. Enligt oss kan avsaknaden bero på två faktorer, bland annat att det inte finns ett behov och att det är för resurskrävande. Informanterna kan ha gjort en avvägning där de väger kostnaden och den förväntade nyttan, och dragit slutsatsen att ISA är mer kostnadseffektivt. De utbildningsprogram vi blev informerade om fanns tillgängliga via intranätet och syftade till att öka anställdas ISA. En uppenbarfördel är utbildningarnas tillgänglighet, då det tillåter samtliga anställda att genomföra den.

Utbildningarna var inte alltid obligatoriska vilket enligt oss kan leda till att särskilda anställda som bör genomföra den slipper undan. Enligt de två informanter med ett utbildningsprogram så genomgår samtliga anställda samma utbildning. Peltier (2005b) hävdar att utbildningen måste skräddarsys utefter de olika avdelningarnas behov. Samtidigt som Awawdeh & Tubaishat (2014) understryker att utbildningen även måste urskilja olika individers behov. Kartläggning av både avdelningars och enskilda individers behov, för att sedan skräddarsy en utbildning är oerhört resurskrävande.

Utbildningsprogrammen behövdes genomföras en gång, utöver det såg vi varierande nivåer av kontinuerlig ISA-spridning. Enligt Whitman & Mattord (2011) måste all utbildning skötas aktivt och kontinuerligt, annars riskerar anställda att ignorera säkerhetsproblem. INF3 förespråkar en E-Learning utbildning som inkluderar veckoliga epost om informationssäkerhet. Peltier (2005b) menar att det är den mest kostnadseffektiva metoden. Utöver det rekommenderar INF3 att behandla informationssäkerhetsfrågor snabbt under veckomöten och arbetsplatsträffar.

Enligt Whitman & Mattord (2011) är det essentiellt att IS-ansvariga har den nödvändiga kompetensen att utforma och vägleda en organisations informationssäkerhetsarbete. Vi kan konstatera att INF2 och INF3s löpande kompetensutveckling är direkt relevant för den bransch de är verksamma i. Whitman & Mattord (2011) rekommenderar universitetsutbildningar och certifikat. Vi tror att den typen av vidareutbildningar är för tidskrävande för befintligt anställda, och att det idag snarare är en förutsättning för anställning.

5.3 Mätning

Kruger och Kearney (2006) menar att ISA aktivt måste mätas för att kontrollera effektiviteten av ISA-programmet. Mätningsresultatet kan ge en indikation över organisationsmedlemmars ISA och ge upphov till extra utbildningsinsatser (Kruger & Kearney, 2006). INF2 mäter indirekt efterlevnaden av deras policys genom att undersöka anställdas ISA och huruvida de genomgått utbildningen via enkäter. Detta är något INF3 också förespråkar. Då Kruger och Kearneys (2006) mätningsmetod inkluderar faktorer som kunskap, attityd och beteende, behöver den nödvändigtvis inte bara mäta ISA. Vi anser att mätningsmetoden kan inkludera frågor direkt relaterade till anställdas beteenden gällande efterlevnad av ISP. Resultatet kan bidra med en mer konkret bild av efterlevnadsgraden än vad en ISA-mätning gör.

Ett av utbildningsprogrammen sammanställer svarsresultaten. De svarsresultaten kan ses som en mätning. Problemet med utbildningen ur ett mätningsperspektiv är att den endast behöver genomföras en gång, samt att anställda genomför den vid olika tidpunkter, exempelvis vid nyanställningar. Det försvårar kontinuerlig mätning och jämförelse med tidigare mätningsresultat. Eftersom utbildningsprogrammet bör uppdateras i takt med ny teknologi och nya identifierade risker (Thomson & Von Solms, 1998), tror vi att det kan bli svårt att dra generaliserbara slutsatser över tiden.

Siponen (2000) menar att användarfelen måste identifieras och kvantifieras. Ett sätt att göra det på ett mer konkret sätt är intern revision. Organisation A granskar årligen huruvida anställdas lösenord är konfigurerade enligt policyns riktlinjer. I efterhand anser vi att sådan intern revision borde ha inkluderats i vårt teoretiska ramverk. Det kan hjälpa IS-ansvariga att granska efterlevnaden av särskilda ISP som samspelar med teknik.

5.4 Övervakning och utvärdering

Von Solms & Von Solms (2004) anser att anställda måste övervakas i realtid för att kunna säkerställa efterlevnaden av ISP. Vi kan konstatera att våra informanter arbetar på ett annorlunda sätt. Visserligen säger INF2 att det är svårt att kontrollera efterlevnaden utan övervakning. Men samtliga informanter är överens om att de inte vill styra anställdas beteenden via övervakning. Informanter ser det som en integritetsfråga, samt att själva handlingen kan ses som ett ifrågasättande av anställdas tillit och förtroende. Enligt Spitzmüller & Stanton (2006) kan övervakning bemötas av motstånd. Enligt oss kan det vara en bakomliggande anledning till varför informanterna i stor utsträckning undviker det. D'Arcy et al. (2009) ser övervakning som en avskräckande proaktiv åtgärd. Men ingen av informanterna övervakar i realtid, och när det sker är det främst ur ett kostnadsperspektiv, eller i utrednings- och mätningssyfte. Vi anser inte att denna typ av övervakning kan uppfattas som speciellt avskräckande.

Samtliga informanter menar att anställda endast utvärderas vid uppföljning av incidenter, då antingen formellt eller informellt beroende på incidentens natur och seriositet. Boss et al. (2008) menar att risken finns en att policys ignoreras om anställdas efterlevnad aldrig utvärderas. Enligt oss blir kontinuerlig utvärdering oerhört svårt utan övervakning. En grundförutsättning är att det finns underlag att faktiskt utvärdera.

5.5 Sanktioner och belöningar

Det råder konsensus bland informanterna att sanktioner är nödvändigt vid överträdelse av ISP. Deras sanktioner kan vara i form av en tillsägelse, ekonomiska påföljder eller i form av uppsägning. Talib (2015) delar upp sanktioner i övertygelse att åka fast samt sanktionens stränghet. Gällande straffets stränghet är det endast INF2 som tydliggjort för sina medarbetare vilka sanktioner en överträdelse kan medföra. I en studie av D'Arcy et al. (2009) fann de att övervakning ökar anställdas övertygelse att åka fast. Men utan övervakning och kontinuerlig utvärdering torde anställdas övertygelse vara låg. Belöningar förekom i någon organisation. Som tidigare nämnt blir det också svårt att identifiera gott säkerhetsbeteende om det inte finns en process för att samla in utvärderingsunderlag. Enligt Talib (2015) kan avsaknaden av belöningar skapa en uppfattning att ISP efterlevnad är oviktigt. Både sanktioner och belöningar kan ses som yttre motivationsfaktor med syfte att uppmana anställda till ett visst beteende. I informanternas organisationer förekom det inte heller några andra motivationstekniker. Enligt oss är faktumet att samtliga använder sig av sanktioner vid uppmärksammade ISP överträdelser inget märkvärdigt. Överlag brukar misskötsel straffas.

6 Slutsats

Vår empiriska undersökning ämnade att undersöka hur IS-ansvariga arbetar med efterlevnad av ISP, och vilka förutsättningar som måste finnas hos ISP för att underlätta det arbetet. Vi har lyckats synliggöra ett flertal skillnader och likheter, både mellan hur IS-ansvariga arbetar med dessa frågor, men även i relation till vad teorin förespråkar.

Vår undersökning har visat att IS-ansvariga arbetar med policyutformning, förankring och revidering på ett snarlikt sätt. Vi kan konstatera att ISP behöver vara relevant och lättförstådd. Vid utformning och förankring är det nödvändigt att ledning och övriga avdelningar involveras. Vidare är ledningsstöd vitalt ur ett symboliskt perspektiv.

Angående hur IS-ansvariga arbetar med ISP efterlevnad fann vi tydliga likheter om hur de går tillväga men stora skillnader i omfattning. I jämförelse med vårt teoretiska ramverk är den största skillnaden IS-ansvarigas synsätt och användande av övervakning i realtid i syfte att kontrollera anställdas beteende. Vi såg att IS-ansvariga förlitade sig på det i väldigt liten utsträckning. Överlag arbetar IS-ansvariga semi-aktivt för att öka efterlevnaden av ISP. Av åtgärderna i vårt teoretiska ramverk använde sig IS-ansvariga i varierande utsträckning ISA-utbildning, mätning, övervakning, utvärdering och sanktioner, medan säkerhetsträning och belöningar förbisågs. Då ingen IS-ansvarig såg efterlevnad av ISP som ett omfattande problem i respektives organisation drar vi slutsatsen att dessa åtgärder är tillräckligt tillfredsställande för deras behov.

Detta ger en inblick i hur IS-ansvariga arbetar med policy och dess efterlevnad, men för att kunna ge en mer universell och generell bild krävs en betydligt mer omfattande undersökning.

Referenser

Andress, J. (2011) The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. S171

Awawdeh, S.A. & Tubaishat, A. (2014): An Information Security Awareness Program to Address Common Security Concerns in IT Unit. S273-278

Boss, S. Kirsch, L. Shingler, R. Boss, W. (2008): If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. S151-163

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3), 523-548.

D'arcy, J. Hovav, A. & Galleta, D. (2009): User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. s79-98

Erickson, K., & Howard, P. N. (2007). A case of mistaken identity? News accounts of hacker, consumer, and organizational responsibility for compromised digital records. *Journal of Computer* , 12(4), 1229-1247. *Mediated Communication*

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & security*, 61, 169-183.

Gollman, D. (2011). *Computer Security.* 3rd ed. Hoboken, NJ.: Wiley.

Jacobsen, D. (2002). *Vad, hur och varför: om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen.* Lund: Studentlitteratur.

Kearney, P. (2010). *Security: The Human Factor.* 1st ed. Ely: IT Governance Pub.

Kruger, H.A. & Kearney, W.D. (2006): A prototype for assessing information security awareness. S289-296

Leveque, V. (2006). *Information Security - A Strategic Approach.* Hoboken, NJ.: Wiley.

Peltier, T. (2005a). *Information security risk analysis.* 2nd ed. Boca Raton: Auerbach Publications.

Peltier, T. (2005b): Implementing an information security awareness program. S37-49.

Puhakainen, P. Siponen, M. (2010): Improving employees' compliance through information systems security training: an action research study. S757-778

PwC (2015b). Information Security Breaches Report [pdf] Tillgänglig: https://www.pwc.co.uk/assets/pdf/2015-isbs-executive-summary-02.pdf [Hämtad: 2017-04-24]

PwC (2015a). The Global State of Information Security Survey [pdf] Tillgänglig: http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf [Hämtad: 2017-04-24]

Sherif, E., Furnell, S., & Clarke, N. (2015). Awareness, behaviour and culture: The ABC in cultivating security compliance. In *Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for* (pp. 90-94). IEEE.

Siponen, M. (2000): A conceptual foundation for organizational information security awareness, s31-41

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer*, *43*(2).

Son, J-Y. (2011): Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. S296-302

Spitzmüller, C. Stanton, J. (2006): Examining employee compliance with organizational surveillance and monitoring. S245-271

Talib, Yurita. (2015):Intrinsic Motivation and Information Systems Security Policy Compliance in Organizations. S1-168

Thomson, M.E. & Von Solms, R. (1998): Information security awareness: educating your users effectively. S167-173

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, *49*(3), 190-198.

Von Solms, B. & Von Solms, R. (2004): The 10 deadly sins of information security management. S371-376

Wheeler, E. (2010): Security Risk Management: Building an Information Security Risk Management Program from the Ground Up.ISBN: 978-1-59749-615-5. S361

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. 4th ed. Cengage Learning.

Young, K. (2010): Policies and procedures to manage employee internet abuse. 5s.

7 Bilagor

7.1 Bilaga 1

Intervjufrågor

Nr	Fråga
1	Har ni ISP?
2	Vem utformar dessa policys?
3	Vilka involveras vid utformandet?
4	Hur informerar ni anställda om de ISP ni har?
5	Förekommer det att anställda inte följer ISP?
6	Vad kan det bero på?
7	Vad gör ni för att öka efterlevnaden av ISP?
8	Skulle du säga att anställda överlag har god säkerhetsmedvetenhet?
9	Sprider ni medvetenhet om informationssäkerhet och era policys? Hur?
10	Har ni ett informationssäkerhetsprogram som utbildar/tränar anställda?
11	Vad består det programmet utav?
12	Mäter ni efterlevnadsgraden av era policys?
13	Övervakar ni anställdas beteende för att se om de följer policys?

14	Hur ser du på övervakning?
15	Hur följer ni upp övervakningsresultatet?
16	Om en anställd bryter mot en IS-policy, hur hanterar ni det?
17	Vilka konsekvenser kan det få?
18	Belönas anställda som agerat korrekt?
19	Finns det andra sätt ni använder för att motivera anställda att följa policys?

7.2 Bilaga 2

Transkribering intervju 1

Rad	Replik
1	E: Hur mycket policyarbete ingår i arbetsrollen?
2	I: Det är ju jag tillsammans med någon annan som har tagit fram IT-policyn. Men, vad ska jag säga, den förra IT-policyn togs väl fram på ungefär samma sätt tillsammans med personalgruppen. Den togs fram för väldigt längesen. Jag kommer inte riktigt ihåg om den kan ha varit ända sen, ja, runt år 2000 eller någonting sånt där. Så att vi har en ny IT-policy som inte är fastslagen, men den har varit ute på 2 remiss-utgåvor, så nu ligger den alltså för genomgång hos företagsledningen och därefter så ska den då ut på remiss till personalgruppen, så att den kan fastslås av koncernledningen.
3	P: Okej, så ni involverar då alltså personalen när ni skapar era policys?
4	I: Nej, inte personalen i den bemärkelsen. Utan vi är en ganska stor koncern så det betyder att vi har ju flera personalchefer som sitter ute på de olika huvudorterna då, och då har de en personalchefsgrupp som leds utav en som är ansvarig för hela koncernchefens personalfrågor. Och där ska den, så att säga, klubbas då. Eller rättare sagt, den ska godkännas, och sen ska den lämnas till koncernledningen som godkänner antagandet. För att få lite tyngd bakom sig.
5	E: När ni utformar en policy, vad bör den innehålla eller bestå av?
6	I: Det är främst riktlinjer.
7	E: Utöver riktlinjerna, beskrivs det hur den ska genomföras, implementeras eller hur den ska efterlevas?
8	I: I mångt och mycket är det upp till varje avdelningschef så tar vi till exempel så att säga den personliga utrustningen så är det egentligen ens chef som avgör vad det är för utrustning som ska användas, hur den ska användas, vad som händer om den förkommer eller blir förstörd.
9	E: Vad är de mest förekommande svårigheterna när en policy tas i bruk?
10	I: Ja det är ju efterlevnaden av de riktlinjer som kan vara svårt. Det händer ju till exempel att anställda vill behålla utrustning när de slutar. Vilket är helt tvärtemot av vad som är gällande policy.

11	P: Det förekommer alltså att anställda inte följer policys?
12	I: Ja, det gör det ju.
13	P: Okej. Överlag, vad kan det bero på?
14	I: I vissa fall tror jag det beror på snällhet, och ibland beror det på okunskap. Ett bra exempel på det är ju just när det gäller våra datorer och våra telefoner då bara, iPhones. Vi leasar all utrustning och det är lite konstigt om man ger bort leasad utrustning. Det är inte ens vår egen utrustning, det tillhör inte ens företaget.
15	P: Vad gör ni då för att öka efterlevnaden av policys?
16	I: Ja vi försöker ju, alltså vi som jobbar inom IT i organisationen försöker se till att de efterlevs. Och det händer ju att det kommer folk och frågar om de får köpa loss utrustning och då säger vi kategoriskt nej. Med en förklaring varför. Skulle det då vara så att någon säger att de vill köpa ut den för, jag vill ändå köpa ut den, så brukar det ändå sluta på att det blir så pass dyrt, eftersom att dels får man betala [04:25-04:27 ?] leasingkostnaden men också betala ett förmodat marknadsvärde när leasingkontraktet har gått ut. Och då blir det minst lika dyrt som att köpa en ny dator. Men det brukar aldrig vara någon diskussion.
17	E: Okej. Men ni har också policys så som lösenordspolicys, policys om internetanvändning och “clear desk”-policys?
18	I: Jadå, det har vi. Och lösenordspolicyn, den sätter ju [04:58-05:00 ?] själva, hur ofta man ska byta lösenord och längd på lösenord och så vidare. Och det är ju någonting som vi utsätts för av revisorerna för revision en gång om året då också, att man går igenom all konton och sådana saker då
19	P: Om ni märker att anställda inte byter lösenord tillräckligt ofta, eller använder internet fel, eller bryter mot några policys, vad kan ni då göra för att öka efterlevnaden av de policyna?
20	I: Rent generellt så efterlevs de faktiskt, så det där brukar inte vara något direkt problem. Utan de vi får frågor om till exempel är “Nu ska jag åka på semester, och vara utomlands. Vad händer då?” Då får man tala om för dem att “det är inte okej att använda din [jobb]telefon för utlandssamtal när du är ute på semester om det inte är så att du behöver jobba och din chef godkänner det”. Så att såna fall har vi återkommande. Och är det så att någon åker utomlands och sen har, då ser vi det på fakturornas telefoni. Och då har vi kontrollfunktioner för det, så då brukar det inte vara något problem, utan då får den anställde betala för den trafiken som har använts när man varit utomlands. Och när det gäller, människor kommer ju och frågar och säger “nu ska jag åka iväg, och jag tar med mig den [telefonen], så att ni kan säga till när det [fakturan] kom-

	mer sen”
21	P: Okej. Men det är då om de kommer och frågar eller säger någonting, men gör ni något förebyggande så att de får reda på det. Har ni något slags informationssäkerhetsprogram som utbildar anställda om informationssäkerhet och om era policys till exempel?
22	I: Alltså det är varje anställds skyldighet att känna till vilken IT-policy som gäller. Det finns till och med så att de ska undertecknas, men första gången som det presenterades så skrev de, så svarade flera stycken, då främst journalister som säger att “det där skriver vi inte på”. Och då svarade vi egentligen bara att det spelar ingen roll om du skriver på eller inte, den gäller i alla fall. Vi har aldrig haft något fall där vi, så att säga, haft några problem.
23	P: Men har ni något slags informationssäkerhetsprogram och utbildar ni användare om informationssäkerhetspolicys?
24	I: Nej, det gör vi inte. Utan vi publicerar ju dem policys som är antagna och som gäller, dem lägger vi ut på vårt intranät helt enkelt. Och när det gäller sådana saker som vi har då, [07:58-07:59 ?] ekonomihantering, det har vi också publicerat på vårat intranät.
25	P: Har ni som arbetar på IT-avdelningar, och du som IT-chef, kontinuerliga utbildningar i exempelvis informationssäkerhet och policy-utformning?
26	I: Nej.
27	E: Det är då tidigare arbetsliverfarenhet och utbildningar?
28	I: Ja, och så tar man hjälp i så fall av någon utomstående.
29	P: Följer ni någon standard för policys?
30	I: Nej.
31	E: Om ni inte har ett utbildningsprogram för anställda, men ändå upplever att policys efterlevs i stor utsträckning, skulle du då säga att ni har en bra säkerhetskultur?
32	I: Det är lite kul att du säger det, för jag hade [hörde? 09:09-09:10] en jättediskussion med en av våra högsta chefer häromdagen som tyckte att det var för jobbigt att använda VPN. “Måste man ha det?” Då blir man [09:23-09:24 ?]-trött kan jag säga!

33	E: Finns det några försök till att fostra ett informationssäkerhetstänk och en säkerhetskultur i organisationen?
34	I: Nja, på sätt och vis gör det väl det. Det är ju sådana saker som att lösenord och sådana saker är personligt. Se till att man har lås på dator och lås på telefon. Och för en yngre generationen så är det där absolut inga konstigheter alls, medan för den äldre generationen så kan det där vara någonting som är fullkomligt främmande för dem. Men det märker jag som har varit med ett tag, då att, då märker man faktiskt en ganska stor förändring att folk är ju mer och mer medvetna. Det är till och med hänt faktiskt att användare som har kontaktat supporten och vill ha hjälp och så ber supporten om deras lösenord för att komma in i deras datorer att de inte får det?
35	P: Har större medvetenhet hos de anställda kommit från informella samtal i organisationen, från nyhetstidningar, och allmänt blivit mer tekniska?
36	I: Ja, det är rent allmänt att man har blivit mer säkerhetsmedveten, absolut, det tycker jag nog. Sen finns det ju givetvis dem, någon användare då som inte ens loggar ut från sina datorer när han går hem om kvällarna, utan bara reser sig upp och går, och så står de [datorerna] där inloggade när han [anställde] är färdig.
37	E: Håller ni anställda ansvarsskyldiga på något sätt, och finns det repressalier som man upplever om man då exempelvis inte loggar ut från sin arbetsstation?
39	I: Nej, inte så, när det gäller det. Men däremot till skillnad mot den gamla IT-policyn, som fortfarande gäller då, för i den nya IT-policyn så ställer vi ett ekonomiskt ansvarstagande på dem [anställda] om man exempelvis… Det vanliga är att man tappar en smartphone i golvet och glaset går sönder. En olycka är en olycka, men inträffar de två tre gånger, då blir man, så som förslaget är utformat, blir man ersättningsskyldig. Och det gäller samma sak med datorerna.
39	E: Motiverar ni anställda att följa policys? Finns det incitament?
40	I: Nej, det kan jag inte påstå.
41	E: Tror du att det finns en förståelse bland anställda varför policyn finns där i första hand?
42	I: Våran organisation är nog lite speciell också, eftersom det är så många journalister. Det ingår i deras jobb att vara starkt kritiska. Ofta när vi tänkt igenom någonting tänker vi att det här är kristallklart. När man då skickar iväg det blir det kritiskt granskat av dem, och då händer det att de blir fundersamma. Då händer det faktiskt att dem kommer, vi hade till exempel, när vi anslöt oss till ett Apple program, så stod det i den här texten att telefonen är förregistrerad på ett bolag. Och att en administratör kan övervaka innehållet i telefonen. Då såg fackklubborna rött. Det var en olycklig formulering. Tyvärr kan vi

	inte styra över den själva, utan vi fick den sådär. Då fick vi förklara vad vi kunde göra, och vad det var vi gjorde. För det som gick att göra tyckte vi själva inte var något som kränkte intregriteten. Sedan talar vi om för dem vad vi gjorde, vad det var för information vi kunde komma åt.
43	P: Hur mottogs det?
44	I: Det räckte med det, sen blev det ganska bra. Erfarenheten av det är att vi skulle ha berättat innan.
45	P: Kan man säga att de misstolkade policyn då?
46	I: Ja, de tolkade den som de ville. Dem förstod nog inte riktigt innebörden av den. …. Stod det att vi kunde se innehållet i deras telefoner. Ska man tolka det där strikt, kan man säga så här. Vi ser telefonens innehåll, men vi ser inte telefonens data. Vi kan till exempel se ifall någon har installerat pokemon, men vi kan inte se vilka pokemons dem har. Deras kontaktlistor, Vi har kan se att dem har applikationen ”kontakter” men vi kan inte se vilka som finns där. Vi kan se att dem har bilder, men inte vilka bilder, samt deras internetanvändning, men inte vart på internet de har varit.
47	P: Om ni nu övervakar deras internetanvändning, har ni en policy som säger vad anställda får använda internet till på arbetsplatsen?
48	I: Låt mig förklara det där lite tydligare, om vi kan övervaka deras internet användning, då är det mängden data som vi övervakar. Det gör vi för att de ska ha rätt mängd. Det vet ni själva hur det funkar. Köp 100 gig i månaden, det är lite onödigt för oss som nästan har 1000 abonnemang att köpa 100gig till alla användare, om 95% av alla användare använder en. Därför följer vi deras dataanvändning. Då händer det att vi ser två personer i samma yrkesgrupp har en väldigt stor differens i dataanvändning. Exempelvis, den ena ligger på 2gb, och bordsgrannen med exakt samma jobb har 35gb. Då frågar vi den som använder 35gb, hur kommer det sig att du har så mycket? Det kan ju uppfattas som negativt. Vi säger då att vi endast är intresserade av vad du har för beteende, så vi vet hur mycket data du ska ha. Det visade att personen som använder 2gb cyklar till jobbet, vilket tog 10minuter för honom. Den andra personen med 35gb åkte tåg 1 timme om dagen och tittade på streamade filmer samtidigt. Där har vi förklaringen.
49	E: Det är förklaringen som är intressant. Lägger ni någon värdering på att personen använde så mycket data?
50	I: Nej. Det gör vi inte. Det kan ju också vara så att någon tittar på något som är relevant för ens jobb. Till exempel en telekonferens, eller vad som helst. Men i just detta fall tit-

	tades det film. Den andra vinkeln på det, gällande internetanvändning har vi policys vad man får göra och inte göra. Det är bra beskrivet i policyn, jag ska se ifall jag hittar den.
51	E: Har ni några kontrollmekanismer för att se ifall det efterlevs, det man får eller inte får göra?
52	I: Nej, det har vi inte. Vi skulle kunna ha det om vi velat, men nej.
53	E: Är det en integritetsfråga?
54	I: Det är det definitivt. Däremot kan det hända att vi behöver göra efterforskning ifall det finns misstankar om någon typ av missbruk. Det har hänt
55	P: Ni utvärderar alltså anställdas beteende när ni vet att något är fel.
56	I: Mja, om vi misstänker att någon begått något brottsligt så gör vi ju det.
57	P: Du talade lite om att folk missförstod eller misstolka den där policyn, hur förklarar ni policies syfte och motiverar dess existens?
58	I: I det fallet var det var en informationstext som låg i grundkonfigurationen, och den kom ifrån apple. Den kunde inte vi påverka. Så det var ingen riktig policy.
59	I: Jag hittade policyn jag talade om tidigare, jag kan läsa högt. Under avdelning internet. Att besöka sidor med olagligt innehåll är självklart förbjudet. Det betyder inte att du får lov att besöka alla sidor med lagligt innehåll där du använt företagets IT-system. Det betyder att du inte får besöka sidor med pornografi, extrema politiska och religiösa budskap, eller annat olämpligt innehåll. Det omfattar även fildelning av material, även dem material med upphovsrätt. Undantag, i det journalistiska arbetet kan det vara motiverat att besöka sidor med pornografi, extrema politiska och religiösa budskap eller på annat sätt olämpligt och lagligt innehåll. Din närmaste chef ska alltid informeras vid besök av sådana sidor. I möjligaste mån ska informationen ges i förväg. Detta är ganska naturligt eftersom det är journalister vi pratar om. Hade det gällt kommunala tjänstemän hade man inte behövt ha den där sista biten. Det händer faktiskt att journalister vänder sig direkt till mig och säger, nu ska jag göra det här. Då brukar jag svara att jag inte behöver veta det, det räcker att din chef gör det.
60	P: Då har de ändå möjlighet att arbeta runt policyn, om de anser att den står ivägen för

	deras arbete.
61	I: Den finns egentligen till för att inte begränsa dem i sitt arbete.
62	P: Finns det något mer ni gör för att öka efterlevnaden, något som vi har missat att ta upp?
63	I: Man kan säga att folk successivt blivit mer och mer säkerhetsmedvetna med åren. Jag kommer ihåg att det tog 2 år innan vi skaffade en brandvägg. Dem tyckte inte att det var nödvändigt. Det är sådant man skrattar åt idag. Tex, inloggning på datorerna, varför ska man ha det? Det är ju bara jobbigt. Säkerhetsmedvetenheten har ökat successivt.
64	P: Det är ju rätt spännande med tanke på att ni inte arbetar med att öka medvetenheten.
65	I: Inte så utstuderat, det känns naturligt att det blivit så.
66	E: Alltså att utbildning och information sker efterhand, efter att det ifrågasätts. Tolkar vi det rätt där?
67	I: Ja, det kan man säga. Det märks framförallt på de äldre medarbetarna. Där man har tyckt att det här var inte så viktigt.
68	P: Om vi ska sammanfatta detta. Ni gör inte speciellt mycket för att öka efterlevnaden? Det är mer att ni undersöker en incident när den väl inträffar?
69	I: Korrekt
70	P: Och ni har inget utbildningsprogram?
71	I: Nej, det har vi inte. Vi ser ju till så att dem säkerhetsrutinerna vi har själva, som i sådana fall har med inloggning att göra.
72	P: Och ni upplever att era åtgärder är tillräckliga för att hålla er information säker?
73	I: Ja
74	P: Och att utbildningsprogram och vissa motivationstekniker är lite överflödigt för er or-

	ganisation?
75	I: Ja, rent datasäkerhetsmässigt så… Våra redaktioner anordnar ju sina egna säkerhetsutbildningar.
76	P: Det är mer decentraliserat? Dem sköter det själva?
77	I: Ja, det gör dem. Vi tillhandahåller inga it utbildningar själva.
78	P: Ger ni några direktiv på hur de mindre it avdelningarna ska sköta informationen om policys?
79	I: Nej
80	P: Det är upp till avdelningschefen?
81	I: Ja, vi jobbar uppifrån och ner. Vi lämnar över det till någon relativt högt uppe och så får de trycka ut det och gå ut med informationen.

7.3 Bilaga 3

Transkribering intervju 2

Rad	Replik
1	E: Vad är din arbetstitel?
2	I: Jag arbetar som informationssäkerhetssamordnare. Tidigare hette rollen IT-säkerhetschef, men sen ändrade man den till informationssäkerhetschef. Då tillhörde rollen fortfarande IT-avdelningen, fortfarande centralt i organisationen. Sen blev tjänsten vakant i 1,5 år, och då kom man på att informationssäkerhet är mer än IT. Det är ett begrepp som innefattar egentligen informationen, varav IT är förpackningen. Och förpackningar finns det massa olika sorter av, men informationen är fortfarande densamma. Så då flyttade man tjänsten till den centrala säkerhetsförvaltningen, och eftersom att mina kollegor inte heter ”chef” utan ”samordnare”, så är min titel också samordnare.
3	P: Vad omfattar ditt arbete med informationssäkerhet?
4	I: Initialt att styra ledare och samordnare i organisationens informationssäkerhetsarbete. Det har tagit några år, men nu är faktiskt den främsta rollen att kontrollera efterlevnad. Att följa upp, göra revision och granska.
5	P: Har ni några informationssäkerhetspolicys?
6	I: Nej, det finns inget behov. Vi har en säkerhetspolicy, och den reglerar allt som har med säkerhet att göra. Därmed har vi ett dokument som heter ”Riktlinjer och Anvisningar för Informationssäkerhet” som är direkt underställt säkerhetspolicyn. Det kan man tolka som en policy, men det är riktlinjer. Men eftersom att riktlinjerna är direkt kopplade till en policy, så är de lika bindande som policyn. Så det finns inget behov av en informationssäkerhetspolicy.
7	P: Exempelvis, vad är det för riktlinjer?
8	I: Ni kan få ta del av dem. De revideras en gång om året. Och innehåller i runda slag 350 olika anvisningar. ”Ska”, inte ”bör, kanske, eventuellt”, utan ”ska”. Det är ett politiskt beslutat dokument. Policyn tar vi i fullmäktige, riktlinjer och anvisningar tas i nästa steg, alltså i kommunstyrelsen.
9	P: Vem utformar dessa informationssäkerhetsriktlinjer?

10	I: Vi är flera, men det är jag som äger ansvaret för dokumentet och innehållet. Däremot har jag behov av annat stöd från juridiken, från IT-driftsidan inte minst, från HR, kommunikation. Så det är många som initialt har varit med och påverkat utseendet av den. Men jag har lett processen, och har sista ordet.
11	P: Vid utformningen, involverar ni också personal som sen ska följa riktlinjerna?
12	I: Det kan jag inte säga att vi har gjort. Vi har inte sett något behov av det. Bakgrunden till det är att den version till styrdokument som ni kommer att få ta del av är en vidareutveckling av ett tidigare styrdokument som hade brister. Men det var så man valde att utforma styrdokument på den tiden. Frågorna har inte varit nya, utan vi har bara förtydligat och satt ner foten och sagt att vi inte accepterar ”bör” utan det ska vara ”ska”.
13	P: Hur förankrar eller implementerar ni policyn i organisationen?
14	I: På flera sätt. Främst så har vi sett till att få ett politiskt beslut, det ger ett mandat till riktlinjerna. Efter det kommuniceras de till varje enskild förvaltning. Vår organisation består av 17 olika förvaltningar. I näringslivet så skulle man kunna säga att vi är huvudkontoret, och förvaltningarna är dotterbolag. Det finns en direktör i varje förvaltning och där finns också en utsedd samordnare för informationssäkerhetsfrågor som är min högra hand. Och då kommuniceras det ut till dem, vi publicerar information på vårt intranät till den stora massan. Första gången då styrdokumentet publicerades, 2013, så bjöd jag in mig själv till varje förvaltningsledning. I förvaltningsledningen sitter direktören och alla avdelningscheferna. Där hade jag en en-timmesdragning av ärendet om riktlinjerna, hur jag ser arbeta för att efterleva innehållet. Och sen har varje förvaltning fått i uppdrag att utse en kontaktperson som har i uppdrag att samordna frågorna på den lokala förvaltningen. En förvaltning kan ha mellan 300 och 5000 anställda, så de är olika stora. Men en utsed samordningsfunktion ska det finnas som ser till att informera de anställda och som är ansvariga för efterlevnaden i sin förvaltning.
15	E: Ges det några direktiv till samordnarna för hur de ska förmedla riktlinjerna?
16	I: Från vår sida så lägger vi oss inte i de enskilda förvaltningarnas arbete för att 17 förvaltningar kan ha olika sätt att arbeta med managementfrågor. Det vi istället gör är att vara tydliga med vad som behöver kommuniceras ut och sen har vi också i uppdrag att leverera i den mån det går exempelvis utbildningar. Vi har en central utbildning som alla anställda har tillgång till på vårt intranät. Varje förvaltning avgör själva om varje anställd på förvaltningen ska genomföra utbildningen. Statskontoret ger dem möjligheten.
17	P: Den utbildningen som finns på intranätet, hur ser den ut?

18	I: Den hittar ni på MSB.SE också, för vi använder oss av DISA [anm: Datorstödd Informations-Säkerhetsutbildning för Anställda] som är en kostnadsfri utbildning som tagits fram av den myndigheten i sverige som har det nationella samordningsansvaret för informationssäkerhet. Den erbjuds till alla som vill använda den.
19	P: Var utbildningen frivillig?
20	I: För vår del så är den frivillig. Eller det är snarare som så att det är upp till förvaltningarna att själva avgöra om utbildningen är tvingande eller inte. På den förvaltningen som jag arbetar på, Stadskontoret, så har vår chef sagt att alla ska genomföra utbildningen. Så redan när man anställs, i rekryteringen, så finns utbildningen med i introduktionscheklistan. När man anställs i organisationen så får man en introduktionschecklista med saker man ska genomföra under de första två veckorna, ungefär. En av dem sakerna är att genomföra utbildningen och så ska chefen sedan skriva under efter genomförandet. Sen behöver inte det innebära att man har förstått någonting, bara för att man har genomfört utbildningen.
21	P: Vad innehåller den utbildningen?
22	I: DISA går att jämföra med en utbildning i handbrandsläckare, om vi pratar brandskydd. Eller en allmän brandutbildning, ”varför börjar det brinna och om det börjar brinna, vad gör jag då?”. På motsvarande sätt så tar DISA upp hur man ska tänka generellt kring hantering av information i olika förpackningar. Men mest med fokus på digital informationshantering.
23	P: Hur vanligt förekommande är det att anställda inte följer informationssäkerhetsriktlinjerna?
24	I: Det vågar jag inte svara på. Vi är 24000 anställda. Jag brukar resonera som så, att vi är så stora och så många att det man kan tänka sig kan hända, det händer i vår organisation. Men det ska snarare vara undantag än regel.
25	P: Mäter ni det på något sätt?
26	I: Det gör vi. Men resultatet är inte vetenskapligt förankrat. Vi har gjort uppföljningar de senaste åren där vi ställt frågor till medarbetare och chefer via enkäter. Frågorna har utgått från styrdokumentet, och så har vi valt ut målgrupper för dem olika frågorna. En av frågorna till medarbetargruppen har varit ”Har ni genomfört utbildningen som finns på vårt intranät?” och 2015 så svarade 9 av 10 att de inte hade genomfört den. Så det är ett sätt att följa upp efterlevnad av styrdokument. Då förstår ni också att även om det inte var en vetenskaplig studie, så ger det en fingervisning på hur det ligger till i just det avseendet. Resultatet av det var att ”det här är ju inte acceptabelt” och effekten av resultatet har blivit åtgärder som man på kommunal ledningsnivå har beslutat att kommunicera ut. Till exempel här på stadskontoret, där vi är 300 medarbetare, så sa vår chef ”det är såklart inte okej att inte 9 av 10 har gjort den, utan här ska alla göra den”. Därför beslutade man att alla ska genomföra utbildningen, och sen förde man in det momentet i introduktionschecklistan. Så jobbar vi också för att våra andra förvaltningar ska tänka i frågan. En del gör det, en del gör det inte.

27	P: Vilka orsaker kan det finnas för att anställda inte följer riktlinjerna?
28	I: Alla man kan tänka sig. Ren okunskap, omedvetenhet. För mig som har arbetat med frågorna i rätt många år så kan jag tänka mig att vissa ibland vet vad som gäller, men gör en egen liten avgränsning. Man tar ett eget beslut. Vår organisation och våra arbetsgivare har varit tydliga med att vi ska vara tillmötesgående och ha stor tillit samt förtroende för våra medarbetare. Vårt ansvar är att tydliggöra för medarbetarna vad som gäller. Men vi har i en hel del fall inga tekniska begränsningar eller tekniska lösningar som omöjliggör, utan det är upp till en själv. Arbetsgivaren berättar för dig vad som gäller, men sen går du själv. Så du tar själv ett aktivt beslut att göra si eller så. Men där har vi också varit tydliga med att om du tar ett aktivt beslut som exempelvis går emot våra riktlinjer så finns det ett avsnitt i riktlinjerna som reglerar påföljder om man inte följer riktlinjerna. Det kan bli arbetsrättsliga, civilrättsliga åtgärder om det visar sig att det var jätteallvarligt. Det kan också bara bli någon form av reprimand eller att man får förklara sig om det uppdagas.
29	P: Vad har ledningen för informationssäkerhetsansvar?
30	I: Informationssäkerhetsfrågorna är alltid en ledarfråga, det är en chefsfråga. Varje medarbetare har givetvis ett ansvar utifrån sin vardag och den informationshantering jag har i min vardag är jag såklart ansvarig för. Att medarbetarna blir informerade om vad som faktiskt gäller, det är arbetsgivarens ansvar. Ytterst är det politiken där beslutet tas sedan respektive nämnd, för i varje förvaltning så finns det en nämnd som är ansvarig för den förvaltningens verksamhet. Socialnämnden är ansvarig för socialförvaltningens verksamhet. Tekniska nämnden är ansvarig för gatukontorets verksamhet. Tekniska nämndens upprag är att kommunicera behoven till förvaltningsdirektören som kommunicerar det till avdelningscheferna, som sen skickar vidare det till enhetscheferna och som slutligen kommunicerar ut det längst ut till den sista medarbetaren i ledet. Där har jag inte insyn fullt ut, överallt.
31	P: Vad gör ni mer för att fostra ett bra säkerhetstänkt genom organisationen?
32	I: Informationssäkerhet är bara ett område. Informationssäkerhet klustrar vi idag till området ”intern säkerhet”. Och Intern Säkerhet har också Fysisk säkerhet, lås, larm, hot & våld etc. Sen har vi krisberedskapsområdet där vi arbetar med risk och sårbarhetsanalyser, beredskapsplanering etc. Sen har vi också prevention, där vi arbetar med mycket riktade insatser mot medborgaren. Jag jobbar mycket med fokus på vår interna säkerhet i organisationen, medan mina kollegor på preventionssidan jobbar mot medborgarna, trygghet, det man läser om i tidningarna. Jag skulle vilja påstå att det är helheten, som vi också kommunicerar till våra medarbetare. Men vi portionerar ut det. Jag kommer med informationssäkerhet, någon annan kommer med något annat. Man kan inte se det här som isolerade frågor.
33	P: Tycker du att de anställda visar ett ansvarstagande mot organisationen och den information man hanterar?
34	I: Ja, det vågar jag nog påstå. Det har resultatet av våra undersökningar visat. Vi har en uppåtgående trend vad det gäller vår säkerhetskultur.
35	P: Hur kommer det sig?

36	I: Som jag sa inledningsvis, det är mitt arbete att sätta förutsättningarna i organisationen. ”Så här ska vi göra när vi pratar informationssäkerhet i vår organisation”. På samma sätt gör vi inom våra andra arbetsområden. Att följa upp efterlevnad och hantera resultatet av uppföljningen för att utveckla arbetet vidare är vad som göder en positiv trend när vi pratar säkerhetskultur. Men sen är vi en stor organisation och mycket kan hända, och det händer. Det är helt ofrånkomligt, ungefär som att bilar krockar på gatan.
37	E: Upplever du att de som inte arbetar med samma frågor som du gör har en bra säkerhetsmedvetenhet i organisationen? Fostras i det i organisationen?
38	I: Vi är en tillmötesgående och flexibel organisation som utgår från tillit och förtroende, men vi har ett ansvar att ge förutsättningarna oavsett om det gäller säkerhet eller något annat. Jag tycker att våra medarbetare är väl insatta och har en bra medvetenhet. Jag kommer från en mindre kommun med betydligt färre anställda, och den stora skillnaden jag ser är att även om frågeställningarna, behoven och lagstiftningarna är desamma i den lilla kommunen som i den stora kommunen, så är vår fördel här i denna organisationen att vi är stora och numerärt fler. Det ger oss möjlighet att dyka ner i detaljfrågor i mycket större utsträckning, än vad man kan i mindre organisationer. På ett sätt ger det oss förutsättningar att skapa en djupare bild, oavsett vilka frågor det gäller. När jag arbetade med säkerhet i den mindre kommunen så hade jag hela denna enhetens arbetsuppgifter. En person, åtta timmar om dagen. I denna enheten jag arbetar nu, så är vi fjorton stycken. Varav jag har 100% informationssäkerhet, och mina kollegor 100% krisberedskap. Jag hade då tidigare fullt ansvar för båda. Det innebär att vi kan bli mycket mer detaljerade i vårt arbetsätt, och då också när vi tar fram metoder och gör uppföljningar. Mycket mer exakt.
39	E: Förmedlar ni även till de anställda förståelse för varför riktlinjerna finns där i första hand?
40	I: I den nyskapande processen när vi tar fram nya styrdokument eller metoder så innebär det också att ta fram en kommunikationsplan. Den kommunikationsplanen ska vara ett stöd i genomförandet, i implementationsfasen. Dels finns det ”vad ska jag tänka på ur ett kommunikationsperspektiv innan beslut, när beslutet är taget och sen löpande under dokumentets livscykel. Så det sker parallellt. Kommunikationsplanen tar jag fram, men det är våra kommunikatörer på kommunikationsavdelningen som stöttar det arbetet. Om vi ska förmedla ett budskap så ska vi vara tydliga och konkreta, och inte formulera vår text så att den skapar fler frågor än svar. Det måste vara väl och noga genomtänkt när man publicerar det.
41	E: Händer det att anställda hör av sig till er och har frågor om riktlinjerna? För djupare förståelse?
42	I: Jag tror inte att de som medvetet går emot riktlinjerna är särskilt många, även om jag givetvis tror att det förekommer. De som hör av sig till mig hör av sig för att de har svårigheter med att tolka en anvisning eller inte förstår den fullt ut och behöver ett förtydligande. I några fall om året hör någon av sig och undrar ”varför har ni skrivit detta?”. Allt finns det belägg för. Men vi skriver inte en motivering till var och en av alla 350 riktlinjerna, utan det finns en liten ingress till respektive område som förklarar varför vi arbetar med just det området.
43	P: Du nämnde att vissa ibland har svårt att tolka dessa riktlinjer, är det något ni fokuserar på när ni utformar policyns?

44	I: Vi kan säga såhär, det är det som är det främsta underlaget till att vi reviderar dem en gång om året. Såklart kan det ske förändringar, lagar kan ändras. Vi har dataskyddsförordningen här nästa år. Som innebär att vi kommer behöva revidera styrdokumentet ganska mycket, när vi pratar personuppgiftsbehandling. Sen kan det komma till nya saker som vi kommer på. Men främst handlar det om att förtydliga riktlinjerna, anvisningarna, de ska inte vara uppsatser. För då läser folk inte dem. Utan det ska vara enkelt, lättillgänglig text som förklarar väldigt tydligt för dig vad som gäller. Men ibland är det svårt. Det är inte busenkelt att formulera sig. Därför behöver vi ibland komplettera med en mening, eller lägga ett litet komma eller parentes någonstans, bara för att få läsaren att förstå. Just det, det handlar ju om detta! Såhär ska jag tänka!
45	P: Jag kom på en till fråga gällande policys. Måste anställda skriva på ett dokument som kräver att de ska efterleva policysna?
46	I: Det gör man inte, däremot har vi mallar, anställningskontrakt kallar vi det. Som vi skriver på då. HR avdelningen har tagit fram den här mallen. Den ser ut på ett speciellt sätt. De som jobbar inom vård och omsorg till exempel, där finns det en klusul med om att man ska följa sekretessbestämmelser och så vidare. I riktlinjer för infosec kan man se i dokumentet, kap 6.4 tror jag, att vi uppmanar förvaltningarna att se till att de anställda skriver på en tystnadsförbindelse/sekretessförbindelse. Som offentlig anställd så har du per automatik i din anställning en tystnadsplikt. Vi pratar ej meddelarfrihet, alla anställda har ju rätt att uttrycka sina tankar om sin arbetsgivare i vilket forum som helst. Yttrandefrihetslagen. Men det finns en tystnadsplikt mot dig som jag arbetar med. Tex, hanterar jag mycket sekretess, och det kan jag inte prata hursomhelst med om. Det jag kommunicerar till HR, tex att jag vill revidera den mallen, för att jag inte anser att den är tillräckligt bra. För jag vill att det ska stå något i anställningskontraktet, som faktiskt alla anställda behöver skriva på. Där ska det stå en hänvisning till den allmänna tystnadsplikten utifrån ens anställning inom offentligverksamhet. Alla som börjar jobba i vår organisation, har inte kommit från en annan kommun. Folk kommer från andra arbetsgivare i näringslivet, utbildningar. Då är det här helt nya saker. Det kan ej ställas krav på att en nyanställd per automatik ska känna till det här[tystnadsplikt] . Då är vi tillbaka till arbetsgivarens skyldighet att informera medarbetaren om vad som faktiskt gäller. Detta kommer ni se, när ni läser styrdokumentet, att vissa frågor är predestinerade HR, ingen annan. HR. Det innebär att de som jobbar med HR, behöver ta tillsig anvisningarna, arbeta in dekm i deras befintliga rutiner, tex rekryteringsprocessen. Vilka frågor ska vi ställa under anställningsintervjun? Vilka bakgrundskontroller ska vi göra? Hur ska anställningskontraktsmallen se ut? Introduktionsprogrammet för nyanställda? Alla dessa grejjer, det är mitt jobb att se till så att HR kommer på dessa grejjer, om de nu inte kommer på det själva. Sedan punktmarkera att det blir gjort. Då kan du som samordnare sätta check för informationssäkerhetsfrågor centralt i organisationen på dem frågorna. Sedan går vi vidare till nästan enhet, upphandlingsenheten, som bara jobbar med upphandling. Punktmarkering där, se till att de lyfter in anvisningarna i deras vardagsrutiner, i sina checklistor, när folk hör av sig och vill göra upphandlingar, ska de veta ”okej, då behöver vi det här, och det här, och så ska vi göra såhär, då uppfyller man informationssäkerhetsrutinerna. Då är det check på den.

	Sedan går man vidare till kommunikatörerna, som arbetar med all publicering på intranätet och hemsidan. Då är det samma process där. Check på den. Tillslut byggar man in allt detta i centralt styrda processer. Sedan kan du jobba med uppföljning och efterlevnad.
47	P: Vi har täckt medvetenhet, och vi har pratat lite om utbildning. Ni själva som jobbar med informationssäkerhet, hur utökar ni er kompetens inom området?
48	I: Deltar i nätverk, externa nätverk, det finns ett Infosec nätverk för kommuner, för alla som arbetar med dessa frågor. Nätverket leds och styrs av sveriges kommun och landsting, och samhällsskydd och beredskap. Där har vi ett forum där vi delar med oss av styrningsdokument, utbildningsmaterial, beslut, antingen man kan tänka sig för att stötta varandra. Det finns också internationella nätverk som vi är med i. Tex Euro city, som är dedikerat för europeiska städer med en befolkning över 300tusen. Där man träffas regelbundet, frekvensen varierar beroende på mån av tid. Utbildningar, konferenser av olika slag. Detta är ett område där fokuset ökar ständigt. I och med det följer den kommersiella biten också med att leverera fler utbildningar, och fler utbildningsaktörer, och fler möjligheter att kompetensutveckla sig.
49	E: Vi har ju pratat om att det finns repressalier. Är det några enklare brott kanske man diskuterar med den anställde.
50	I: Vi utreder inte brott, det överlämnar vi till dem som har i uppgift att göra det. Polisen. Det vi kan konstatera, det vi gör är att granska efterlevnaden av våra policys. Och det är inget brott att bryta mot policys. Därför byter vi ut ordet brott mot bryt. Man bryter mot våra policys. Beroende på vad det är kan man behöva göra en utredning, internt. I det arbetet kan man komma fram till att man misstänker, eller att det är helt uppenbart att det också begåtts ett brott. Då tar vi ställning till ifall det ska bli en polisanmälan eller inte. Vårt fokus är har du följt arbetsmiljölagstiftningen eller våra interna policys. Det är main priority.
51	P: Övervakar ni anställda, beteende, och ser ifall dem bryter/ följer dessa riktlinjerna ?
52	I: Från och till, i riktlinjerna ser vi att det finns en anvisning som tydliggör att vi kan göra det. Att vi gör det. Och utifrån det, vilka förutsättningar.
53	P: Vad är det för...
54	I: Det kan vara nätverkstrafik, kontroll av lagring. Vi har restriktioner till vad och hur medarbetare får använda sin tjänsteutrustning, telefonen, dator och paddan. Där har vi vart tydliga med var och hur man kan använda de. Också, vad vi kan göra för granskningar för att kontrollera lagring och sånt där, så att det inte sker privat. Så vi går inte in och kollar vad det är, på viss fillagrnings typ-nivå, kan man göra. Men det är ingenting som vi gör i realtid, alltid. På hela organisationen, det är väldigt omfattande. Vi gör övervakning i den mån att vi ser behov helt enkelt. Tidsmässigt också utifrån vissa bedömningar.
55	E: Görs det mer som på en stickprovs basis, eller när det finns misstanke om en brytelse?

56	I: Jag skulle vilja påstå det första.
57	E: Finns det några incitament för att följa riktlinjerna, tex belöningsform eller uppmuntran. Precis somen viss motivation att veta att man kan bli övervakad.
58	I: Jag tror inte övervakning som sker i stickprovsform, tror inte jag är något som – jag har varit här 6 år- jag har inte fått någon indikation från något håll att den eventuella övervakningen skulle vara bekymmer't. Vi har skrivit in i riktlinjerna för att tydliggöra för medarbetarna att vi faktiskt har rätt att och kan göra det. Det är inte vårt huvudsyfte, utan vi arbetar med att skapa motivation, medvetenhet. Jag brukar ställa 3 krav på medarbetare, detta kommunicerar jag alltid när jag är ute och föreläser. 3 Krav: Du ska veta vad du gör, varför du är här, för vem du gör det, och vem som ställer krav på det du gör. Har du svar på dessa frågor kan du känna dig ganska trygg i din tjänsteutövning. Alla vi som arbetar i vår organisation arbetar för kommuninvånarna. De är mottagarna av allt vi gör. Min roll, tex, är inte direkt riktad mot medborgarna. Mitt fokus är organisationen. Mitt uppdrag är att vi som organisation har förmåga och leverera det som organisationen ska göra till medborgarna. Vi är den verksamhet i Sverige som är mest lagreglerad. Ingen annan offentlig verksamhet är så lagreglerad som den kommunala. Bara på säkerhetsområdet, skulle jag kunna rabbla 100 författningar eller lagstiftningar som reglerar kommunalt säkerhetsarbete på ett eller annat sätt. Det hittar ni inte i någon annan organisation. Vi har offentlighet och sekretesslagen, personuppgiftslagen, patientdatalagen. [vård och omsorg] en stor del av den kommunala verksamheten, oavsett om vi pratar vår storlek eller mindre. Vård och omsorg är en tredje del eller hälften av den komunala verksamheten. Där är det urtuffa krav för sekretess, och det är dem väl insatta i. Det finns ingen morot mer än att se till att göra rätt, och vi ska kunna stå rakryggat ifall något av det vi gör ifrågasätts. Att vi har gjort det som kan förväntas göras av oss. Det är den moroten vi har. Inga bio-checkar eller fancy utflykter eller middagar.
59	P: Konsekvenser, belöningar och övervakning kan ses som yttre motivationsfaktorer som ni kan använda eller applicera för att forma deras beteende.
60	I: Vi vill inte styra det[beteenden] genom övervakning, men vi tycker det är viktigt att möjligheten finns. Det är klart att vi ska ha koll, hur kan man annars kontrollera efterlevnad. Men det är ju inte så att vi hugger direkt. Utan det kan vara att vi i samband med ett stickprov konstaterar om det är någon beteende grej, någon okunskap. Det genererar kanske en utbildnings eller informationsinsats, ur ett brett perspektiv, snarare än på individnivå.

61	E: Skulle du säga att övervakning är en integritetsfråga?
62	I: Det är det ju, men o andra sidan har arbetsgivaren en rätt. I min tjänsteutövning har jag ett uppdrag och jag använder arbetsgivarens utrustning, och arbetsgivaren har berättat hur jag får använda den. Om jag använder den mot dig, gör jag det antingen av okunskap eller med full medvetenhet. Skulle det vara att det uppdagas så kan det få följder beroende på vad det är för typ av aktivitet jag har gjort. Återigen, vi är många anställda, sett över ett årsperspektiv är det inte en promille ens, på det sättet.
63	P: Använder ni något mer motivationsteknik, utöver övervakning, sanktioner och belöning?
64	I: Jag kallar inte övervakning motivation på det sättet. Motivation för mig är en känsla av trygghet hos medarbetaren att jag gör rätt. Jag som arbetsgivare-representant, vilket jag kallar mig själv då jag kanaliserar ett politiskt budskap, har ansvar för det. Det ska vara lätt att göra rätt, helt enkelt, och svårt att göra fel. Men det kommer alltid att finnas möjlighet för att göra fel. Och det kommer alltid finnas en möjlighet för medarbetarna att nyttja arbetsgivarens utrustning, på ett sätt som kanske inte är förenligt med arbetsgivarens värdegrunder. Det kommer nog att finnas i alla organisationer, sådant här arbete när vi pratar säkerhet, trygghet, tillit, förtroende är beroende av människan. Den enskilde medarbetaren. Människan är en förutsättning, en tillgång men också en risk. Min roll är att minimera risken. --- Följer ni några standarder eller ramverk när det kommer till efterlevnad, utbildningsprogram eller policy?
65	I: Det gör vi. Vi har valt att följa ISO 27000 standarden. Den omfattar ganska många delar. Vi har valt del 1 och 2. Vi har valt att använda den som best-practice. Vi har ingen ambitions att certifiera oss, utan vi har valt dem delar vi tycker är tillämpbara för oss. Vi har valt omfattningen i dem delarna också, på en nivå som vi anser rimlig och lämplig för oss.
66	E: De hanterar inte efterlevnad så ingående, hur det kan uppnås. Jag tänker på ISO 19600 för compliance. Har ni någon ytterligare standard för efterlevnad?
67	I: Det vill jag påstå. Vi har ett styr och ledningssystem för vår organisation. Vårt interna kvalitetssystem. Sen har vi något som kallas intern kontroll, vilket innebär att utöver de granskningar jag själv gör i min vardag(enkät uppföljningar, stickprovskontroller) hur jobbar den förvaltningen med systemsäkerhet kring IT-system. För varje förvaltning och nämnd har sina egna IT-system. Sen har vi den centrala driften som driftar systemen, men ägande och förvaltningsansvaret har den enskilda nämnden. Då har jag ställt krav på hur dem ska jobba med dem bitarna. Jag följer upp hur dem arbetar med det, granskar alla säkerhetsåtgärder och skriver protokoll. Det andra då, intern kontroll som är lagreglerat, genomför varje år ett antal kommunövergripande frågeställningar, som bestäms centralt. Alla verksamheterna över (stad?) ska kontrollera, tex informationssäkerhets efterlevnaden 2015. Nu är inte infosec varje år, men det har förekommit. För den kommunala offentliga verksamheten är intern kontroll det starkaste instrumentet för att påverka efterlevnaden av någonting. Där redovisar man resultatet till politi-

	ken, och då behöver man följaktligen göra någonting åt det. Sedan har vi något som heter stadsrevisionen som granskar nämndernas ansvar. Intern kontroll som jag nämnde först, där granskar nämnden sig själv. Medan stadsrevisionen är en politiskt tillsatt organisation som har till uppgift att granska våra nämnder. Tex nämnderna kontrollerar sig själva, sedan konstaterar stadsrevisionen nämnden kollar ej sig själv, det är en avvikelse. Då föreslår man åtgärder. Dem granskar också infosec. Sedan har vi styr och ledningssystemet i övrigt. Det är många påtryckare för att kontrollera efterlevnaden. Där varje aktör eller instans redovisar sitt resultat. Och varje sånt resultat lägger till ett litet steg på mognadstrappan.
68	E: Skapar en helhetsbild över hela organisationen när det sammanställts.
69	I: Jag vet inte hur det funkar i näringslivet, men jag kan tänka mig att det är en skillnad i det.
70	P: Känner du att vi har missat att ta upp något som ni gör för att öka efterlevnaden, som vi inte pratat om?
71	I: Jag tycker att ni sammanfattat frågorna rätt bra. Det finns förutsättningar, varje enskild förvaltning och medarbetare behöver gå själv. Ibland behöver man hålla dem i handen, ibland sätta ett finger i ögat eller pannan. Men överlag handlar det om att kommunicera budskap och vara tillgänglig och svara på frågor. Vi har ju många som arbetar med dem här frågorna. HR de kan svara på infosec relaterade frågor utifrån sitt ansvarsområde. Juridiken arbetar med detta varje dag. Kommunikatörerna på sitt sätt. Kris och beredskapssamordnare arbetar med riskanalys till exemepl, och kontinuitetsplanering, vilket är ett kapitel i 27000. Det jag säger då, i vår organisation ska vi arbeta med kontinuitetsplanering. Men jag gör inte det själv, utan det gör dem. Sedan följer jag upp det.
72	E: Då är vi klara. Tack så mycket. Du får en kopia av transkriberingen när den är klar, och inspelningen kommer att raderas.

7.4 Bilaga 4

Transkribering intervju 3

Rad	Replik
1	E: Hur ser den organisationen som du arbetar i ut?
2	I: Vi är ett företag som heter XXX. Vi är 9 personer, 6 stycken sitter i ZZZ, 2 stycken på ett kontor i YYY och en till som är under uppstart som jobbar mot Halland i RRR. Företagets och dess medarbetares uppgift är att vara oberoende rådgivare, huvudsakligen inom IT-området. Ska man förenkla det så är ett typiskt uppdrag för oss att arbeta som deltidsanställda IT-chefer, eller IT-rådgivare. Till mindre organisationer så är det ofta vi som får hela IT-ansvaret, för då har man ingen egen avdelning för IT. I större organisationer så har man oftast en IT-organisation, och då kan vi jobba som rådgivare, mentorer, bollplank eller ta hand om specifika IT-projekt och upphandlingar. Jag är en av delägarna i företaget, och mina arbetsuppgifter är helt beroende på vilken typ av kund som vi jobbar med. I dagsläget jobbar jag med tre företag. En större organisation, en lite mindre som omsätter runt hundra miljoner – handelsföretag, där jag har rollen som IT-chef. Sedan även ett tredje där jag har drivit lite större affärssystemsprojekt. I det företaget har jag i första hand mer rollen som upphandlare, och projektledare i andra. Svaren jag kommer lämnar blir väl lite mer generellt utifrån de företag jag arbetar mot.
3	P: Hur kommer informationssäkerhet in i arbetet?
4	I: Det är nuförtiden lite av en vardagsuppgift. Säkerhet är en stor fråga hos företag. Det finns många aspekter på säkerhet och IT. Vi blir inblandade i stöldskyddsfrågor, om man nu ska ta en typ av säkerhet, det vill säga larm, dörrlås och koder. Alltså den typen av system. Det är en del av det, den andra säkerhetsfrågan när man pratar IT är generellt sett, det man råkar ut för. Då pratar vi antivirus, hackningsförsök och sånt.
5	E: Utöver fysisk och teknisk säkerhet, hur arbetar organisationerna du jobbar mot med administrativ säkerhet, såsom policy och dess efterlevnad?
6	I: Ja, det är bra att vi kommer in på policy, för det är i våran roll viktigt. IT-policyn är ett dokument som i många lägen är en grundpelare. Vi som ansvariga rådgivare på IT-sidan jobbar ganska mycket med att det finns en genomtänkt policy att efterleva. Det är en första nivå, att det faktiskt finns en policy. Nästa nivå är efterlevnaden. Där jobbar vi på det viset att vi försöker implementera policyn i andra rutiner. Tar vi personalfrågor så handlar det om att när någon ska börja på ett företag, nyanställning, så behöver man ha en process där man hanterar nycklar, datorer, telefoner och så vidare. Och i samma veva så behöver man prata IT-policy också, för det är ett dokument som alla måste få ha fått säga okej på när de startar sin anställning.
7	P: Vem är det som utformar och skapar policys?

8	I: Ja, oftast så är det den som har fått ett IT-ansvar. Jag kan tycka att det är en ledningsfråga, det är en fråga för ett ledningsrum och en ledningsgrupp. Men krast så kan man påstå att det tyvärr lite för ofta är en fråga som ”sätt du ihop en sån” och så får IT-chefen den sen. Finns det ingen IT-chef och vi inte är där, då åker väl någon ekonomiansvarig på det.
9	E: När man tar fram en policy, vilka borde då involveras i arbetet? Involveras i regel andra?
10	I: Det där behöver vara någonting som har input från alla avdelningar i bolaget. Det tycker jag, för det är något som berör samtliga i företaget. Är man ett större företag så är HR en viktig del i det [utformandet], för de har ofta personalansvarsfrågorna och kanske den första kontakten gentemot fackliga organisationer. För att en IT-policy sätter en hel del regelverk eller ramar för bör, får och ska jobba med IT-frågor. Som medarbetare kan man anse att det kan vara ganska, låt oss säga tuffa saker, som står där i – och vilket ansvar man har som anställd. Därför behöver den synkas, dels med alla avdelningar så att man är överens om den dels naturligtvis gentemot HR och fackliga organisationer så att man är överens på den sidan med.
11	P: Hur kan man förankra policyn i organisationen?
12	I: Den första, och relativt vanligen lyckas, är att ha ett dokument som man får ta del av i samband med att man startar sin anställning. Det är det första tillfället. Jag ser gärna att man i det läget har både fått läsa och signera det faktiskt. Alltså att man sätter sin namnteckning på och säger att ”jag är med på vad som står där i och jag ska jobba efter det”. Då är vi överens i det första läget. Sen behöver den [policyn] naturligtvis finnas tillgänglig. Många har någon typ av arkiv för dokumentation. Om det är ett ledningssystem eller om det är ett intranät, alltså där man har personaldokumentation, så det där det ska finnas naturligtvis. Så att det alltid är tillgängligt för medarbetare. Sen vid revideringar så måste man naturligtvis gå med det dokumentet från ledning, som då säger ”nu reviderar vi våran IT-policy, följande förändringar gäller”. Om man reviderar dokumentet, på grund av… ja egentligen av att saker och ting händer väldigt snabbt nu. Jag ser många IT-planer som är gjorda för tio år sen, och det står samma saker i dom. Det står saker om hur man hanterar en fax, men det står ingenting om mobiltelefonen där man idag har lika mycket information eller mer än vad man har i datorn. Av den orsaken behöver man ofta revidera dom [policys] och förnya dom. Och i det läget behöver dom ut från ledning till respektive avdelning så att det verkligen kommer ut i hela bolaget igen.
13	E: Bör man lägga ner mer eller större arbete än att bara publicera den reviderade policyn när man förmedlar ut den?

14	I: Ja, det korta svaret är ja. Om man lyckas med sitt intranät i en organisation, då är det ett levande ställe där många är inne och tittar. Men långt ifrån alla trots allt. Tittar man på hur det ser ut i verkligheten så är inte alla medarbetare inne och tittar där. Det innebär att om jag går in och skriver en uppdatering på min IT-policy och lägger upp version två på intranätet, så innebär det inte att det är implementerat i min värld. Utan, nu finns det ett nytt dokument, men det har inte medarbetare köpt, om man får uttrycka sig så. Alltså accepterat vad som står där i, utan som alltid måste det vara någonting som man presenterar ut, när det är så pass viktiga saker.
15	E: Brukar organisationer arbeta med att skapa förståelse för varför policys och riktlinjer finns där i första hand?
16	I: Om det brukar… Nej, det kan jag inte säga. Det finns jättebra exempel på organisationer som arbetar med IT-policy och andra sådana dokument på ett proaktivt sätt. Det gör det absolut. Men det generella företaget som jag stöter på så är svaret att: nej, inte innan vi kommer dit och dels driver den frågan. Men det måste också finnas en accept från ledningen om att det är en viktfråga. Och där är det väldigt olika beroende på vem som leder och driver företaget och dess erfarenheter. Det finns jättemycket mer att göra där, och det blir allt viktigare, i och med att det blir en större och större fråga för företaget. Det enkla svaret på detta är faktiskt att företag som har intrat IT har en konkurrensfördel. De har satt sin IT-ansvarige i ledningsgruppen. Då finns det ganska bra förutsättningar. Den som säger att ”IT är en stödjande process”, och det är det, men… ”IT är någon som springer i korridoren och fixar med någons mail i telefonen, eller kopplar in en ny skrivare.” Den har inte riktigt samma intresse av att lägga tid och kraft på IT och IT-policys så att de blir implementerade på ett bra sätt.
17	P: Vilka orsaker kan det finnas till att anställda inte följer säkerhetspolicys?
18	I: Ja, i första läget så är det mognaden egentligen för IT och hur viktig den anses vara för organisationen. Det är nog den största, men sen finns det otroligt mycket saker att fokusera på. Att bli mer effektiv i sin produktion, fokusera på sälj eller fokusera på allt det som är kärnverksamhet. Då måste IT komma lite lägre i prio.
19	P: För att öka mognaden så är det alltså bra att ha med IT-chefen i ledningsgruppen. Men bortsett från det, vad mer kan man göra för att skapa ett säkerhetstänk bland anställda?

20	I: Idag är det som så att det IT-säkerhet berör, och de största riskerna egentligen upptäcker man att det är medarbetarens misstag, får vi nog uttrycka det som. För det är väldigt väldigt sällan det är illvilja. Går vi tillbaka de senaste tolv månaderna så har ordet ransomware, som ni säkert hört talas om, blivit ett av de stora bekymmer som poppat upp, och tidigare inte varit en fråga. Jag har stött på en handfull företag senaste tolv månaderna som har råkat ut för den här typen av händelser. Vad som har hänt är att en medarbetare har fått ett mail, normalt sett, och tror att det faktiskt är PostNord, eller Swedbank eller Nordea, som har skickat ut någonting och tänker ”att det här är nog bäst att ta tag i”. Och då kan det vara okunskap eller slarv som gör att de klickar på den där länken, som man inte ska klicka på. Det är en ganska ny företeelse att man kan orsaka jättestora problem, kostnader och driftstörningar genom att man klickar på en länk i ett mail. Det som är relativt vanligt nu är att man fokuserar kraften, när det gäller just IT-säkerhet, till att utbilda personal. Utbildandet i det avseendet avser huvudsakligen E-learning-programvara. Det vill säga att man får gå igenom ett program. Det finns företag som säljer den typen av utbildningar, kan man säga. Där man får ett mail i veckan, eller hur ofta det nu kan vara, och som medarbetare får man chans att då besvara lite frågor kring det här med hur man ska hantera osäkra mail eller vilket område det nu är som anses vara säkerhetsfrågor.
21	P: Får alla anställda genomföra samma utbildning?
22	I: Ja, om man har ett arbete som innebär att man har access till datorer som är inkopplade på företagets nät.
23	P: Om man bortser från exempelvis lagerpersonal. Gäller samma utbildning för chefer och medarbetare?
24	I: I grovt kan man nog uttrycka att tjänstemän, kontorspersonal, generellt: ja absolut. Sen är det kanske lätt att glömma den där lagerpersonalen som du nämner, för att lagerpersonalen har access till lager- och logistiksystem, transportadministration och där med internet, mail och hela den biten. Så att egentligen alla som har access till datorer som finns på företaget och nyttjar dem i sitt arbete.
25	P: Du nämnde att utbildningarna innehöll frågor som man fick svara på som anställd. Sammanställs det för att se var det kan behövas extra insatser?
26	I: Ja, det gör man. Det finns företag som är duktiga på den här sortens utbildningar, och i paket när man genomför dem brukar man först fokusera på att genomföra utbildningarna och få alla att göra dem, naturligtvis. När det är gjort sen, då kan man backa tillbaka och titta på svaren, bearbeta resultatet av det och konstatera ”ja, i stort sett alla förstår sig på den och den frågan, men inte den här”, och då har man möjlighet att göra aktiva insatser på de områdena där man känner att ”här måste vi lära folk ännu

	mer”. Så det finns bra verktyg för det i de här produkterna tycker jag.
27	E: Det låter som ett sätt att mäta säkerhetsmedvetenhet i organisationen?
28	I: Ja.
29	E: Finns det andra verktyg eller metoder som man använder för att mäta efterlevnadsgraden i av säkerhetspolicys i organisationer?
30	I: Det gör det, men tyvärr så används det ganska lite. Ett verktyg för att nyttja det och få med frågor är naturligtvis medarbetarenkäter och den typen av undersökningar. Dom handlar ofta om hur man som anställd mår, trivs och vilka förbättringar man tycker man kan göra på företaget. Men där har man ett tillfälle att ställa ett gäng frågor till medarbetare. Där skulle man kunna nyttja chansen att prata medvetenhet kring IT-säkerhet.
31	P: Ni som arbetar med dessa frågor, hur utökar ni er kompetens inom ämnet?
32	I: Dels så jobbar vi inom företaget med vad vi kallar Kompetensgrupper. Det betyder egentligen att vi ser till att ha ansvariga personer och små grupper som driver kompetensen i respektive område. Det kan vara allt från säkerhet till affärssystem till driftansvar och så vidare. I de grupperna så ingår dels att köpa utbildningar och gå utbildningar inom respektive område. Det andra är att träffa leverantörer, vi har ett väldigt stort kontaktnätverk på leverantörssidan, det vill säga IT-företag som är duktiga på olika saker. Det kan vara allt från PUL, eller numera GDPR, till alla andra kompetensområdena. Man kan säga att vi dels lyssnar på leverantörsföretagen, på vad de är duktiga på och hur de arbetar med frågorna. Och dels går vi kurser och utbildningar för att skaffa oss den kunskapen löpande.
33	E: Hur motiveras anställda att följa policys? Används några motivationstekniker?
34	I: Återigen är nog svaret att nej, det brukar man inte. Det är ofta någonting som man har som en alldeles för sällan företeelse. Det är ingenting som kommer per automatik. Vi vill gärna driva de här frågorna, IT policy. Att de ska revideras på årsbasis, det är en del av årsplanen för IT. I samband med att man reviderar dem så är man en mindre grupp som tittar på om de är moderna och färska eller inte, och om något behöver ändras. Men om man brukar? Nej, det är sällan man jobbar med någon typ av annan motiverande än att – “du är anställd här, därmed gäller ett antal ramar som vi faktiskt har bestämt inom verksamheten”.

35	E: Hur ser du på övervakning av anställdas beteende, för att kunna fastställa om policys efterlevs eller inte?
36	I: Det finns allt fler möjligheter till det. Framförallt om man tittar på mobiltelefonsidan. Framförallt lite större verksamheter administrerar ofta mobiltelefoner centralt idag. Det vill säga att de har programvara som kan styra innehållet. När du får din telefon kan vi skicka ut appar som måste finnas på telefonen. Man kan se data förbrukning och sådana där saker. Men i syfte att övervaka.. Nja, det är väldigt väldigt sällan ett företag vill göra det. Då hamnar man i en mycket mycket svårare situation som handlar om förtroende och om man litar på sin personal eller inte. Och det gör man generellt. Annars hade man inte haft den [personalen]. Men det som definitivt övervakas är dataförbrukningar och sådant. Men det gör man oftast ur ett kostnadsperspektiv, snarare än att kolla om personer efterlever policyn. Lägger du dokument på rätt eller fel ställe, använder du USB-stickor och råkar slarva bort dem. Alltså den typen av händelser i övrigt.
37	P: Låt säga att någon hanterar ett dokument fel, att informationen misshanteras. Vad får det för följder för den personen, hur hanterar organisationen det?
38	I: Det här är företagsinformation och det beror precis på vad det är för information, men det är naturligtvis en jätteallvarlig fråga, om det är någon som till exempel tar ut ett kundregister och sparar ner det någonstans, och tar med det utanför företaget, och så uppdagas det. Det är en superallvarlig fråga, givetvis. Det blir en IT fråga på så vis att IT blir inblandade för att ta reda på vad som är fakta, “vad har hänt? Vad har mailats, eller vad har tagits ut?” och så vidare. Men konsekvensbiten är egentligen ingen IT fråga, utan det är en personal och ledningsfråga. Alltså är det grund för en varning eller en uppsägning? Alltså sådana saker. Det blir ingen IT-fråga, det är mer en ledningsfråga. IT blir involverade i att ta fram fakta.
39	P: Till exempel om det är vanligt förekommande att man bryter mot mindre grova policys, exempelvis att man inte loggar ur sitt användarkonto och går från jobbet. Hur hanteras det?
40	I: Det enkla svaret är att om det är IT som upptäcker det så tar de den dialogen rakt av med medarbetaren. Om man upptäcker någon typ av slarv eller misstag, då kan vi påminna den personen om att det är fel. Upptäcker man att det är väldigt vanligt att man använder mobiltelefonen på ett obegåvat sätt eller riskfyllt sätt eller till exempel tar med sig känslig data ut ur företaget och lagrar det på sin privata dropbox. Vanligtvis är det så att IT upptäcker det och säger, “här har vi säkerhetsrisker”. Vilket återigen, för IT är det, eller borde det vara, en årligen återkommande revision. Sen lyfts det till en ledningsgrupp oftast. Där radar man upp de olika utmaningarna, här har vi brister eller risker på IT säkerhetssidan som vi måste ta tag i. Och utifrån det får man ta fram ett åtgärdspaket. Hur får vi ut den här kompetensen? Det är ofta kunskap som saknas hos medarbetare, inte illvilja. Sedan får man utbilda personal, ofta på dem arbetsplatsträffar eller avdelningsmöten eller vad man nu har inom organisat-

	ionen.
41	P: Följer ni några standarder eller etablerade best-practices för policy, utbildningsprogram eller just för compliance?
42	I: Gällande policys har vi arbetsmetoder för att bygga upp dem. Låt säga att det saknas en IT-policy hos ett företag, vilket är rätt vanligt får jag nog erkänna. Så kommer vi dit, och så får vi i uppdrag att implementera det. Då har vi en metodik för hur vi går tillväga. Men den metodiken är mer byggd på best-practices snarare än någon formell metodik. Sedan finns det ju standarder och metoder för att genomföra säkerhetstester i organisationer. Inom EU finns det sådana standarder. De är rätt generella och oftast riktade till stora organisationer. De passar sällan små och medelstora företag. Vilket innebär att då blir det mest best-practice och erfarenhet från vårat håll, och våran metodik vi bygger fram.
43	P: Gällande best-practices om policys, vad är det för best-practices och varför används de?
44	I: Låt oss säga att vi ska implementera en IT-policy hos ett företag. Då är det erfarenhet och kunskap om området som gör att vi är aktuella att hjälpa till hos företaget. Vi startar sällan från vitt papper. En färdig mall för någonting är bra att ha, det kan vara rubriker och den typen, snarare än färdiga fakta. Någon som får färdig fakta beskrivet för sig kan tycka att det låter bra, “det kör vi på”. Den texten kan vara jättebra, och innehållet kan vara jättebra innehåll, men problemet är att det efterlevs inte för att man inte har tagit fram materialet själva. Som alla viktiga dokument, om man jobbar fram materialet själv har man större chans att få det att fastna. Får man något ”skrivet på näsan”, om man uttrycker sig så, som säger att “så här är det”, då är det mycket svårare att få det att efterlevas. Det handlar om delaktighet, att andra får vara med och ta fram sakerna, och att de kan känna att det här är något jag vill skriva under på. Om alla har varit med och tyckt till om policyn är det mycket lättare att få det att efterlevas. De best-practices vi tar fram dels är det erfarenhet och historik. Saker som vi märkt har funkat. Sedan är det nya saker som kommer in genom att omvärldens förändras. Vi utbildar oss till det, och då märker vi nya saker som vi måste ta med. En kombination av erfarenhet av saker som har funkat och nya saker som man behöver fylla på med.
45	E: Rent generellt, vilka är de största svårigheterna när du kommer ut till en organisation och ska hjälpa dem med policy arbete och dess efterlevnad?
46	I: Först är det att få högsta ledningen engagerad i frågorna. Om du har en VD eller en ledningsgrupp som tycker att “IT är en extremt viktig fråga för oss som organisation”, då är resan som konsult ganska enkel. Då finns det stort intresse och en förståelse för att det här är viktigt. Och därmed den som inte... “Vi är en verkstadsindustri och vi har alltid jobbat på detta viset. IT är att det går att skriva ut”. Det är klart, då finns det inte så stort intresse att

	driva igenom det. Det största problemet är då att om IT driver en fråga, och säger att “detta och detta är viktiga frågor tycker vi på IT”. Då får det en viss tyngd. Men om ledningen för bolaget säger att “det här är viktiga frågor för organisationen”. Då får det mycket större tyngd, och ett större fokus. Ledningen är en utav de största utmaningarna. Den andra är nog kompetens på IT sidan.
47	E: Du upplever att det kan vara bristande kompetens på IT sidan?
48	I: Ja, där vi kommer ut, där har vi ofta haft fördelen att det finns det någon som förstår att om de köper kompetens från ett företag och får ett gäng IT-kompetenta människor i leveransen från oss. Då får man färsk och bra information. Har du istället anställt någon till IT vars arbetsuppgift är mer riktad till att sköta dagliga ärenden, och tekniska problem, installation av telefon och dator osv. Jag vill inte förringa den typen av uppgifter, de är jätteviktiga, men den personen har sällan stor kompetens gällande IT-säkerhet och IT-policy frågor. Är du duktig på och tycker det är roligt att arbeta med installation av teknik, då är det det man gör mycket av. Är man däremot, mer som vi, rådgivare, då är det klart att man försöker ta en mer strategisk position. Då driver vi den typen av frågor.
49	E: Tycker du att organisationer borde ha eller har någon som enbart sysslar med informationssäkerhetsfrågor, med tanke på att det är väldigt relaterat till IT-frågor? Eller är det bättre att den rollen är delad?
50	I: Oftast är det rimligt att båda rollerna ligger hos en ansvarig på IT sidan. Beroende på bolag så har man en och samma person, eller så är det uppdelat. Nu är jag partisk, så det får man ta med en nypa salt. Utifrån mitt perspektiv, och det företag jag är med och driver- om vi inte har kompetens kring till exempel marknadsföring inom sociala medier då är vi ganska tidigt ute med säga att vi får köpa den kompetensen. En konsult exempelvis. I vårt fall är det just det vi jobbar med. Har du den tekniska delen, men inte den strategiska och administrativa, köp den delen av konsulter som både kan det och arbetar med det dagligen. Någon som kan hjälpa till och driva och komma i mål med sådana frågor.
51	E: Är det något annat du tänker på som du tycker att vi har missat angående policys och dess efterlevnad?
52	I: Med tanke på digitalisering och att allting ska kopplas upp så blir frågorna för IT och IT-säkerhet väldigt snabbt förändrade. Hantering av förändringstakten inom IT är en jätteutmaning för organisationer. IT planen finns där och har funnits där i 10 år, sedan säger man att “nu får vi nog titta över den”, och då gjorde man det för 5 år sedan och anser att den nu lever ett bra tag till. Men ta en funderare över vad som hänt de senaste fem åren inom IT. Det går så otroligt fort. Det innebär att IT-policys alltid ligger

	steget efter. Hur'et i att hålla sig ajour med policydokument, och framförallt efterlevnaden, och få ut den i organisationen. Det är ett riktigt centralt område. Det är många som har börjat fatta den biten nu. Det är medarbetarna vi måste utbilda, löpande. Det är det som är lösningen på våra säkerhetsproblem. Inte en bättre brandvägg eller bättre lås till porten. Utan det blir väldigt mycket fokus på att utbilda medarbetare så att de förstår vad dem gör när dem surfar eller klickar på en länk i ett mail.
53	E: Skulle man kunna säga att bra träning och medvetenhet hos de anställda gör mer för info-sec än policyn i sig?
54	I: Visst är det så, det tycker jag verkligen. Policyn är bara pappret som jag tittar på när jag är osäker. En IT-policy hänger inte på väggen i kontoret. Gör den det så tittar man inte på den. Det nästan som ett avtal. Ett avtal har man för att konstatera hur var det vi bestämde. När vi är överens tittar man inte på den. Av den orsaken blir policyn ett styrdokument vi plockar fram med jämna mellanrum. Men där i mellan måste vi säkerställa att folk arbetar på ett visst sätt och har kunskap. Då är utbildning mycket viktigare än att man kan rabbla innehållet i IT-policyn. Det ger mycket större effekt. Policyn kan man ändra en gång om året som mest, men oftast inte ens i närheten av så ofta. Medan vidareutbildning av personal, det kan man ta upp på varje måndagsmöte i en kort fråga, och tipsa om att "tänk på detta, eller tänk på att göra såhär". Det kan man göra under vardagen på ett effektivare sätt.
55	E: Tack så mycket för att du tog dig tid för intervjun.