LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Informationssäkerhetspolicyer i organisationer

Inblick i hur IT organisationer inom Sverige arbetar med utveckling och förmedling av informationssäkerhetspolicyer.

Kandidatuppsats 15 hp, kurs SYSK02 i informationssystem

Författare: Ardian Xhafa
Danial Dastbaravardeh

Handledare: Anders Svensson

Examinatorer: Umberto Fiaccadori
Magnus Wärja

Informationssäkerhetspolicyer i organisationer: En inblick i hur IT organisationer inom Sverige arbetar med utveckling och förmedling av informationssäkerhetspolicyer.

Författare: Ardian Xhafa och Danial Dastbaravardeh

Utgivare: Inst. för informatik, Ekonomihögskolan, Lunds universitet

Dokumenttyp: Kandidatuppsats

Antal sidor: 52

Nyckelord: Informationssäkerhet, Informationssäkerhetspolicy, ISP, Utveckling, Förmedling.

Sammanfattning (Max. 200 ord):
Vi lever i en värld där tillgängligheten till information är lättare än någonsin. Detta har medfört en ökad nivå av hot mot känslig information som existerar hos företag. Informationssäkerhet är inte längre en teknologisk fråga utan en mänsklig fråga. Människor är det största hotet mot informationen som finns på ett företag. För att hantera detta problem så väljer företag att skapa informationssäkerhetspolicyn som anställda måste följa för att minimera riskerna som kommer med informationshantering. Men hur ser processen ut i svenska IT organisationer när det kommer till utvecklingen och förmedlingen av informationssäkerhetspolicyer? Finns det några skillnader i hur företag gör när det kommer till utveckling och förmedling av informationssäkerhetspolicyer? Författarna har valt att utföra en kvalitativ intervjuundersökning hos tre IT organisationer för att få en inblick på om det existerar några skillnader när det kommer till företagens utveckling och förmedling av informationssäkerhetspolicyer. Resultatet av studien visade att det existerar skillnader mellan de tre företagen när det kommer till utveckling och förmedling av informationssäkerhetspolicyer.

Innehållsförteckning

Förkortningar

ISP - Informationssäkerhetspolicy

IS - Informationssäkerhet

IT - Informationsteknologi

Figurer

Tabeller

1 Introduktion

Vi lever i en mer digitaliserad verklighet där tillgängligheten till information är enklare än någonsin tidigare. Digitaliseringen ökar drastiskt vilket leder till att det allmänna hotet mot informationssäkerhet ökar. Idag handlar informationssäkerhet inte längre endast om att skydda sig från skadliga virusprogram, snarare handlar det idag mer och mer om integritet och andra aspekter kring informationssäkerhet som bör beaktas i och med den ständiga utvecklingen inom samhället (Hanson et al., 2015). Orsaken till att det sker ett informationsläckage eller en säkerhetsincident är oftast på grund av att en anställd begår ett misstag internt inom en organisation än att det sker direkta dataintrång utifrån. Informationssäkerhet är inte längre en teknologisk fråga utan en bredare fråga om människor och dess påverkan på det hela (Security Intelligence, 2014).

Bilden av en angripare har ändrats ända sedan 90-talet, årtiondet då internet kom. Då sågs och beskrevs en förövare som en yngre individ med knappa sociala förmågor som ville göra sig hörda genom att utföra attacker och intrång av olika slag. I ytterst sällsynta fall så utfördes attacker med målet att tjäna pengar. Idag är det lite mer annorlunda då allt fler kriminella nätverk har börjat verka på webben. Dagens förövare har mindre intresse av att utföra attacker med avsikt att bli lyhörda. Istället läggs allt mer fokus på att plantera virusprogram och stjäla känslig information som lösenord med olika ändamål som exempelvis att sälja information vidare. (Gollman, 2011)

Den ständiga utvecklingen har även lett till att dagens organisationer förändras strukturellt. Faktorer som outsourcing och cloud computing har en stor påverkan på hur organisationer verkar och ser ut idag. Dessa faktorer leder till att organisationer delas upp på olika områden och i vissa fall, sammanfogas. Detta leder vidare till att säkerheten av den existerande informationen inom organisationerna blir allt mer viktigt och mer svårhanterlig. Det är inte ovanligt att dagens organisationer befinner sig spritt hos exempelvis underleverantörer, vilket i sin tur gör att det uppstår allt mer påverkande faktorer kring säkerhet och policys som man bör iaktta. (Gollman, 2011)

För att kunna hantera problem som dessa så skapar företag och organisationer ISP:s som medarbetare måste följa för att minimera riskerna för incidenter och för att skapa säkerhetsmedvetande. ISP:s som inte följs utgör en mycket stor risk för en organisation menar Siponen et al., (2009). Det finns flera steg i skapandet av en ISP. Det absolut första steget är identifieringen av en risk för att sedan skapa och förmedla en policy och säkerställa att den följs. Företag kan skapa ett ISP dokument med syfte att minimera riskerna avsevärt om anställda förstår och lyder den. Däremot, om företaget misslyckas med att förmedla en ISP på ett bra sätt så har hela förarbetet gjorts i onödan och policyn kommer inte att ha någon eller väldigt lite effekt (Tuyikeze & Pottas, 2010).

1.1 Problemområde

Organisationer är idag beroende av informationsteknologi för att hantera sina dagliga affärsprocesser. Detta beroende har som resultat medfört en ökning av potentiella hot mot organisationers informationstillgångar. Flowerday och Tuyikeze (2016) menar att organisationer behöver skapa något sorts skydd för att säkerställa konfidentialitet, integritet och tillgång till den informationen som finns inom organisationen. Flowerday och Tuyikeze (2016) påpekar att en viktig åtgärd för att skydda informationstillgångar i en organisation är skapandet av en ISP.

Att skapa en effektiv ISP dokument är inte enkelt. Det existerar alltid olika åsikter inom organisationen om vad som ska vara med i dokumentet, hur den ska se ut, hur lång den ska vara samt vem som ska godkänna och ansvara för policyn. Om det uppstår svårigheter kring ett ISP dokument så vänder man sig ofta till andra företags ISP:s för att få inspiration och vägledning. Problem som däremot kan uppstå när man vänder sig till andra företags ISP dokument blir då att ens egna ISP dokumentet inte reflekterar organisationens egna kultur. Resultatet av detta blir att policyn inte kommer att bli lika effektiv jämfört med en ISP som är skapad internt från grunden (Höne & Eloff, 2002).

Det existerar även externa faktorer som möjligtvis har en inverkan vid utvecklingen av policys och som kan ha ett kraftigt inflytande på en ISP. Externa förhållanden som har ett inflytande är bland annat ekonomiska faktorer, tekniska faktorer, industristandarder, legala krav och externa hot (Knapp et al., 2009).

Då varje organisation kan ses som unik så blir det intressant att se hur pass mycket det skiljer sig när det kommer till utvecklingen av ISP i dagsläget.
Det är även intressant att se hur sedan ISP:n förmedlas vidare genom organisationen efter att den är redo för utgivning då det kan existera större skillnader mellan organisationer och hur de förmedlar ISP:n. Storlek, företagskultur och bransch är exempel på faktorer som kan påverka utvecklingen, samt avgöra hur man bör effektivt förmedla policyn.

1.2 Forskningsfråga

Vilka skillnader existerar mellan IT organisationer i Sverige när det kommer till utveckling och förmedling av informationssäkerhetspolicyn?

1.3 Syfte

Denna studie ämnar visa hur några större IT organisationer inom Sverige arbetar med ISP:n, både när det kommer till utveckling samt förmedling av policys. Eftersom att det existerar få studier på hur Svenska IT organisationer arbetar med ISP:n så vill vi ta reda på om IT organisationer i Sverige använder sig av liknande metoder samt om det finns större skillnader när det kommer till förmedling och utveckling av ISP:n.

Uppsatsen vänder sig främst till personer som arbetar inom informationssäkerhetsbranschen

och som även är ansvariga över frågor kring ISP. Vi tror att dessa personer kommer att få nytta av vår undersökning och resultatet vid utveckling och förmedling av framtida ISP:n.

1.4 Avgränsningar

Vi väljer att fokusera på hur företag arbetar med utveckling och förmedling av ISP:s, därför har vi inte valt att behandla resterande delar inom Information Security Policy Development Life Cycle. Vår uppsats är till för att ge en inblick inom några större IT organisationer som finns i Sverige samt ge en idé i hur ett sådant arbete kan gå till och därför kan vi inte garantera att vår uppsats är lika relevant för andra branscher än IT-branschen.

2 Litteraturgenomgång

2.1 Informationssäkerhet

Informationssäkerhet definieras som följande: att skydda information och informationssystem från obehörig åtkomst, användning, avslöjande, störning, modifiering eller förstörelse (Legal Information Institute, 2017). I grund och botten handlar informationssäkerhet om att skydda ens egna data och system från de som har som mål att missbruka dem menar Andress (2011).

Information ger tillgång till kunskap och fungerar som en resurs för människor och organisationer. Information kan kommuniceras, lagras och styra processer. Information behövs för att det allra flesta delar inom en organisation ska fungera. Stor del av den information som existerar inom en organisation är viktig, ibland även livsviktig. Ett exempel är Information i form av en patientjournal. Om den informationen går förlorad eller är felaktig så kan det leda till större komplikationer för en patient. Detta är ett konkret exempel på varför det är viktigt att se till att informationen alltid är tillgänglig när den behövs, att informationen är korrekt, att endast behöriga personer har tillgång till informationen och att det går att följa informationen om den ändras eller kommuniceras vidare. (Vad är informationssäkerhet, 2017)

CIA triaden är ett grundläggande, relevant och välkänt ramverk till informationssäkerhet där det beskrivs tre grundkoncept i hur man bör upprätthålla informationssäkerhet. Dessa tre grundkoncept är konfidentialitet, integritet och tillgänglighet. Konfidentialitet är förmågan att skydda data från att obehöriga får tillgång till den. Integritet hänvisar till förmågan att förhindra data från att förändras på ett obehörigt sätt. Tillgänglighet hänvisar till förmågan att ha tillgång till data när den behövs. CIA triad modellen kan användas för att avgöra om en tillgång är säker genom att tillämpa modellen mot den specifika tillgången. (Andress, 2011)

2.2 Informationssäkerhetspolicy

En ISP är i grunden ett antal dokumenterade regler för hur anställda säkert ska hantera information på ett företag eller i en organisation. Förutom att fungera som ett regelverk så hjälper även en ISP organisationer med att följa regler och lagar som är kopplade till IS-hantering (Flowerday & Tuyikeze, 2016). Det finns flera olika säkerhetsåtgärder som ett företag kan implementera, exempelvis tekniska eller avtalsmässiga åtgärder, men enligt Höne och Eloff (2002) så är ISP:s en av de absolut viktigaste säkerhetsåtgärder man kan implementera i ett företag när det kommer till informationssäkerhet.

Enligt Kostadinov (2017) så existerar det flera orsaker till varför organisationer väljer att utveckla ISP:n och varför det är en viktig säkerhetsåtgärd, några av orsakerna beskrivs som följande:

- För att upprätta en allmän riktlinje angående informationssäkerheten i organisationen.
- För att skydda organisationens rykte angående etiska och legala ansvar.

- För att upptäcka och förhindra information missbruk i organisationen.

ISP:s ska även beskriva organisationens vision och mål med informationssäkerheten samt även informera organisationens anställda om varför informationssäkerhet är viktigt (Höne & Eloff, 2002). ISP:s används i grund och botten till förutom att ändra och förbättra anställdas säkerhetsvanor, även till för att skydda information från att behandlas på fel sätt av anställda menar Karlsson et al., (2017).

2.3 Information Security Policy Development Life Cycle

En omfattande ISP livscykel som beskrivs av Tuyikeze & Pottas (2010) förser en organisation med ett ramverk för skapandet av en komplett ISP dokument. Organisationer kan med hjälp av ramverket säkerställa att nödvändiga steg för ISP utveckling fullföljs och utförs kontinuerligt. Att använda ramverket som ett tillvägagångssätt är en mycket fördelaktig sätt att skapa ISP:n. Ett ramverk som ovan nämnd kan användas för att granska om en organisations tillvägagångssätt vid ISP utveckling saknar någon viktig process (Alshaikh et al., 2016).

Information Security Policy Development Life Cycle består av fyra faser, Riskbedömning, policyutveckling, policy förmedling samt policy övervakning & underhåll. Varje fas beskriver olika aktiviteter eller steg som ska göras när man arbetar med ISP. Det som är viktigt att tänka på är att policyarbetet är en kontinuerlig process. Policyarbetet är en kontinuerlig process då teknologi, affärsmiljöer och legala villkor hela tiden förändras. Efter att en policy förmedlats så är det viktigt att övervaka och underhålla nuvarande existerande policys, eftersom att en ändring av en policy ofta kan vara aktuellt (Tuyikeze & Pottas, 2010).

Anställdas stöd är av stor betydelse för att en policy ska kunna få full effekt. Förmedling av en ISP till de anställda är ett utav de viktigaste processerna inom en policy lifecycle. Det är viktigt att man har de anställdas stöd under hela policyns livscykel. Bra kommunikation mellan de som förmedlar ISP:n och de anställda är en viktig faktor under hela policy livscykeln för att slutresultatet ska bli så bra som möjligt (Tuyikeze & Pottas, 2010).

2.3.1 Riskbedömning

Under denna fas så identifieras potentiella hot mot tillgångar som företaget vill skydda.

Målet med denna fas är att bedöma om nuvarande ISP:s fortfarande är relevanta, att granska nya versioner av standarder som finns tillgängliga och att identifiera nya potentiella risker (Rees, et al 2003).

Identifiering av hot görs genom att ställa följande frågor inom organisationen (Tuyikeze & Pottas, 2010):

- Vad är det som ska skyddas?
- Vad ska det skyddas från?
- Hur mycket är företaget villig att spendera för att ha ett effektivt skydd?

- Vad är kostnaden gentemot fördelen för företaget?

2.3.2 Policyutveckling

Utifrån resultatet från föregående fas så sker skapandet av själva policydokumentet under utvecklingsfasen. En rekommenderad lösning för varje risk presenteras i dokumentet.

Dokumentet inkluderar även aspekter såsom affärsstrategier, mål och legala villkor (Tuyikeze & Pottas, 2010). Det är viktigt att policys som introduceras täcker de kraven som finns inom organisationen. Kraven identifieras genom att utföra en riskbedömning (Alshaikh et al., 2016).

Processen vid skapandet av ISP:s innefattar valet av lämpliga mål som ska vara möjliga att uppnå. Målet kan exempelvis vara att minimera incidenter där information läcker, en policy som förklarar hur information ska hanteras på ett säkert sätt kan då vara aktuell att implementera. Idéer eller exempel för policydokumentet kan hämtas från internationella standarder som ISO 27002 där det beskrivs bästa praxis inom ISP:s (Tuyikeze & Pottas, 2010). Alshaikh et al., (2016) menar att ett policydokument ska vara kort och lättförstådd för att minimera risken att de anställda inte kommer att läsa dokumentet.

2.3.3 Policy förmedling

Tuyikeze & Pottas (2010) påpekar att policy förmedling går ut på att förverkliga de policys man har tagit fram under de föregående faserna. Tuyikeze & Pottas, (2010) anser att kommunikationen är den absolut viktigaste faktorn under denna fas för att uppnå en lyckad förmedling av en ISP. Slutgiltiga versionen av policyn ska vara tillgänglig för alla anställda. Man ska på ett formellt sätt förmedla policyn så att den blir läst och förstått av de anställda (Tuyikeze & Pottas, 2010). Genom att endast dela ut policydokumentet så kan det leda till att de anställda inte tar sig tiden att läsa och får full förståelse. Bra kommunikation med anställda leder även till bättre samtycke från de anställda (Alshaikh, Maynard, Ahmad och Chang, 2016).

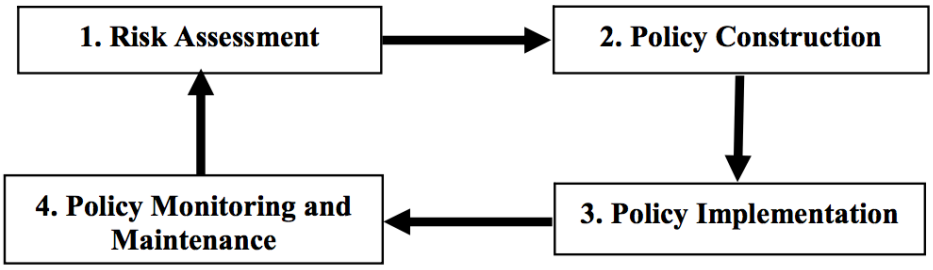
Generellt sett har man tre mål när man förmedlar policydokument till de anställda. Målen är att få medvetenhet om policydokumentet, förklara anledningen med en ISP och att se till att anställda förstår hur dessa policys kommer att påverka dem samt vilka konsekvenserna är om en ISP inte följs (Alshaikh et al., 2016).

2.3.4 Policy övervakning och underhåll

I denna fas så sker övervakningsmekanismer av de ISP:s som har förmedlat i föregående fas. Det är viktigt att ha som mål under denna fas att se till att policys som har förmedlats följs upp av de anställda. De anställdas samtycke för de nya policyerna är en viktig aspekt för att de nya policyerna ska lyckas och förbli hållbara (Tuyikeze & Pottas, 2010).

Under denna fas så är det även viktigt att undersöka om det behöver ske ändringar i den nuvarande policy dokumentet, speciellt om nya lagar, teknologiska ändringar eller risker upptäckts under processen. Målet med denna fas enligt Alshaikh et al., (2016) är att undersöka om de nuvarande policys fortfarande är relevanta och att identifiera möjliga ändringar. En policy kommer förr eller senare att föråldras vilket betyder att en uppdatering

kommer att vara nödvändigt. En policy som inte utvärderas eller uppdateras kontinuerligt är av inget värde menar Rees et al., (2003). När en uppdatering av ISP är nödvändig så upprepas livscykeln och dess olika faser (se Figur 1) (Tuyikeze & Pottas, 2010).



Figur 1: De fyra faserna inom Information Security Policy Development Life Cycle, (Tuyikeze & Pottas, 2010)

2.4 Policyutveckling

Något som är viktigt att förstå är att utvecklingen av ISP:s inte är en process som bara görs en gång, utan att det är istället en process som bör ske kontinuerligt för att garantera att en ISP förblir aktuell (Tuyikeze & Pottas, 2010). Ett ISP ramverk kan användas för att se till att ISP:n i företaget förblir aktuella menar Tuyikeze & Pottas (2010).

Alshaikh et al., (2016) förklarar att det första steget i utveckling av en ISP inom en organisation är att man tar fram ett team som ansvarar för policyutveckling. Teamets två huvudsakliga uppgifter ska vara att identifiera intressenter samt definiera roller och ansvarsområden inom utvecklingsteamet (Alshaikh et al., 2016; Diver, 2007). Teamet som väljs bör även ansvara för att förmedla och driva igenom ISP dokumentet menar Diver (2007).

Identifiering av intressenter är en avgörande framgångsfaktor för utveckling av en ISP förklarar Alshaikh et al. (2016). De intressenter som identifieras bör vara alla som kommer att påverkas av policyn (Alshaikh et al. 2016; Sorcha Diver, 2007). Detta arbete ska ske genom hela organisationen och dess relevanta delar (Alshaikh et al., 2016). När det sedan kommer till definiering av roller och ansvarsområden så menar Alshaikh et al. (2016) att detta steg är viktigt för att minimera risken att det ska uppstå eventuella förseningar inom utvecklingsarbetet.

Diver (2007) påpekar att ISP dokumentet kommer att utvecklas utefter intressenterna för att se till att de förstår anledningen till varför specifika ISP:n existerar.

Anledningen till att varför en ISP faktiskt existerar kan vara mer uppenbart för exempelvis en chef eller en IT anställd inom organisationen än intressenter som inte arbetar med IT. Sådana skillnader i bakgrundsförståelse kan ses som en stor anledning till att förklara bakgrunden till varför ISP:n existerar. (Diver, 2007)

Efter att ett team har tagits fram så nämner Alshaikh et al att nästa steg bör vara att avgöra vilka säkerhetsbehov som ska existera. Det är väsentligt att identifiera säkerhetsbehov för att kunna upprätthålla säkerhet inom en organisation (ISO/IEC 27002, 2013).

Detta ska göras genom två huvudsakliga uppgifter, identifiering av säkerhetskrav samt bedömning av organisationens nuvarande policy och rutiner (Alshaikh et al., 2016).

Säkerhetskraven bör spegla de krav som krävs genom att utföra riskbedömningar för att hantera säkerhetsrisker. Här bör det även definieras vilken nivå av säkerhet som man vill uppnå inom organisationen. (Alshaikh et al., 2016)

Att göra en bedömning av nuvarande policyn och rutiner har flera fördelar. En bedömning av nuvarande policyn och rutiner stödjer teamets förståelse för policyn och processer, säkerhetsställer att nya policyn anpassas till nuvarande policy standards samt hjälper till med att samla in nyckelobjekt såsom redan existerande policyn. (Alshaikh et al., 2016)

Den slutgiltiga uppgiften i utvecklingen av en ISP är att sammanställa samt att recensera policyn som man har konstruerat. Detta bör göras innan man förmedlar säkerhetspolicyn till organisationen. (Alshaikh et al., 2016)

En recension av policyn bör även ske vid planerade intervaller eller när det skett viktiga ändringar för att säkerhetsställa att policyn fortsätter vara effektiv (ISO/IEC 27002, 2013).

2.4.1 Ramverk och regelverk vid policyutveckling

En säkerhetspolicy kan grundas på ett flertal ramverk och även regelverk beroende på en organisations struktur samt geografiska läge (Höne & Hoff 2002). En anledning till varför organisationer väljer att utveckla ISP:n är för att kunna möta legala krav och föreskrifter. Det är absolut nödvändigt att kunna visa att dessa följs inom organisationen (Sorcha Diver, 2007).

Personuppgiftslag
Personuppgiftslagen är en svensk lag som har till syfte att skydda personuppgifter som lagras hos exempelvis myndigheter eller företag. Denna lag är viktigt att ha till kännedom när det kommer till policyformulering då informationssäkerhet handlar om just säkerheten kring känsliga uppgifter. Då lagring av personuppgifter kan endast ske efter samtycke med den vars uppgifter man lagrar så måste även sådant framföras. Lagen ser till att den personliga integriteten förblir skyddad, även vid inblandning av ett tredje land men där då utrustningen som sköter personuppgifter finns i Sverige. (Personuppgiftslag, 1998:204)

ISO 27002
ISO2700 är en internationell standard som används av många företag världen över. Ramverket förklarar olika delar som man kan beakta när det kommer till exempelvis policy formuleringar samt informationssäkerhet inom ens organisation.

Ramverkets huvudsakliga uppgift är att fungera som ett stöd för organisationer vid en implementering av större informationssystem. Eftersom att ramverket är brett och täcker ganska många delar inom informationssäkerhet så kan man också endast ta ut de delar som man anser passar ens verksamhet eller det man huvudsakligen sysslar med. Ramverket/modellen anger krav för etablering, genomförande, övervakning, underhåll och förbättring inom informationssäkerhet. (ISO/IEC 27002, 2013)

Offentlighets- och sekretesslag
Lagen innehåller bestämmelser som gäller vid alla myndigheter och organisationer inom Sverige. Lagen täcker områden såsom tystnadsplikt samt förbud mot att lämna ut allmänna

uppgifter. Denna lag påverkar privata organisationer om de exempelvis samarbetar med myndigheter och därför är det viktigt att iaktta en sådan lag när man utformar en ISP. (Offentlighets- och sekretesslag, 2009:400)

2.5 Policy förmedling

Anställda som inte följer ISP:s utgör en allvarlig risk mot organisationen anser Siponen et al., (2009). De incidenter som uppstår kan orsaka stora skador för organisationer. Exempelvis kan organisationer mista potentiella inkomster, få känslig information läckt, få dålig publicitet eller leda till att organisationer bryter mot legala villkor och ställs inför rätta (Siponen et al., 2009).

Bland annat har det visat sig att bristande samtycke för ISP:n från anställda är ett stort problem. Dessa problem uppstår när exempelvis de anställdas arbetsprocesser kommer i konflikt med säkerhetspolicyn och dess regelverk. Detta leder till att de anställda måste prioritera mellan att följa policyn eller fortsätta med ens egna arbetsprocesser. (Karlsson et al., 2017)

Siponen et al., (2009) rekommenderar för att få anställdas samtycke för ISP:n att pressa anställda på ett positivt och verbalt sätt, d.v.s. på ett visuellt sätt presentera ISP:n under ett möte med anställda. Anställda ska förväntas följa ISP:n från organisationen och på så sätt pressas till att få deras samtycke. Det är även viktigt att anställda får se vad som kan bli konsekvensen om en policy inte följs, detta kan göras genom att presentera och diskutera informationssäkerhetsincidenter som exempelvis rapporterats i media Siponen et al., (2009).

Om anställda inte förstår anledningen till varför ISP:n behöver existera, så är chansen liten att få de anställdas samtycke menar Siponen et al., (2009). Därför är det viktigt att personalen i organisationen som har som uppgift att förmedla ISP:n inser hur viktigt det är att få anställda att inse vilka konsekvenserna blir om ISP:n inte följs beskriver Siponen et al., (2009).

Knapp et al., (2009) anser att organisationer ska utbilda sina anställda angående informationssäkerhetsfrågor med anledning att få anställdas stöd för ISP:n så att de följs vid deras vardagliga arbete. Knapp et al., (2009) påpekar också att träningsarbetet ska ske kontinuerligt i och med att ändringar i ISP dokumentet kan förekomma. Knapp et al.,(2009) beskriver också att informationssäkerhets träningen måste förekomma direkt efter att en policy har utvecklats, då det underlättar att förklara motiveringen bakom ISP:n.

Alshaikh et al., (2016) påpekar även att policyförmedling är en kontinuerlig process. Efter att ISP:n har utvecklats så ska den distribueras till alla intressenter i organisationen. Organisationen ska välja på vilket sätt ISP dokumentet ska distribueras, exempelvis om dokumentet ska skickas via e-mail, laddas upp på interna nätverk eller om dokumentet ska distribueras som papperskopia. Alshaikh et al., (2016) menar att distribuering av en ISP inte är tillräckligt, då det inte går att garantera att anställda faktiskt har läst och förstått ISP dokumentet. Därför rekommenderar Alshaikh et al., (2016) att organisationer bör på något sätt kommunicerar ISP dokumentet genom exempelvis utbildning inom säkerhet eller medvetenhet. Alshaikh et al., (2016) anser att organisationer även ska hålla en genomgång av ISP:n minst en gång i månaden.

Flowerday och Tuyikeze (2016) påpekar att det kan bli svårt att få anställdas samtycke för det nya ISP dokumentet, men med träning och utbildning så blir den processen mycket enklare. Målet med träning och utbildning är förutom att få anställdas samtycke, även för att se till att alla anställda förstår och har ett ansvar mot ISP:n (Flowerday och Tuyikeze, 2016). Flowerday och Tuyikeze, (2016) anser att säkerhetsutbildning, säkerhetsträning och medvetenhetsträning är de viktigaste metoderna för att hantera informations missbruk.

Identifierade metoder för policy förmedling:

Författare	Metod	Beskrivning
Siponen, Mahmood och Pahnila (2009).	Positiv verbal social press gentemot anställda under ett möte för att få samtycke.	Författarna menar att organisationen ska pressa anställda genom att presentera konsekvenserna på vad som kan hända om en policy inte följs och på så sätt vinna deras samtycke. Anställda behöver förstå anledningen till varför en ISP existerar.
Knapp, Morris, Marshall & Byrd (2009).	Kontinuerlig utbildning av anställda angående informationssäkerhetsfrågor.	Författarna anser att organisationer ska utföra kontinuerliga utbildningar med anställda för att få deras stöd angående ISP:n. Kontinuerliga utbildningar ska göras på grund av att det ständigt sker ändringar i ISP:n.
Alshaikh, Maynard, Ahmad och Chang (2016).	ISP dokument distribution och säkerhets och medvetenhetsträning.	Författarna anser att ISP:n först ska distribueras i organisationen till alla anställda men att det inte är tillräckligt. Författarna tycker att organisationen även ska hålla i säkerhets och medvetenhetsträning för anställda. Detta arbete ska ske kontinuerligt påpekar författarna.
Flowerday och Tuyikeze (2016).	Säkerhetsutbildning, säkerhetsträning och medvetenhetsträning..	Författarna anser att Säkerhetsutbildning, säkerhetsträning och medvetenhetsträning är de tre viktigaste metoderna för att hantera informations missbruk.

Tabell 2.1 Teoretisk tabell för policy förmedling

3. Metod

Vi har valt att utföra en kvalitativ studie med intervjuer som ska stå till grund för vår empiri. Vår undersökning utgår från faserna utveckling och förmedling som är två av faserna i Information Security Policy Development Life Cycle. Primärdata kommer från intervjuerna som vi har fört med respondenter från It-företag som opererar inom Sverige. De personer vi har intervjuat innehar kunskap och erfarenhet inom ämnet informationssäkerhet och ISP:s. Vi har valt att intervjua tre olika personer på tre olika It-företag. Det är viktigt att respondenterna kan bidra med god insyn kring ämnet för att vi ska kunna få kvalitativa resultat på den empiriska delen. Vi samlar in sekundärdata i form av relevanta artiklar och litteratur som berör ämnet och problemområdet informationssäkerhet och ISP:s (Jacobsen, 2002).

3.1 Intervjuteknik

Vi har valt att genomföra fysiska intervjuer parallellt med teoretiska undersökningar då vi finner ett större djup i ett sådant arbete. Vi anser att vi helt enkelt får en verklig uppfattning av området samt även en verklig bild gentemot oss själva för vårt senare arbete. Fysiska intervjuer ger helt enkelt mer djupgående svar då vi i grunden för en diskussion kring ämnet och inte förväntar oss svar på mail eller liknande då det oftast slutar med korta svar utifrån författarnas egna erfarenhet.

Våra intervjuer har varit semistrukturerade där vi har kunnat använda oss utav våra frågor utifrån litteratur som endast en bas till vad som sedan faktiskt diskuteras under intervjun. Vi har varit väl medvetna om att vi kan få olika svar angående säkerhetsaspekter då de som vi intervjuade besitter olika roller och erfarenheter.

Vår struktur på intervjuerna tillåter helt enkelt de som blir intervjuade att tala fritt och ge deras verkliga uppfattning kring ämnet utan att känna sig bundna till att svara på specifika frågor. Detta var något som vi också märkte av när vi väl utförde intervjuerna, vilket visar på att konceptet kan ses som vinnande.

De gånger vi har fört intervjuer med hjälp av ljudinspelning har setts som en fördel då vi har kunnat fokusera på själva intervjun och personen i fråga istället för att ställa allt för stor fokus på att föra anteckningar. Detta gör även att vi enkelt kan citera vad en person sagt då vi transkriberar allt som sägs ord för ord. Den gången vi inte har fått möjlighet att spela in har gjort det svårt för citering men ändå blivit tidsbesparande i form utav att vi inte behöver transkribera i efterhand. Oavsett om vi har spelat in eller antecknat så har vi försökt att koppla ihop allt material med relevanta teorier i litteraturen som vi använt oss av i vår rapport.

3.2 Urval av respondenter

Valet av de intervjuade respondenter till vår uppsats har skett genom mailförfrågan. Vi har sökt efter relevanta respondenter som skulle passa in i vårt forskningsområde, exempelvis säkerhetsexperter eller säkerhetschefer. De respondenter som vi har haft kontakt med har svarat direkt till oss via mail. Det har även förekommit telefonkontakt med respondenterna när vi blivit hänvisade genom telefonnummer.

Våra förfrågningar har skett genom att vi har skickat mail till ett flertal intressanta privata företag inom IT-branschen som har en stark koppling till informationssäkerhet. När vi skickade förfrågningar så valde vi att vara öppna och ärliga kring ämnet våra intervjuer skulle behandla. Vi förklarade att vi inte är ute efter några detaljer eller företagshemligheter utan bara vill ha svar på våra forskningsfrågor utifrån respondenternas expertis och erfarenheter.

Företagen som vi kontaktat har varit geografisk belagda inom Skåne då vi skulle ha möjligheten för att utföra fysiska intervjuer. Företagen är alla även organisationer med en blandning av nationella och internationella arbetsområden.

3.2.1 Företag 1

Företag 1 är en ledande svensk leverantör av cybersäkerhet. Företag 1 utvecklar, tillverkar och säljer avancerade cybersäkerhetslösningar som förhindrar intrång, stöld och dataläckage vid informationsutbyten. Vi valde att inkludera Företag 1 i vår studie med anledning att Företag 1 arbetar med informationssäkerhets lösningar och hanterar känslig information. Detta gör Företag 1 ett mycket intressant företag att intervjua då vi vill ta reda på hur ett företag som detta utvecklar och förmedlar ISP:s.

3.2.2 Företag 2

Företag 2 är ett It-företag som säljer IT-tjänster. Företag 2 skapar IT-lösningar åt bland annat banker, detaljhandelsföretag, kommuner, landsting, media, statliga bolag och myndigheter samt tillverkningsföretag. Valet att inkludera Företag 2 i studien grundar sig på att de arbetar med IT-lösningar och ligger i framkanten inom det området. Detta gör att företag 2 är ytterst intressant för vår forskning.

3.2.3 Företag 3

Företag 3 är ett konsultföretag som erbjuder IT-lösningar med expertis inom flera områden där informationssäkerhet är ett av dessa. Företag 3 är ett internationellt företag som opererar i många länder. Företag 3 är ett intressant företag att ha med i vår undersökning på grund av att det är ett internationellt företag vilket gör det intressant att ta reda på hur ett It-företag som detta utvecklar och förmedlar ISP:s.

3.3 Intervjufrågor

Målet med intervjufrågorna var att få en så omfattande och komplett inblick på hur företagen utvecklar och förmedlar ISP:s. Intervjufrågorna konstruerades på så sätt att vi kunde först få en överblick över företaget och dess informationssäkerhet för att sedan få en mer djupare inblick.

3.3.1 Intervjuguide

Vi har skapat ett utkast av en intervjuguide innan vår första intervju för att kunna behålla en viss struktur under intervjun, då Jacobsen (2002) påpekar att det är viktigt att skapa en viss struktur. Intervjuguiden lägger grunden för den teori vi har samlat in och vad vi vill svar på när det kommer till forskningsfrågan. När vi utförde våra intervjuer så utgick vi ifrån att det ska vara ganska öppet även om vi har ganska bestämda intervjufrågor.

Vi börjar alltid med att diskutera lite allmänt med den respondent som ska intervjuas då för att slippa den stela intervjukänslan som man brukar oftast känna. Vi diskuterar fritt kring våra frågor och låter den intervjuade att tala fritt utifrån vårt samtalsämne, även om vi ser att det kanske inte är helt relevant till vad vi är ute efter. Våra intervjuer sker på respondentens arbetsplats för att dels göra det bekvämt för personen och för att få en enklare uppfattning utav andre parten.

3.3.2 Intervjuanalys

För att analysera intervjuerna så har vi använt oss av analysprocessen som Jacobsen (2002) rekommenderar vid denna typ av analys. Efter att en intervju är gjord så transkriberade vi innehållet (om intervjun blev inspelad) och sedan så arbetar vi med den material vi fått och kan se i transkriberingen för att koppla ihop resultatet med relevant litteratur. Vi valde att kategorisera intervjutranskriberingarna efter intervjufrågorna inom tabeller för att lättare kunna referera till intervjuerna. Detta även för att läsaren ska slippa att gå igenom allt som sagts och endast få tillgång till det allra viktigaste.

3.4 Etiska aspekter

Jacobsen (2002) beskriver i sin bok om tre grundkrav som måste uppfyllas av undersökarna, samtycke, krav på privatliv och krav på att bli korrekt återgiven. Vi anser också att det är viktigt med dessa tre regler och vi har strävat för att uppfylla dessa etiska krav.

3.4.1 Samtycke

Inför varje intervju så har vi berättat för respondenterna inom vilket område intervjun kommer att behandla. Respondenterna har frivilligt accepterat att bli intervjuade. Vi anser att respondenterna är medvetna om vilka risker och vinster som existerar genom att delta i en intervju som Jacobsen (2002) beskriver. Vi har erbjudit att skicka en kopia av uppsatsen till respondenterna innan inlämning av uppsatsen. Detta för att de kan påpeka eventuella missuppfattningar och andra eventuella invändningar som de vill att vi ska ändra på.

3.4.2 Krav på privatliv

Vi har valt att inte använda respondenternas namn eller företag de arbetar på för att vi anser detta är känsliga uppgifter och det ska vara anonymt i vår uppsats. Vi har istället valt att beskriva respondenterna efter deras roll i företaget. Företagen har vi valt att beskriva som Företag 1, Företag 2 och Företag 3.

3.4.3 Krav på korrekt återgivning

För att bevisa att vi har korrekt återgivit vad som sades under intervjun så har vi bifogad transkriberingen från intervjuerna som bilagor så att läsaren kan se att primärdatan är giltig. Vi anser att respondenterna vill bli korrekt återgivna och respekterar om det uppstår krav på förändring från respondenterna utifrån det vi har skrivit.

3.5 Undersöknings värde

3.5.1 Validitet

Under våra intervjuer har vi utifrån Jacobsen (2002) valt att agera i en reserverad roll. Dels för att skapa en öppen atmosfär där respondenterna ska kunna tala och berätta fritt kring deras erfarenheter och expertis, men även för att kunna uppnå och stärka möjligheter för att uppnå en hög validitet, det vill säga, det som sägs ska kunna bedömas som kvalitativt och pålitligt. Förutom att hålla en reserverad roll när det kommer till intervjuerna så har vi även valt att ställa frågan om hur respondenterna definierar informationssäkerhet. Anledningen till detta är för att dels är informationssäkerhet vårt huvudämne och på så sätt kan vi få intressanta svar kring ämnet i helhet, men även för att ge läsarna en inblick i hur insatta respondenterna verkligen är inom informationssäkerhet.

3.5.2 Reliabilitet

Varje intervju har genomförts på respondenternas arbetsplats genom anpassade tider utifrån respondenternas önskemål. Detta för att göra det så bekvämt som möjligt för respondenterna. Genom att göra på detta vis så minimerar man den så kallade kontexteffekten som Jacbossen (2002) nämner kan påverka den information som man samlar in. Genom att använda oss utav inspelning av intervjuerna så har vi på så sätt garanterat att samtliga författare kan analyser och tolka informationen i efterhand. Även de transkriberingar som vi skapat utefter intervjuerna har säkerhetsställts med respondenterna för att på så sätt utesluta några tänkbara missuppfattningar. Om det har skett missuppfattningar så har samtliga respondenter fått återkoppla och på sätt få missuppfattningarna korrigerade.

4 Resultat

Organisation	Respondent
Företag 1, Cybersäkerhet	IT-Chef
Företag 2, Konsulttjänster	Säkerhetsansvarig
Företag 3, IT-Lösningar	Säkerhetsexpert

Tabell 4.1 Referenslista med respondenter

4.1 Hur uppfattar företagen Informationssäkerhet?

Definitionen av informationssäkerhet är ganska bred och det är många delar som täcks upp när det kommer till att förklara hur informationssäkerhet fungerar inom dagens organisationer. Vi har under våra undersökningar försökt få fram enligt definition hur de olika organisationerna ser på informationssäkerhet samt hur det definieras i dagsläget. Ganska tidigt inom vår undersökning märks det att informationssäkerhet har en existerande grund definition. IT-chefen på företag 1 definierar informationssäkerhet som ett sätt att hantera och skydda information (Appendix 2, Rad 8). Säkerhetsansvarige på företag 2 definierar informationssäkerhet som en livsviktig faktor inom ett företag. Säkerhetsansvarige menar att om man frågar personer som inte är experter inom säkerhet så ser de oftast säkerhet som en hygienfaktor, alltså något som är bra att ha. Detta håller säkerhetsansvarige inte med om. Säkerhetsansvarige menar att i och med den ständiga utvecklingen inom IT och dess påverkan på samhället så är säkerhet mer viktigare än någonsin. Slutligen definierar Säkerhetsexperten på företag 3 informationssäkerhet som det skyddet man har inom ett digitalt ekosystem där människan pratar med teknik (Appendix 2, Rad 6).

Som vi ser så har alla dessa företag en gemenskap när de definierar informationssäkerhet. Att skydda känslig information. Även om alla respondenter inte väljer att gå in i djupet på frågan om definition så är det ändå väldigt klart till hur de ser på helheten.

4.2 Policyutveckling

4.2.1 Företag 1

Hos företag 1 så är det säkerhetschefen som ansvarar för att upprätthålla, utveckla och driva igenom ISP:s (Appendix 2 Rad 11). Vår respondent, IT-chefen har ansvar för all informationsteknologi som finns på företaget (Appendix 2 Rad 2). Företag 1 har då en säkerhetschef som har en högre post i organisationen än IT-chefen. De arbetar tillsammans med ISP dokumentet då den även innehåller IT-relaterade policys.

IT chefen förklarar att deras policyformulering är strikt då de hanterar känslig information. Oftast är det information gällande statshemligheter vilket gör att det ställs höga krav hos företaget då det existerar flertal lagar kring informationshantering som måste beaktas. Specifikt nämner IT chefen lagen om offentlighet och sekretess som en av de viktigaste lagarna. IT chefen berättar att deras policy är väl utvecklade och definierade utefter de krav som ställs och anser även därför att de är långt framme i deras arbete med att konstruera policys (Appendix 2, Rad 13 och Rad 15).

IT-chefen anser att privata organisationer kan använda sig av lagen om offentlighet och sekretess vid utveckling av sina ISP:n även om lagen inte kan appliceras till privata organisationer (Appendix 2, Rad 21).

"Lagen om offentlighet och sekretess det är en bra grund bas och ur den så kan man bygga policys" (Appendix 1, Rad 51).

IT-chefen påpekar även att de använder sig utav ISO standarden, version 2001, men att de kommer att gå över till 2015 versionen. Men IT-chefen förklarar att ISO inte är något lagkrav och om ISO standarden står emot de regulativa kraven så vinner alltid de regulativa kraven. (Appendix 2, Rad 17-19). IT-chefen förklarar att ISO standarden innehåller mycket som Företag 1 kan dra nytta av men att de kan även välja att avstå från den om innehållet om den går på kors med lagen om offentlighet och sekretess.

*"i och med att vi följer lagen om offentlighet och sekretess så får vi ju mycket på köpet när det gäller ISO standard" (*Appendix *2, Rad 19)*

"För det går att använda det regelverk som finns i lagen om offentlighets och sekretess även om det är en privat verksamhet även om det egentligen inte styrs av denna lag. Så kan man använda den på ett bra sätt och därigenom få en bra policy" (Appendix 2, Rad 21).

"Vi är dessutom ålagda att en uppdatering varje år" (Bilaga 1, Rad 23). IT-chefen berättar att de genomför årlig genomgång av företagets ISP:s för att undersöka om det har skett några ändringar i lagkraven eller om ett projekt kräver något extra. (Appendix 2, Rad 23).

4.2.2 Företag 2

Säkerhetsansvarige på företag 2 påpekar att det finns en missuppfattning mellan informationssäkerhet och IT-säkerhet. Säkerheten på ett företag bör inte kontrolleras av IT, den ska istället övervaka IT menar Säkerhetsansvarige på företag 2. Varje företag bör ha en säkerhetsansvarig som befinner sig över IT-chefen för att säkerställa att hela företagets behov tas med i policyn och inte bara IT frågor. IT-chef och säkerhetschef bör inte vara en enskild roll utan istället två enskilda roller menar säkerhetsansvarige som har arbetat mot att se till att de två rollerna blir separata inom företag 2. (Appendix 3, Rad 10)

Man bör börja med att identifiera externa och interna krav och se dem som kärnan i ens policy menar den säkerhetsansvarige. Han förklarar att de yttre kraven kommer från lagar, myndigheter och kunder, samt att de inre kraven kommer från ledningen. Han förklarar även att en policyutveckling kan ske utifrån ramverk och standarder, exempelvis ISO 27000. En policy ska vara strukturerad och förklara exakt för den som läser vad man får och inte får göra. Här blir det viktigt att språket är korrekt så att de anställda förstår sig på vad som står i policyn (Appendix 3, Rad 12).

Säkerhetsansvarige anser även att vid utveckling av en policy så bör man tänka mer människocentriskt än kontrollcentriskt. Det sker ständigt fler förbättringar på den tekniska aspekten men inte hos självaste människor. Man bör helt enkelt ha ett helhetsperspektiv menar säkerhetsexperten (Appendix 3, rad 28).

Vi uppfattar att i och med att Företag 2 utför nya tester vid förmedling av policys vid en ändring av ISP:n så går det att fastställa att Företag 2 kontinuerligt utvecklar sin ISP (Appendix 3 Rad 21).

4.2.3 Företag 3

Säkerhetsexperten förklarar att det är ledningen som ansvarar för ISP dokumentet hos Företag 3, säkerhetsexperten påpekar också att han själv tillhör ledningen. (Appendix 4, Rad 9–11).

Säkerhetsexperten berättar att deras nuvarande ISP:s är väldigt juridiskt inriktade och att den är väldigt enkel att förstå även för anställda som inte arbetar med säkerhet (Appendix 4, Rad 14).

Säkerhetsexperten förklarar att man bör utveckla policys som är konkret kopplade till informationssäkerhet. Vid framtagning av en sådan policy så förklarar säkerhetsexperten att man måste ta hänsyn till faktorer inom trendbevakning som hot och digitaliseringstrender. Detta sker oftast i en analytisk workshop, förklarar säkerhetsexperten. I princip tar man fram en grund för en risk och sårbarhetsanalys där resultatet påverkar framtagandet av en policy. Säkerhetsexperten förklarar även att man kan använda sig utav ramverk, även säkerhetsexperten nämner ISO 27000 som ett naturligt val när det kommer till policyutveckling (Appendix 4, Rad 16, Rad 18 och Rad 22).

Vi tolkar även här att i och med att Företag 3 utför nya tester vid förmedling av policys vid en ändring av ISP:n så går det att fastställa att Företag 3 kontinuerligt utvecklar sin ISP (Appendix 4 Rad 24).

4.3 Policy förmedling

4.3.1 Företag 1

När en ISP ska förmedlas till de anställda så håller företag 1 i utbildningar beroende på vilken säkerhetsnivå den anställde har. Företaget utför även utbildningar med alla anställda oberoende på vilken säkerhetsnivå de tillhör. Vidare berättar IT-chefen att nyanställda får en introduktion med de ISP:s som kommer att gälla specifikt den individuella personen. Företag 1 utför även kontinuerliga utbildningar varje år där de utbildar personalen i hur man arbetar med säkerhetsfrågor. När sedan en ny version av policydokumentet utvecklas och ska förmedlas så går man igenom den med alla i företaget en gång till berättar IT-chefen (Appendix 2, Rad 24–31).

4.3.2 Företag 2

Respondenten som ansvarar för säkerhetsområdet på företag 2 menar att vid förmedling av ISP:s så måste man förstå vad anställda hos företaget anser om policyn och hur den påverkar dem. Att arbeta med olika utkast eller versioner av policydokumentet där man kommunicerar och diskuterar med alla i företaget, från vanliga anställda till chefer innan publicering är viktigt menar säkerhetsansvarige på företag 2. Säkerhetsansvarige för företag 2 anser att policy förmedlingen ska påbörjas högst upp inom organisationen och sedan arbeta sig nedåt för att få stöd från resterande organisationen (Appendix 3, Rad 8). Vid förmedling av ISP:s så berättar säkerhetsansvarige på företag 2 att de utför ett skriftligt test för de anställda för att säkerställa att de läst och förstått ISP:n efter att de har distribuerat ISP dokumentet ut i organisationen. En signatur av de anställda krävs också efter att testet blivit godkänd för att se till att den anställde tar på sig ansvaret ifall en incident skulle ske där en anställd är ansvarig. (Appendix 3, Rad 15–17). Säkerhetsansvarige berättar även att de utför nya tester varje gång det uppstår stora ändringar i ISP dokumentet (Appendix 3, Rad 21).

4.3.3 Företag 3

Säkerhetsexperten som arbetar på företag 3 tillhör ledningen på företaget. Ledningen i företag 3 är de som formar policydokumentet för informationssäkerheten i företaget.
På företag 3 så sker arbetet med ISP från högsta nivån för att på så sätt få ledningens samtycke från början (Appendix 4, Rad 9–12).

Förmedling av ISP sker dels vid anställningsprocessen samt även fortlöpande när det kommer nya versioner av ISP dokumentet berättar säkerhetsexperten. ISP:n distribueras genom ett digitalt forum så att alla har tillgång till dokumentet. Företag 3 förmedlar ibland policys genom att få anställda att utföra ett test, men Säkerhetsexperten menar att den metoden ska förändras (Appendix 4 Rad 23–26).

Säkerhetsexperten föredrar en metod som går ut på att man skickar ut mindre testfrågor via mail som grundar sig på policydokumentet. En anställd kan svara i lugn och ro på frågorna som kommer med testet. Säkerhetsexperten menar att denna metod fungerar mer som en informativ pedagogisk ledd utbildning, vilket varar under ett fåtal minuter. Företag 3 utför denna metoden med anledning om att påminna de anställda om ISP:n som gäller i organisationen samt för att öka medvetandet (Appendix 4, Rad 23–28).

Respondent	Metod
Företag 1	Utbildning kopplade till ISP:s utförs utefter vilken säkerhetsnivå som en anställd befinner sig på. Utbildningar sker gemensamt oberoende av vilken säkerhetsnivå som de anställda tillhör. Även kontinuerliga utbildningar sker gemensamt årsvis och vid förändring av ISP dokumentet
Företag 2	Skriftligt test för att få anställda att förstå och läsa ISP dokumentet efter att det har distribuerats ut i organisationen. Ett test utförs även när större ändringar sker i ISP dokumentet.
Företag 3	Distribution av ISP dokumentet och kontinuerlig utbildning i form av test via mail. ISP dokumentet går företaget även igenom med anställda under anställningsprocessen.

Tabell 4.2 Identifierade metoder för förmedling av ISP

5 Diskussion

5.1 Policyutveckling

Här kommer vi att jämföra hur de olika företagen bedriver sin policy konstruktion gentemot hur den beskrivs i litteraturen

När man ska utveckla fram en konkret policy som ska till syfte ha att vägleda hur man bör hantera information på ett säkert sätt så finns det ett flertal faktorer som kommer att påverka arbetet. Oavsett om man har en policy sen tidigare eller ska precis påbörja ett utvecklingsarbete så måste man tänka på att utveckling av en säkerhetspolicy som Tuyikeze & Pottas (2010) nämner är en kontinuerlig process.

De resultat som har framkommit utifrån våra empiriska resultat framhäver olika aspekter kring utveckling av en ISP hos de tre företag som har undersökts.

Företag 1 förklarar att de arbetar med en strikt policyutveckling då deras arbetsområde påverkas av svensk lag p.g.a. att de bland annat hanterar statshemligheter. Detta visar direkt på att deras utvecklingsarbete påverkas av externa faktorer såsom lagar.

Precis som Diver (2007) förklarar så är det viktigt att företag kan visa att de har förståelse samt uppnår de legala krav som ställs. Detta menar då företag 1 att de konkret kan visa genom att utveckla och formulera en strikt policy. Företag 1 berättar även att deras policyutveckling bygger på ramverk som ISO 27000. På företag 1 så är det dessutom säkerhetschefen som ansvarar för utvecklingen av ISP. Däremot så förklarar företag 1 att själva utvecklingsarbetet av ISP sker i samarbete mellan IT- och säkerhetschefen.

Säkerhetsansvarige på Företag 2 berättar att en utveckling påverkas av externa och interna krav som bör analyseras innan själva utvecklingsarbetet av en ISP. De kraven kan vara lagar och regelverk, ramverk samt interna krav från organisationen menar den säkerhetsansvarige. Här nämns specifikt ISO 27000. När det kommer till själva utvecklingsarbetet av ISP:n så menar även säkerhetsansvarige att bör den styras av en säkerhetschef som tillsammans med en IT-chef arbetar med utvecklingen. Ett team med högt samarbete är väsentligt som första steg i en utveckling av en ISP menar både säkerhetsansvarige på företag 2 och Alshaikh et al., (2016). I allmänhet menar även säkerhetsansvarige att det sker för stort fokus på IT än själva människan vid utveckling av ISP och därför fokuserar företag 2 mestadels på att arbeta med mänskliga aspekter. Precis som Höne & Eloff (2002) berättar så riktar sig en ISP just mot att informera de anställda om säkerhetskrav inom en organisation.

På företag 3 så förklarar säkerhetsexperten att ansvaret av ISP ligger hos ledningen där han själv tillhör. Företag 3s ISP är väldigt juridiskt inriktad, vilket även visar på att deras utvecklingsarbete påverkas av externa krav precis som resterande respondenter tidigare har visat. Här nämner säkerhetsexperten att trendbevakning är viktigt vid utvecklingsprocessen.

Det krävs att man gör en risk och sårbarhetsanalys som ska stå till grund vid utveckling av ISP menar säkerhetsexperten. Detta förklaras även av Alshaikh et al., (2016) som ett konkret steg vid utvecklingsprocessen. Även på företag 3 nämns ISO 27000 som ett konkret ramverk vid utveckling av ISP.

Det första vi kan fastställa efter vi har analyserat resultatet är att alla tre respondenter som vi har intervjuat utför utvecklingsarbetet kontinuerligt. Precis som Tuyikeze & Pottas (2010) påpekar så är det en process som ska göra kontinuerligt för att säkerställa att ISP:n förblir aktuell. Då samtliga respondenter är renodlade It-företag så antar vi - som det sedan även visade sig - att företagen bedriver kontinuerligt utveckling av ISP:s för att dessa inte ska bli inaktuella.

Alshaikh et al., (2016) påpekar att en organisation ska bestämma vem eller vilka i organisationen det är som ska ansvara för att ta fram ISP dokumentet. Den eller de som får ansvar för att utveckla ISP dokumentet ska även driva igenom och förmedla ISP dokumentet menar Diver (2007). På de företagen som vi har intervjuat har vi identifierat skillnader i vem det är som ansvar för ISP dokumentet. På Företag 1 så är det säkerhetschefen som ansvarar för att upprätthålla, utveckla och driva igenom ISP:s. Även på Företag 2 så är det säkerhetschefen som ansvarar för ISP:s. På Företag 3 så ansvarar ledningen för ISP:s.

Vi kan konstatera att det inte ser ut likadant på de företag som vi har intervjuat när det kommer till vem det är som ansvarar för ISP:s, då Företag 3 skiljer sig gentemot Företag 1 och 2.

Utifrån resultatet kan vi se att det finns ett flertal externa faktorer som kan påverka organisationers utvecklingsprocess av en ISP. Det vi konkret ser från samtliga respondenter när det kommer till användning av ramverk är att de rekommenderar ramverket ISO 27000 som ett hjälpmedel när det kommer till ISP utveckling. Ramverk kan vara till stor hjälp när man ska utveckla en ISP, då ramverket specifikt stödjer många olika delar kopplat till informationssäkerhet samt att det används av flertalet organisationer internationellt (ISO/IEC 27002, 2013).

Förutom ramverk som kan vara påverkande faktorer vid utveckling så har vi även sett utifrån resultatet att lagar och regelverk påverkar respondenternas utvecklingsarbete.

Samtliga respondenter påpekar att lagar har stor påverkan vid utvecklingsarbetet av ISP. Oavsett geografiskt läge eller bransch så bör en organisation ha koll på de lagar som kan komma att påverka deras arbetsområde och därför inkludera dessa inom deras ISP. Här kan man se företag 1 som ett exempel på detta då deras arbetsområde specifikt påverkades av att de hanterar statshemligheter och att de utefter det får anpassa deras ISP. Samtidigt visar både företag 2 och företag 3 att man bör genom analyser få fram vilka specifika lagar och regelverk som kan påverka utvecklingsarbetet. Vi förutsätter att detta är även något som företag 1 utför då de visar att de är väl medvetna om påverkande faktorer även om de inte specifikt nämnt detta.

5.2 Policy förmedling

Det empiriska resultatet visade att de tre företagen vi har intervjuat använder sig av olika metoder vid förmedlingen av ISP dokumentet.

Företag 1 använder sig av en metod som går ut på att utbilda anställda beroende på vilken säkerhetsnivå de tillhör. Företag 1 utför även kontinuerligt utbildningar som gäller för alla anställda oberoende vilken säkerhetsnivå de tillhör. Vid en uppdatering eller ändring i ISP dokumentet så utför Företag 1 även då utbildningar.

Företag 2 använder sig utav en annan metod som går ut på att först distribuera ISP dokumentet i organisationen. För att sedan hålla i ett test som anställda får utföra. Testet upprepas vid varje stor ändring av ISP dokumentet. Anledningen att Företag 2 utför tester på detta sätt är för att se till att anställda verkligen förstår och läser ISP dokumentet.

Företag 3 börjar med att distribuera ISP dokumentet så att de anställda har tillgång till det. Vid anställningsprocessen så går man igenom ISP dokumentet med den nyanställda. Sedan så skickar Företag 3 kontinuerliga små testfrågor via mail till anställda för att påminna anställda om ISP:n i företaget.

Vi kan konstatera redan från början att alla företag vi har intervjuat genomför någon sorts utbildning, träning eller andra metoder för att förmedla ISP dokumentet. Det hade även kunnat vara så att företagen bara distribuerar ISP dokumentet och väljer att inte fullborda förmedlingsarbetet med någon extra aktivitet. Som Knapp et al., (2009), Alshaikh et al., (2016) samt Flowerday och Tuyikeze (2016) påpekar så bör organisationer hålla i utbildningar eller träningar av något slag för att få anställdas samtycke, samt att få anställdas stöd och förståelse till varför ISP:n existerar.

Det som alla tre företagen har gemensamt vid förmedlingen av ISP är att de utför sina förmedlings metoder kontinuerligt. Som Knapp et al., (2009) påpekar så ska organisationer utföra sin förmedling kontinuerligt då ändringar ofta förekommer i ISP dokumentet. Även Alshaikh et al., (2016) påpekar att förmedlingsarbetet är en kontinuerlig process.

Företag 2 och företag 3 har som gemensamt med att de börjar med att distribuera ISP dokumentet i organisationen så att alla har tillgång till det. Företag 2 och 3 utför liknande metoder där de får anställda att utför test för att få bevis att anställda verkligen förstått och läst ISP dokumentet. Även om metoderna som företag 2 och 3 använder sig av skiljer sig lite så är konceptet likadant. Man kan konstatera att Företag 2 och Företag 3 utför tester som en extra åtgärd förutom att bara distribuera policydokumentet för att få anställda att läsa och förstå ISP dokumentet. Företag 3 går steget längre där de dessutom går igenom ISP dokumentet med en nyanställd. Som Alshaikh et al., (2016) menar så är detta inte tillräckligt att bara distribuera ISP:s för att garantera att anställda läser och förstår ISP dokumentet. Det krävs att organisationer utför fler aktiviteter för att garantera att anställda läser och förstår ISP dokumentet.

Det som skiljer Företag 1 gentemot de två andra företagen är att Företag 1 inte genomför någon extra åtgärd för att på något sätt garantera att anställda verkligen läser eller förstår ISP:n. Flowerday & Tuyikeze (2016) och Knapp et al., (2009) menar att utbildning ger ökad samtycke och stöd från de anställda. Då kanske Företag 1 inte behöver genomföra tester då man istället genom utbildning förklarar syftet och vad konsekvenserna blir om man inte följer ISP:n precis som Siponen et al., (2009) utpekar.

Metoderna som de tre företagen använder sig av är olika men slutresultatet som företagen vill uppnå är detsamma. Alla de tre företagen vill förmodligen att anställda följer de ISP:n som förmedlas och att anställda även förstår syftet och vilka konsekvenserna kan bli om ISP:n inte följs. Vilken metod företagen föredrar är inte viktigt så länge slutresultat uppnås.

6 Slutsats

Efter att vi har gjort vår undersökning så har vi kommit fram till slutsatser angående den forskningsfråga som ställdes:

- *Vilka skillnader existerar mellan större IT organisationer i Sverige när det kommer till utveckling och förmedling av informationssäkerhetspolicyn?*

Det resultat som vi har fått fram utifrån våra undersökningar visar förutom på klara skillnader, även vissa likheter mellan våra respondenter. Då vår forskningsfråga har som grund att se konkreta skillnader som existerar mellan respondenterna så är det just det vi lägger fokus på. Vi har identifierat en rad aspekter när det kommer till ISP men fokuserat på två delar av Information Security Policy Development Life Cycle som vi anser är mer viktiga, utveckling och förmedling.

6.1 Policyutveckling

Av det som vi har undersökt kring utvecklingsaspekter av ISP:s så kan vi konstatera att det existerar vissa skillnader mellan respondenterna. När det kommer till vem som bedriver och ansvarar för själva utvecklingen av ISP så fanns det klara skillnader mellan respondenterna Hos företag 1 så ansvarar en säkerhetschef för ISP, däremot så utvecklas den tillsammans med IT-chefen. Detta kan även konstateras hos företag 2. Hos företag 3 däremot så förklarar säkerhetsexperten att det är ledningen som har helhetsansvar-där även han själv sitter-för utveckling av ISP.

En annan klar skillnad mellan respondenterna när det kommer till utveckling av ISP är vilket fokus som existerar hos samtliga respondenterna när det kommer till utvecklingsarbetet. Företag 1 visar på att de är mer tekniskt inriktade när det kommer till ISP utveckling då deras huvudområde består utav teknisk mjukvara. Företag 2 och 3 däremot som arbetar mer brett inom flertalet områden kring IT visar på att de arbetar mer med människor i fokus än teknik.

6.2 Policyförmedling

När det kommer till förmedling av ISP:s så kan vi konstatera att det existerar skillnader mellan respondenterna. Metoderna de använder sig av skiljer sig mellan företagen. Företag 1 skiljer sig mest från de två andra företagen. Företag 1 håller i utbildningar kontinuerligt för alla anställda. Utbildningar beroende på vilken säkerhetsnivå den anställde tillhör utförs av Företag 1. Företag 2 använder sig av en förmedling metod där man istället först distribuerar ISP dokumentet så att anställda har tillgång till det för att sedan hålla i ett test som de anställda ska göra angående ISP dokumentet. Även Företag 3 börjar även att distribuera ISP dokumentet så att alla anställda har tillgång till det, däremot så skickar Företag 3 ut små testfrågor via mail för att påminna anställda om ISP efter distributionen. Företag 3 går även igenom ISP dokumentet med en nyanställd.

Anledningen till att det skiljer sig så mycket mellan företagen är svårt att svara på, men vi tror att anledningen till att företagen utför dessa olika metoderna när de kommer till utveckling och förmedling av ISP är att företagen har valt metoder som de anser passar bäst för dem själva.

6.3 Förslag på vidare forskning

Denna undersökning har haft som syfte att identifiera om det finns skillnader mellan IT-organisationer i hur de utvecklar och förmedlar ISP:s. Men det finns två faser inom Information Security Policy Development Life Cycle som vi inte har berört. Då kan det vara intressant att undersöka hur IT-organisationer i Sverige gör när det kommer till de två återstående faserna, Riskbedömning, Policy Övervakning och Underhåll. Det som även är intressant och som vi inte har berört är anledningen till varför det existerar skillnader mellan företagen när det kommer till utveckling och förmedling av ISP:s. Det kan även vara intressant att gå ännu mer på djupet kring själva IT företagen och se om det existerar skillnader om de företag som undersöks har liknande huvudinriktning, som exempelvis IT företag som säljer säkerhetsmjukvara likt företag 1 i vår undersökning.

Referenser

Alshaikh, M, Maynard, S, Ahmad, A, & Chang, S 2016, 'Information Security Policy: A Management Practice Perspective', arXiv, EBSCO*host*.

Andress Jason, J 2011, The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. n.p.: Burlington : Elsevier Science, 2011, 1 Edition, Syngress.

Diver, S. 2007. Information Security Policy - A Development Guide for Large and Small Companies. Sans Institute.

Flowerday, S, & Tuyikeze, T 2016, 'Information security policy development and implementation: The what, how and who', *Computers & Security*, 61, pp. 169-183, ScienceDirect, EBSCO*host*.

Gollmann, D. 2011: Computer Security. 3rd ed. Wiley. ISBN 978-0-470-74115-3, 460 p.

Hanson M, Johansson T, Lindgren C, Oehme R, 2015, Information Security - trends, A Swedish perspective, Publication MSB851. ISBN 978-91-7383-572-5.

Höne, K, & Eloff, J 2002, 'Information security policy — what do international information security standards say?', *Computers & Security*, 21, pp. 402-409, ScienceDirect, EBSCO*host*.
ISO/IEC 27002, 2013 Information technology -- Security techniques -- Code of practice for information security management, ISO.

Jacobsen, D. I. 2002: Vad, hur och varför: om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen. Studentlitteratur, Lund. ISBN: 9789144040967, 503 s.

Karlsson, F, Hedström, K, & Goldkuhl, G 2017, 'Practice-based discourse analysis of information security policies', *Computers & Security*, 67, pp. 267-279, Business Source Complete, ScienceDirect, EBSCO*host*.

Knapp, K, Franklin Morris, R, Marshall, T, & Byrd, T 2009, 'Information security policy: An organizational-level process model', Computers & Security, 28, pp. 493-508, Inspec, ScienceDirect, EBSCOhost.

Kostadinov, Dimitar. 2017. InfoSec Resources. *Key Elements of an Information Security Policy*. http://resources.infosecinstitute.com/key-elements-information-security-policy/. (Hämtad 08 May 2017).

Kryzewski, Jackie. U.å. Policy Development Manager - Protocol Policy Systems. https://mpa.co.nz/media/44980/Protocol-Policy-The-Importance-of-IT-Policies.pdf. (Hämtad 08 Maj 2017).

Legal Information Institute. 2017. *44 U.S. Code § 3552 - Definitions | US Law | LII / Legal Information Institute*. [ONLINE] Available at: https://www.law.cornell.edu/uscode/text/44/3552. (Hämtad 15 April 2017).

Rees, J, Bandyopadhyay, S, & Spafford, E 2003, 'PFIRES: A Policy Framework for Information Security', *Communications Of The ACM*, 46, 7, pp. 101-106, Business Source Complete, EBSCO*host*.

Riksdagsförvaltningen. 2017. Personuppgiftslag (1998:204) Svensk författningssamling 1998:1998:204 t.o.m. SFS 2010:1969 - Riksdagen . [ONLINE] Available at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/personuppgiftslag-1998204_sfs-1998-204. (Hämtad 03 April 2017).

Riksdagsförvaltningen. 2017. Offentlighets- och sekretesslag (2009:400) Svensk författningssamling 2009:2009:400 t.o.m. SFS 2017:184 - Riksdagen . [ONLINE] Available at:http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/offentlighets--och-sekretesslag-2009400_sfs-2009-400. (Hämtad 03 April 2017).

Security Intelligence. 2014. *Security Is Not a Technology Problem but a Process and People Problem*. [ONLINE] Available at: https://securityintelligence.com/security-risks-mobile-cloud-social-media-ciso/. (Hämtad 01 May 2017).

Siponen, M, Mahmood, M, & Pahnila, S 2009, 'Are Employees Putting Your Company At Risk By Not Following Information Security Policies?', *Communications Of The ACM*, 52, 12, p. 145, EBSCO*host*.

Stephen V. Flowerday & Tite Tuyikeze. 2016. Information security policy development and implementation: The what, how and who. Department of Information Systems, Computers & Security, 61, pp. 169-183, ScienceDirect, EBSCOhost.

Tuyikeze, T & Pottas, D. 2010. An Information Security Policy Development Life Cycle. Proceedings of the South African Information Security Multi-Conference (SAISMC 2010), pp 165-174.

Vad är informationssäkerhet?. 2017. *Vad är informationssäkerhet?*. [ONLINE] Available at: https://www.informationssakerhet.se/Om-informationssakerhet-kon/vad_ar_informationssakerhet/. (Hämtad 16 April 2017).

Appendix 1 – Intervjufrågor

Frågor som ställdes under intervjuer:

1. Vad heter du och vad är din roll på företaget?
2. Vad gör ditt företag?
3. Hur länge har du arbetat med säkerhet?
4. Vad är din uppfattning/definition utav informationssäkerhet?
5. Vem ansvarar för IT policys på ert företag?
6. Hur ser företagets policyformulering ut i dagsläget när det kommer till informationssäkerhet?
7. Följer ni eller använder ni någon/några ramverk eller standarder?
8. Anser du att det är viktigt att det finns konkreta policys kopplat till informationssäkerhet? Varför?
9. Hur arbetar ni med att ta fram och definiera policys kopplat till informationssäkerhet?
10. Är policyarbetet en kontinuerlig process eller sker det endast en gång?
11. Hur förmedlar ni policys till de anställda?
12. Vem tar ansvaret om någon bryter mot en policy?
13. Kan vi använda företagets namn samt ditt namn i rapporten eller vill du att det ska vara anonymt?

Appendix 2 – Transkribering av intervju, Företag 1: IT-chef

Rad	Text
1	Danial: Vad är din roll på företaget?
2	IT-chefen: Jag är CIO, IT-chef på svenska då och ansvarar för all informationsteknologi som finns på företaget.
3	Danial: Alright, som du vet så handlar vår intervju om policys inom informationssäkerhet och kan du berätta lite kort om vad Företag 1 gör?
4	IT-chefen: Företag 1 bygger och konstruerar produkter för säker nätkommunikation. vi har dels en VPN lösning som innebär att du kan på ett säkert sätt kommunicera mellan två delar i ditt företag eller i verksamheten via en krypterad linje. Sen har vi en data diod som ser till att du har kontroll på trafikflödet, alltså om du vill att trafik in i nätverket enbart ska gå på ett håll så sätter du en data diod. Så säkerställer den att trafik inte kan gå på två håll. Och sen slutligen har vi något som kallas för ******* och det är en produkt som är väldigt bredd men framför allt handlar om att den ska garantera att det du verkligen får in i ditt nätverk eller för ut ur ditt nätverk är rätt saker. Alltså vi kan på dokument nivå sätta till exempel att dokumentet 1 eller 2 inte får lämna huset och försöker du flytta det dokumentet antigen via mail eller via Dropbox eller vad det nu är, så kommer då den här tjänsten stoppa detta. Och sen slutligen så har vi en produkt som (tredomänsseperation) och det handlar om att bygga bort det som kallas för Snowden effekten. Snowden om ni känner till honom han satt ju egentligen som en tekniker, han hade ju ingenting med det som NSA egentligen gjorde. Men i och med att han satt i ett läge där han såg all information, så kunde han då lyfta den och spridda den. Och det vi har byggt är en patenterad teknologi som innebär att du kan ha tekniker i väldigt känsliga utrymmen men där de absolut inte får tillgång till vår data. Så det är Företag 1.
5	Danial: Hur länge har du arbetat med säkerhet?
6	IT-chefen: Oj, Säkerhet har jag nästan jobbat i 16 år. Samma dag som du satte foten i ett It-företag eller IT-verksamhet. Så börjar du prata om säkerhet. Olika typer av säkerhet och det har ju ändrats över åren. Första åren jag började jobba med datorer och IT så handlade det mer om att sätta upp en brandvägg och så var man skyddad tyckte man, och idag då när man sitter i nätverk idag så har du så mycket mer än bara en brandvägg. Även om brandväggen finns kvar men den ser mycket mer annorlunda ut än va den va tidigare.
7	Danial: Vad är din uppfattning eller definition utav informationssäkerhet?
8	IT-chefen: ja alltså, min uppfattning kring informationssäkerhet det beror ju lite grann på vad du ät ute efter. Om du vill prata definitionen informationssäkerhet eller hur det ser ut i Sverige eller världen i stort? Tittar man på definitionen informationssäkerhet så handlar det ju om ett sätt att definiera hur du ska hantera din information. Vi som företag eftersom vi levererar till statsmakter så lyder vi

	ju oftast under deras regelverk, det betyder att vi har en enklare väg fram. Vi har ganska fördefinierat hur olika dokument ska klassas, om de är hemliga, om de är sekretess eller om de är till och med topphemliga och så vidare. Och där igenom finns där då ett regelverk för hur man ska hantera detta. Det är väll så jag definierar om man skulle säga så.
9	Danial: Ja men det är lite det vi är ute efter liksom, själva ordet.
10	Danial: Om vi då ska börja prata lite om policys. Finns det nån som ansvarar för IT policys på ert företag eller är det ett helhetsansvar i företaget?
11	IT-chefen: Alltså, i vårt företag så är det ju så att vi har en säkerhetschef och hennes ansvar är att upprätthålla, utveckla och driva igenom säkerhetspolicys som vi har. Det ligger i hennes i hennes tjänst eller arbete. Så i vårt fall är det en säkerhetschef.
12	Danial: Alright, nu är det en ganska allmän fråga som vi inte är ute efter detaljer, men om vi ska se på företagets policyformulering i dagsläget hur ser det ut då när det kommer till informationssäkerhet?
13	IT-chefen: Alltså den är väldigt strikt, och det är ju på grund av att vi hanterar känslig information. Vi hanterar ju i många fall statshemligheter och det innebär att vi har ett ganska hårt tryck på oss att följa då dels dom länders lagkrav som finns kring hur man ska hantera känslig information. Och det gör ju också att vårt företag är ganska mogen i den diskussionen Vi kan ju ibland se på med förvåning över att vissa diskussioner som förs på nätet och utanför, för oss är detta en självklarhet. En hemlig handling är en hemlig handling, och den hanteras därefter. Och vi har en väll utvecklat och väll definierat policy regelverk både för dom dokument som finns utanför vårt hus alltså det vi tar emot men även våra interna dokument. Så där är vi ganska så långt fram skulle jag vilja säga.
14	Danial: Alright och om vi då går in på dem lite policys, är det typ nåt specifikt ramverk eller nån modell ni följer utöver er egna som ni har skapat då?
15	IT-chefen: Ja, det är ju klart. Alltså vi återigen eftersom vi jobbar med svenska statsmakten så lyder vi ju under offentlig sekretess lagen. och sekretesslagen är ganska tydlig vad som gäller och där finns en definition ifrån dem kunder vi har. Typ alltså polisen, säkerhetspolisen, försvarsmakten, försvarsunderrättelsetjänst och då finns där ett regelverk som vi måste anamma. Och det är ganska tydligt vad vi ska välja där. Så att om man pratar regelverk och vilken form så är det ju lagen om offentlighetens sekretess som vi lyder. Och det är de regelverket vi styr efter.
16	Danial: ISO standarderna då?
17	IT-chefen: Ja, alltså vi har ISO 2001 då vi kommer gå över till 2015 nu, Men det är den ISO standarden vi följer om man tittar på dokumenten hanteringen. Men för oss är ISO en underordnad för ISO är en trots allt ändå inte ett regulativt krav. Skulle det nån gång hamna i en situation där ISO står emot det regulativa kravet så vinner ju alltid det regulativa kravet. Så att ur vår synvinkel så är det inte så att vi tittar mer på lagen och offentlig och sekretess än vi tittar på ISO.

18	Danial: Tror du man skulle kunna säga att ISO'n fungerar som bara typ en hjälpväg eller liten grund.
19	IT-chefen: Alltså nej ISO om man säger så som att i och med att vi följer lagen om offentlighet och sekretess så får ju mycket på köpet när det gäller ISO standard. Och det gör ju att vi följer ISO standarden utifrån dess regelverk, men vi har också möjlighet att göra avsteg när ISO'n går på kors med lagen om offentlighet och sekretess i så fall.
20	Danial: Alright, när det då kommer till policys anser du att det är viktigt att man har just konkreta policys kopplat till informationssäkerhet eller liksom räcker det med att det finns bara policys lite mer allmänt?
21	IT-chefen: Nej, det är väll det som är lite grann av vår affärsidé också att vi menar ju på att svenska företag och verksamheter idag är alldeles för dåliga. Dom är väldigt naiva i tron om att de faktiskt är skyddade. Det finns så uppenbara fel där man inte har en policy och där man inte följer policyn. Det finns säkert om du frågar dem flesta statliga verk att de har en informationssäkerhet policy, ja det har nog alla för det är de skyldiga till att ha. Men det är en hyllvärmare och det är ingen som följer dem eller använder dem. Man kan ju ta ett gyllene exempel jag vet inte om ni har läst det här om den är bilverkstan, som med jämna mellanrum får personalakter skickade till sig till sin fax från socialkontoret i Lund. Det finns ju informationssäkerhets policy på socialkontoret i Lund hur dem ska hantera känsligt material, trots det så upprepade gånger så har en tjänsteman skickat känsligt material över en fax. Och inte ens en gång brytt sig om att kontrollera vilken mottagares fax den landar i, utan i detta fallet så kan då personliga integritets kränkande dokument dyka upp i bilverkstads fax. Och trots att han har både upplyst socialkontoret och gått ut i tidningarna så är det ju en ständig återupprepande av detta felet. Och där kan man ju konstatera att dem tar ju inte tag i detta och lutar sig på sin policy som egentligen säger nånting misstänker jag. Där hade jag väll sett gärna att departement och även företag går mer åt den lite hårdare vägen som vi nu har med de här regulativa kraven. För det går att använda det regelverk som finns i lagen om offentlighets och sekretess även om det är en privat verksamhet även om det egentligen inte styrs av denna lag. Så kan man använda den på ett bra sätt och därigenom få en bra policy. Så ja jag tycker det är jätteviktigt.
22	Danial: Ok, nu vet jag inte om detta är ditt område så mycket men hur arbetar ni på ett ungefär med att ta fram eller definiera policys kopplat och är detta alltså kontinuerligt eller gör ni kanske det några enstaka gånger?
23	IT-chefen: Igen då så när det gäller våra policys, så är dem då reglerade i lagtext för att kunna bedriva den verksamheten vi har. Och det gör ju att policyn tas fram eftersom det regelverk som finns helt enkelt och det är vi ålagda att göra. Vi är dessutom ålagda att en uppdatering varje år och då gör vi ett uppföljningsarbete och det handlar ju mer om att titta över, har det skett någon ändring i lagkraven, finns där några projekt som kräver något extra. Så ja vi gör en årlig uppdatering kan man säga.
24	Danial: Ok, Hur förmedlar ni policys till de anställda?

25	IT-chefen: Dels så har vi en introduktion när dem anställs, dels så har vi ju utbildningar beroende på vilken säkerhets nivå dom har på företaget. Och där får dom i alla dem utbildningarna oavsett vilken nivå dem är så får dem hela tiden utbildning i den policyn som gäller för alla. Och sen har vi kontinuerliga utbildningar årsvis där vi utbildar hela personalen i hur man jobbar med de här frågorna.
26	Danial: Nya anställda får då en introduktion?
27	IT-chefen: Ja
28	Danial: Men säg att det kommer en ny version eller nån ny uppdatering då tar ni in alla all in samtidigt?
29	IT-chefen: Då gås den igenom med alla
30	Danial: Så alla kör en uppdatering tillsammans?
31	IT-chefen: Yes
32	Danial: Yes och nu kanske vi vill peka på en person men allmänt men vem tar ansvaret om någon bryter mot en policy? eller blir typ företaget i allmänhet som får ta ansvaret för såna saker?
33	IT-chefen: Nej och där är vi ju tillbaka till de regulativa kraven vi har, får vi en incident så är vi skyldiga att anmäla detta upp till då våra beställare eller kunder. I det fallet som om tydlig gång där säkerhetschefen får en incidentrapport av den personen eller av den personens chef att detta har hänt, sen gör ju vi (jag tillsammans med säkerhetschefen) en utredning hur det har drabbat företaget, vad är det för informations läcka vi har och sen drar vi ju det då vidare till dem myndigheter som vi jobbar mot. Och sedan är det upp till dem att ta beslut huruvida det ska göras en större utredning eller om det ska införas nån lagföring. Alltså har vi begått brott då blir det den enskilda personen för du har ju alltid ett personligt ansvar. I den verksamheten vi bedriver så är det alltid personligt ansvar, det är aldrig företagets ansvar.
34	Danial: Så att om någon läckte information?
35	IT-chefen: Ja
36	Danial: Och dem är skyldiga till det och ni får reda på då är det dom som ansvarar för det?
37	IT-chefen: Ja det är så att om du läcker statshemligheter så är det ju spioneri av något slag och du lyder du under spionerilagen och då blir du lagförd. Så att det är ganska enkelt. Är det sen våra egna produkter så kommer vi inte driva det vidare. Vi har ju både en civil del och vi har en militär del så att säga, och är det den civila delen då blir det ju mer en intern. Då kan man ju säga att om du skulle läcka uppgifter även om den civila delen så jobbar du ju inte kvar här, är du beredd på att läcka civila uppgifter då kan vi inte ha dig på den militära sidan så det är ganska enkelt. så det kvittar kan man säga.

38	Danial: Ni har ju system ute hos kunder och det är väll lite samma sak där måste det va att om något sker alltså när era system är inblandade på ett annat ställe då liksom tar dom också ansvaret då eller?
39	IT-chefen: Det beror ju på, alltså vi tar ju ett ansvar att vår produkt är så säker som den är. Skulle det vissa sig att vår produkt inte är det så får vi ta ett ansvar för det, men däremot om deras anställda begår brott eller dem gör någonting felaktigt så är det dem som får ta det ansvaret och det gör ju inte vi. Så länge vår produkt gör det den ska så är vi ju "Scot-Free" så kan man säga.
40	Danial: Ni kan inte alltid vara exakta, men så länge ni liksom följer inom ramarna så är det ändå lugnt. Vi pratar mycket om typ mänskliga faktorn eftersom oftast är det just mänskliga faktorn som är ett säkerhets hot i företag. Allmän syn på mänskliga faktorn och dina erfarenheter skulle du anse att det är typ det som är det största problemet när det kommer till informationssäkerhet?
41	IT-chefen: Alltså tittar man på en riskanalys på ett företag så är alltid den mänskliga faktorn det svåraste, alltså det som är högst risk. Tittar man på en angrepps synvinkel så är det lättaste vägen in. Skulle du angripa t.ex. mitt företag här, att göra det teknik vägen kräver i princip en storlek om NSA eller Kinas eller Rysslands cyberförsvar. Det är dom som klarar det. Men det som är risken med det är ju upptäcks risken. för skulle vi få attacker mot oss, bruteforce attacker eller vad det nu än är. Så har vi ju ett alarmsystem som signalerar att nu är du under attack. Och det gör att vi landar i en situation där vi blir en svår motståndare att komma åt utifrån. Tittar man på dem länder som driver underrättelsetjänst i Sverige, så bedriver dem enbart mänsklig verksamhet. Dem vill plantera nån, rekrytera nån för att det är den lättaste vägen. Att få någon att bära ut ett USB minne med hemliga uppgifter är enklare än att försöka penetrera elektroniskt. Det gör också att den mänskliga faktorn måste man alltid ta hänsyn till när man diskuterar säkerhet och det man måste hela tiden titta på, det är ju att man inte bygger in en Snowden effekt, där någon enstaka person kan få tillgång till så att säga hela informationsmassan. Utan att man hela tiden strikt får tillgång till det som man behöver till sitt arbete. För det som om man tittar på Snowden det han snodde eller det han tog och det han släppte, inget av det va ju nån information som han behövde för sitt arbete. Utan han hade ju tillgång till strömmen och det är den vi försöker med vår teknik bygga bort och vi har definitivt den synen på den verksamheten vi bedriver.
42	Danial: Men när det kommer till då säkerhet som ni bedriver alltså skulle du eftersom du ändå vill snacka om mänskliga faktorn att det är människor som rör på sig och hämtar ut grejer, då kan man säga lite så att liksom man kan bara gör så mycket typ mjukvarumässigt för att stoppa sånt. Men sen om man tänker på annat bara på typ kontoret liksom.
43	IT-chefen: Alltså vi eller dom produkter som vi gör som vi levererar handlar om ju mer om att skydda dig rent tekniskt. Vi har ingen produkt som skyddar dig från att en anställd tar en kopia av ett hemligt dokument, stoppar det i fickan och går ut härifrån.

44	Danial: Så typ såhär kameror eller liksom som ändå kan identifiera enstaka individer?
45	IT-chefen: Vi har ju inte valt att göra det och det är ju en svår väg att gå, jag tror ju inte vi är ett samhälle som kommer att acceptera kameraövervakade arbetsplatser. Tittar du på dem allra hemligaste platserna i Sverige så tror jag inte ens att dem är kamera övervakade. Inte ur perspektivet att man övervakar personalen. Utan där menar väll vi och även om man tittar på militär underrättelsetjänsten och SÄPO, deras syn på det så menar dem att personkännedom är bättre än teknisk övervakning. Därför att du kan se på en person, det är ganska tydligt vad som händer med en person som bedriver underrättelseinhämtning. För det första så har du ju, det är inte som så tittar du på rekrytering till exempel av en källa. Så är det inte så att du går fram till en person som mår bra, har liksom bra ekonomi, bra äktenskap så är ju den personen extremt svår att rekrytera. Utan det du letar efter är ju en person som antigen har en lite kass ekonomi eller har äktenskapet eller kärleken är på väg att krackelera eller har någon form av alkohol eller narkotikamissbruk. Dom tre faktorerna är ju oftast kända på förhand. Vi som företag vet ju om har en person som har ett alkoholmissbruk eller man börjar se signalerna på samma sätt om det börjar bli taskigt hemma så brukar man se det. Och det gör ju att har man bara en uppmärksamhet så kan man ju se dom personerna som är på väg in i en riskzon. Och då gäller det ju att vi som säkerhetsorganisationer håller ett lite större öga. Och då blir det ju så att mönstret bli ju ganska tydligt för den som ska komma åt dem här dokumenten, jobbar senare än vad dem har gjort tidigare kanske, dyker upp på udda tider och alla dom mönster tittar vi på. Och när vi ser sånt mönster, ja det är då vi då agerar.
46	Danial: Om vi då kommer tillbaka till policys, alltså eftersom ni gör produkter åt andra. Säg då att ni ska ge ut er tjänst till nån myndighet eller nånting som kanske inte har så bra säkerhets policy som du sa liksom. Försöker ni på något sätt liksom förmedla alltså att det är viktigt till dem eller liksom hålla nån sorts föreläsning eller hjälpa dem?
47	IT-chefen: Vi är ju samtidigt som i ett säljande företag också ett utbildande företag. Vi försöker ju hela tiden prata med dom företag som vi kommer i kontakt med. Oftast får vi en problembild där man tror att vi kan lösa hela bilden. Där vi är väldigt tydliga att vi kan gå in och lösa det tekniska till dig men där vi också pekar på vad dem måste göra rent intern mässigt, utifrån hur dem ska hantera det. Återigen bara för att du kommer burk och sätter in den så har du egentligen inte löst problemet. Du har skyddat dig, det har du ju men du har ju inte löst det interna hotet det har du inte.
48	Danial: Så det är liksom eftersom ni har ändå har så starka policys i ert företag så vet ni att, om ni ska ha ert system så är det utan problem. För att skickar ni en högteknologisk lösning till någon annan, men sen har dem inte ens koll på sin personal något sånt så har den nästan ingen mening.
49	IT-chefen: Ja precis, där kan man ju också se att tittar man på angreppen som har gjort i världen så är 70% av dem att man bär ut information. 30% är att du skickar över nätet, det är ju väldigt lite egentligen. Det är ju övervägande att du bär ut information. På dig på USB minne eller nånting, men det är det handlar

	om. Det är egentligen bara av nå underlig anledning pedofiler som tror att man inte kan hitta dem i företags nätverket, men alla andra verkar ha fattat at vi har en övervakning. Så det är väldigt sällan, de här 30% är dem här jätteklumpiga försöken som oftast blir upptäckta vid första dokument släpp. Medan dom som bär ut kan i princip tömma ett företag innan det upptäcks.
50	Danial: Yes, om du personligen tycker att exempelvis nån policy som finns där ute eller någon modell är alltså något man bör följa alltid eller tycker du man borde bygga det från scratch liksom?
51	IT-chefen: Nej alltså, Som jag har sagt ett par gånger tidigare så lagen om offentlighet och sekretess det är en bra grund bas. Och ur den så kan man bygga policys och följer man den och den tillhörande informations klassning som finns där så är man i princip hemma med sitt arbete.
52	Danial: Så du skulle säga att det gäller för oavsett vilket företag man är eller vilka man jobbar med liksom?
53	IT-chefen: Ja, men det kokas ju alltid ner till vad man är beredd att göra, för det är ju det de handlar om. Inför du en strikt informations säkerhetsklassning, inför du en strikt informationssäkerhets policy. Ja då blir det inte lika lätt som när du inte hade det. Det är ju därför det inte funkar ute på myndigheterna. Därför att dom inte orkar ta striden med sin personal, att säkerhet inte är enkelt. Ja det blir lite kluddigare än det var igår men målet är ju fortfarande att vi faktiskt ska bli en säkrare myndighet. Och det är väll det som jag brukar säga, pendeln snurrar alltid ett par hundra varv innan liksom är färdig. Jag menar de senaste 10 åren har vi spenderat med att det ska bli så enkelt och du ska alltid få tillgång till allting var du än befinner dig, och hur du än befinner dig på vilken plattform. Nu har ju folk börjat inse att ja det har ju ett pris. Det har ett pris med riggade val, Fake News, informations läckor och så vidare. Därför att det är att tar du inte hand om dig, skyddar du inte dig och du samtidigt ska ha den öppenheten än detta. Och det är ju där nu pendeln är på väg tillbaka när alla inser att jo men det var jättekul att ha hela företagshemligheten i Dropbox ända fram tills kineserna snodde den och byggde ett plan som ser exakt likadant ut. Alltså då är det inte lika roligt. Och då helt plötsligt börjar man inse att den där enkelheten för din medarbetare kostar mig just nu 2 miljarder. Hade det inte varit enklare att han hade kanske lite tuffare och komma åt sitt dokument. Så att det är ju där vi står nu och vacklar. det är där jag hoppas liksom att folk ska trilla över på den här andra sidan. Därför du kan bygga säkerhet smidigt, du kan komma åt dina dokument, du kan komma åt dina dokument på olika plattformar. Det är bara det att vi vill lägg ett säkrare skall på det. Och det gör kanske du får logga in en gång extra än vad du i vanliga fall brukar göra, men om det räddar ditt företag så har jag svårt att förstå att man tvekar i det läget.
54	Danial: Så typ i allmänhet så skulle du säga nästan att företag är typ om vi nu ska prata såhär vardagligt är lata typ?
55	IT-chefen: Nej, alltså inte lata utan det handlar ju om att för det första tror jag att man alltid utgår från att det inte händer inte mig. Och sen har man ett medarbetar krav, där man liksom är mer orolig för vad medarbetaren ska tycka än att man säkerställer att man inte förlorar pengar. Har man aldrig förlorat

	några pengar så blir det ju svårt att övertyga den Vd:n att det finns en risk i att du förlorar pengar. Men vi har ju aldrig förlorat några pengar, nej men det finns en risk. Alltså den ju ganska så tuff att ta den diskussionen. Min förhoppning är ju att det har ju sen varit en tradition att har du blivit hackad, har du förlorat så är det inte så att du ställer dig på piedestalen och säger att jag blev hackad. Och det gör ju att vi vet ju inte egentligen inte hur mycket har våra företag förlorat egentligen. Vi vet ju till exempel att det finns ett väldigt tydligt tecken. SAAB, deras spaningsplan vet ju finns i Kina det finns ju en exakt kopia det radar och spaningsplan som SAAB byggde finns ju i Kina och driftas i Kina. Men Saab har ju aldrig erkänt att man har snott ritningarna. Och dom har nog tänkt efter ett par gånger om sin säkerhet. Och det gör ju att många företag säkrar upp sig utan att berätta för sitt grannföretag och det gör ju att alla vi möter, dels att det inte händer mig och dels hur utbrett är det. Och då blir det ju den här effekten. Och sen har man då det interna kravet från sina säljare, sina anställda att oh shit, jag måste kunna i princip när jag sitter i båten utanför min sommarstuga så ska jag på en halv taskigt 3G lina komma åt alla mina dokument och kunna göra alla mina affärer. Ja, då blir det ju vad det blir liksom. Sen att man kanske skulle ha haft en sundare inställning att när du sitter där i den båten utanför din sommarstuga så ska du nog skita i den dokument för så ska du nog ha semester. Så att det är ju lite så det är väll där jag står.
56	Danial: Har du något vi vill tilläga?
57	Ardian: Nej
58	Danial: Det var nog majoriteten av våra frågor liksom, men vi tackar så mycket för att din tid vi har lagt på intervjun så avslutar vi den nu.
59	IT-chefen: Inga problem, tack själva.

Appendix 3 – Anteckningar under intervjun – Företag 2: Säkerhetsansvarig

Rad	Text
1	Danial – Vem är du samt vad är din roll?
2	Säkerhetsansvarig - Jag är ansvarig för säkerhetsområdet, roll som konsultchef, utvecklar affärsområdet, håller kontakt med kunder, ser till att krav o arbete görs. Utveckla medarbetarkompetens, detta breddar portfölj. Företag 3 är ett konsultföretag under en teleoperatör.
3	Danial - Hur länge har du arbetat med säkerhet?
4	Säkerhetsansvarig - Arbetat med säkerhet i 17 år. Sysslat med säkerhet sedan 1997.
5	Danial - Vad är din uppfattning/definition utav informationssäkerhet?
6	Säkerhetsansvarig - Om man frågar de som inte är säkerhetsexperter så säger de att säkerheten är hygienfaktor, alltså att det är bra att ha. Jag håller inte med, dagens samhälle är digitaliseringsera som är påväg mot slut, nu kommer automatiseringsera. Då är säkerheten en livsviktig faktor jämfört med hur det ser ut idag. Idag kan en hackare ta över exempelvis en bil genom olika sensorer vilket visar på detta. Jag skulle inte säga att säkerheten är hygienfaktor, alltså något som är bra att ha. Säkerhet för företag som jobbar inom informationsbranschen eller med människor är livsviktigt. Först online betalningar, sen point of sales, allt övervakas. Ikea kommer exempelvis bli en leverantör av det digitala hemmet medans för bilföretag så blir det i självkörande bilar. Sony fick 70 miljarder stämningsansökan på grund av bristande säkerhet. Ju mer vi kommer in i digitalisering och automatisering så är informationssäkerhet ännu viktigare. Människor som inte förstår detta och oftast är chefer från ekonomiska delar (sälj, marknad etc). Dessa människor har oftast inte förståelse, det är säkerhetschefen som är viktig då han måste övertyga dessa människor. Det är genom att lära de som inte är kunniga inom säkerhet. När man uppfyller otalade behov så öppnas en ny värld för kunden, vi använder säkerheten som en differentiella själv mot kunderna. Säkerheten används som en unik sellingproposal vilket ökade antalet sälj och kunder. Anpassa budskapet till motparten.
7	Ardian - oftast är det väl att tills de börjar förlora pengar så inser de hur viktigt säkerhet är.
8	Säkerhetsansvarig - Ja men även att förlora kunder. Kunder är viktiga. På grund av säkerhetsbrister kan företag förlora hela deras identitet eller förtroende. Allt hänger på hur

	man paketerar det och hur man säger saker än vad man säger. Man ska hänvisa till företagets värde. Vid implementering av policys måste man leva sig i hur mottagaren lever sig in i detta, bearbeta olika delar av företaget, jobba med olika versioner/drafts till allt från chefer till vanliga anställda. Först ska man vinna företagsledningen förtroende och stöd.
9	Danial - Vem ansvarar för IT policys på ert företag?
10	Säkerhetsansvarig - Det finns missuppfattning mellan infosäkerhet och it säkerhet vilket är den största nackdelen. Säkerheten ska inte kontrolleras av IT, den ska istället övervaka IT. Varje företag bör ha en säkerhetsansvarig. Det finns vissa standarder som är viktiga att uppnå. Företag väljer oftast säkerhetsansvariga men lägger dem under IT. Detta skapar problem oftast inom företaget då det kommer mycket input från just IT chefen o inte utifrån hela företagets behov. När jag kom in på ett tidigare bolag så blev jag placerad under infrastruktur. Efter ett tag lobbade jag med att säkerheten inte ska vara placerad inom IT. Det ska aldrig vara placerat under IT om det inte är ett renodlat IT företag. I renodlade IT företag i ex google eller blizzard sitter säkerhetschefen i styrelsen. Adobe flash försvann pga säkerhetsrisker hela tiden. Adobe tog in säkerhetschef till styrelsen för att lösa problemet. Ju mer viktigare IT blir desto mer makt vill de på IT ha. Säkerhet ska rapporteras till ledningen. Integriteten ifrågasätts som säkerhetschef då man har stort ansvar. Det gäller att man är fri från brott och kan ses som pålitlig. Det görs många kontroller oftast vid sådana positioner. Tekniker och business är skilda mentaliteter. IT människor är i sin egna bubbla och har ingen aning om vad marknaden vill ha. Business är en viktig del att förstå. Balans är viktigt i ett företag.
11	Danial - Hur ser företagets policyformulering ut i dagsläget när det kommer till informationssäkerhet?

12	Säkerhetsansvarig - Man börjar med att identifiera externa och interna krav. Sedan samlar man dem kraven. Dessa är kärnan i policyn alltså det grundläggande. Ut-kraven kommer från lag, myndighet och kunder. Inre krav kommer från ägare, ledningen och interna krav. Kring dessa tas alltid olika beslut. Man försöker gör policyn så struktuerat som möjligt. Det ska stå allt från vad man exempelvis inte får göra till exempelvis om företaget övervakar medarbetare etc. Det kommer även input från risksidan, detta är byggt på analyser. Det kan även byggas på standarder. Exempel här kan vara ISO27000. När allt detta som nämnts sammanfattas så får man ett ganska brett policydokument. Detta dokument ska göras i olika draft versioner och sedan spridas till olika delar i företag (ledning, hr, operation, sälj finans etc). Mycket måste avgöras genom juridiska aspekter, exempelvis om man får driva sin policy gentemot ens anställda. Språket ska vara tydligt så att alla förstår. Först skapas ett dokument det går till resten av företaget för utvärdering och sedan så ska det kommuniceras när man har en skarp version av allting. Det ska först till cheferna där det ska förklaras varför man ska göra exempelvis det som står i policyn. Uppföljningen när det kommer till implementering av policy är den viktigaste delen.
13	Ardian - På frågan, hur ser du att någon har läst policyn?
14	Danial - Man kan få dem att gå igenom ett test?
15	Säkerhetsansvarig - Ja korrekt, eller få alla att signera. När vi gjorde ett quiz innan så är det viktigaste att få alla att göra alla frågor och gå igenom policyn samtidigt som man får en signatur vilket säger att personen är medveten. Ett Quiz är ett bra sätt att gå till väga när det kommer till uppföljning då man får en signatur på att medarbetarna i företaget har gått igenom policyn.
16	Ardian - Skulle ni säga att ni kom på metoden med quiz när det kommer till policy och uppföljning?
17	Säkerhetsansvarig - jag har inte uppfunnit hjulet så att säga men utifrån erfarenheter så har jag kunnat ta fram detta sätt att följa upp säkerhetspolicyn. Samtidigt får man en mätbar punkt för exempelvis kunder. Jag tittar på mänskliga sidan av företag för att förstå helheten (mentaliteter etc)
18	Ardian - Så du tycker compliance är viktigast?

19	Säkerhetsansvarig - Jag skulle säga uppfyllning, compliance är det man uppfyller så som förklarat innan det med in o ut, standarder, risk etc. Policy ska vara byggt på kunskap och även ansvar. Policies måste skräddarsys till företags identitet. Ge ut diplom eller ha kunskapstest, ökar chansen. När det förhandlas i säkerhet går man med i avtal och därför bör policies innehålla marknads ställda krav.
20	Danial - Är det kontinuerligt?
21	Säkerhetsansvarig – man gör det en gång, varje ny anställd ska göra det och vid major changes.
22	Ardian - eller när nya GDPR kommer.
23	Danial - Följer/använder ni någon/några ramverk eller standarder?
24	Säkerhetsansvarig - Standarder för mig är verktyg, alltså något som underlättar. Ska man använda standarder ska man göra det för att man har genuina önskemål att vilja använda sådant. Jag valde iso27000 på grund av det naturliga till säkerhet. Jag hittade gemensamma nämnare av krav och policy och kunde bygga mer utefter detta.
25	Danial - Vem tar ansvaret om någon bryter mot en policy?
26	Säkerhetsansvarig - Bryter man mot policy har man personansvar. I policyn står det att slutgiltiga ansvar för företagssäkerhet ligger på ledningen. Ledningen har direkt ansvar mot ägarna. Ledning vill bestämma men slippa ansvar, policy specifierar att ledning får bestämma men även tar ansvar. Policy visar varje rolls ansvar där säkerheten har en viss aspekt.
27	Danial - Är det skillnad land till land eller mellan endast företag när det kommer till policy.

28	Säkerhetsansvarig - Policyn håller ganska vanligt innehåll så länge man är i EU eller USA. Det som skiljer mycket är mognadsnivåer bland länder. Varje rättinstans i olika länder får ta beslut. Man ska kunna prata om risker på affärsmässig nivå. Förståelse för policys av ledning etc avgörs om hur man är som person i grunden. Helheten spelar roll. Strategin för implementering av policy är top-down. Det tekniska när det kommer till säkerhet har blivit bättre men det som inte förbättras är själva människan. Istället för att vara kontrollcentriska ska man vara människocentrisk. Mognadsnivån är ganska låg i Sverige. Mänskliga faktorn får alltid vara med. Man ska vara pedagogisk. Kör topdown, blanda in olika grenar som psykologi, finans, hr, sälj etc.

Appendix 4 – Transkribering av intervju - Företag 3: Säkerhetsexpert

Rad	Text
1	D - Vad gör då Företag 3, företag du jobbar på?
2	SE – Företag 3 de sysslar med en verksamhet inom IT där vi gör säkerhetstestning, där vi kommer se sikta oss till att verksamheten ska sätta fokus på våra kunders verksamhet kan man säga och ser till att den följer digitaliseringen säkert.
3	D - Vad är din roll exakt på företaget?
4	SE - Cyber security expert, inriktning analyser, policy, dokument och säkerhetslyrik.
5	D - Hur länge har du jobbat med säkerhet?
6	SE - 24 år.
7	D - Om du skulle definiera informationssäkerhet, hur skulle du göra det då?
8	SE - Informationssäkerhet är det skyddet som människan har ett digitalt ekosystem när de pratar med varandra eller teknik.
9	D - Vem ansvarar för IT-policys på ert företag?
10	SE - Det är ju ledningen, det är sverigeledningen som sätter policydokumenten för informationssäkerhet och säkerhetsstrategi.

11	D - Sitter du med i ledningen?
12	SE - Jag tillhör den ja.
13	D - Om vi kollar på policys kopplade till informationssäkerhet, hur skulle du säga att er policy ser ut i dagsläget, alltså inte i detalj utan mer översiktligt, lite så som du förklarade i början.
14	SE - Vi har nog glidit som många andra IT bolag att vi har nog hamnat i kategori 2, det vill säga att vi har haft en väldigt juridisk riktad policy. Nu vill jag påstå att den är väldigt mycket kategoriserad, den är väldigt enkel, den är väldigt enkel att förstå, den är väldigt enkel att förstå riktningen framöver från den som kommer och inte sitter i management och inte sysslar med säkerhet. Så att jag skulle vilja påstå att vi är mycket (enklare?) idag.
15	D - Följer ni eller använder ni ramverk/standarder?
16	SE - Absolut. Sogeti är ju mer än bara Sverige så vi använder naturligtvist globala ramverk, vi använder oss naturligtvis utav ISO27000.
17	D - Anser du att det är viktigt att det finns policys som är konkret kopplade till informationssäkerhet eller att det är bara en del som man kan ta med i helheten?
18	SE - Nej, det ska finnas särskilt utstuderade policydokument som styr informationssäkerhet och det är min fasta åsikt.
19	D - Och varför skulle du säga att detta är viktigt?
20	SE - Därför att, tittar vi på IT säkerhetspolicy så styr den tekniken. Informationssäkerhetspolicy har varit väldigt tekniskt betingade men i och mer o

	mer individen i det digitala ekosystemet, och så länge vi är levande individer så måste det finnas ett särskilt ramverk som styr interaktionen mellan varandra.
21	D - Hur arbetar ni med att ta fram policys kopplade till informationssäkerhet?
22	SE - Naturligtvis så blir det väldigt mycket trendbevakning, alltså vad finns det för hotbildstrender, vad finns det för positiva digitaliseringstrender, och då sker det i oftast en analytisk workshop forum där vi identifierar att vad kan det här få för impact assesement (overall?). Och då gör man i princip i grunden en risk och sårbarhetsanalys, och är resultatet av den att det här kräver att vi justerar ???? eller ändrar inriktningsstrategi. Beroende på omfattning så lyfter man ju upp det och då kommer det att ta tid innan det kommer med. Men är det mindre lokala grejer så finns det ansvar för de lokala kontoren att göra anpassningar.
23	D - Hur förmedlar ni policys till de anställda?
24	SE - Det sker fortlöpande, dels vid en anställningsprocess, dels fortlöpande när det kommer ändringar. Det används i huvudsak av digitala forum eller på mycket sällan men även där på öppna forum där vi håller våra regionsmöten.
25	D - Skulle du säga att ni använder er utav quiz eller liknande för att kolla att de anställda har förstått de policys som existerar?
26	SE - Både ja och nej, quiz är påväg ut. Den pedagogiska effekten utav det vill jag inte lägga någon värdering i, jag gillade quiz men jag tror mer på det formatet som kallas för nano? utbildning, du får mindre block via din mail där du i lugn och ro kan sitta och svara i quiz visserligen form, men det blir mer, “har du tänkt på det här?”, det blir en informativ pedagogisk ledd utbildning inom ett par minuter.
27	D - Ja, alltså istället för att alla frågor ska komma på en och samma gång?
28	SE - Yes.
29	D - Vem tar ansvaret för om en anställd bryter mot någon policy på företaget?

30	SE - Vem tar ansvar.. Naturligtvis finns det ju, vad ska man säga, en intern rättsordning, där man följer de arbetsmiljölagarna som finns. Man har ju samtal, man har det även skriftligt, och sen får man tala om, men jag vill ändå påstå att, ju enklare du gör det desto mer får du att den anställde att ta ansvar och så vill jag påstå att det är på Sogeti. Man tar ansvar för sitt eget, och du rapporterar att "nu har jag gjort det här, nu hände det här, nu klickade jag på den här länken, och jag vet att det står i informationssäkerhetspolicyn att det inte skulle vara bra.". Men det ser jag mest som ett betyg på att vårt rättssystem intern är så pass högt i tak och öppet att man vill göra rätt.
31	D - Om vi nu säger att en anställd gör fel men att det är såpass är ett större fel så att ledningen måste blandas in. Kan detta på något sätt leda till att ledningen också måste ta ansvar för en sådan incident?
32	SE - Det ansvaret är ju ofullkomligt, alltså det är ju alltid personuppgiftsansvarige eller vad ska man säga, den informationssäkerhetsansvarig i slutändan som är ytterst ansvarig för att informationssäkerhetspolicyn följs. Så att även om det är en liten eller stor sak så kommer det ändå hamna på den ansvariges bord att ta ställning till att, är det här något som jag måste agera på, eller är det här någonting som jag får ta, kan bli rättsprocesser och så vidare. Men nej, det går upp ändå.
33	D - Hur ser du på så kallade top-down implementation av policys? Skulle du säga att det är något som du verkligen rekommenderar eller har du någon annan åsikt om detta?
34	SE - Jag skulle vilja säga såhär att oavsett vilken modell man vill använda sig utav så måste man börja med att implementera en modell som fungerar i den specifika företagsstrukturen eller så. För att det finns myndigheter eller annan verksamhet där det inte funkar, även om top-down är ett föredrag i många andra, så just här funkar det inte. Så, nulägesanalys innan man inför någon form utav metodik.
35	D - Skulle du säga att mänskliga aspekten är det största hotet?
36	SE - Ja, tveklöst. Jag har en bra bild som jag alltid brukar ta när man förklarar det. Tänk dig en boxningsring, och så är det en promoter i mitten som säger "in this corner, där står en server, and this corner is Dave.". Det är när människan kommer i kontakt med det som det blir problem.

37	D - Det var nog alla frågor, går det bra att använda ditt namn och företagsnamnet?
38	SE - Jajjemen.
39	A - Vill du även ha en kopia innan vi skickar in vår uppsats?
40	SE - Ja, med då regeringsrätten? att då om vi känner att, men här vill vi kanske inte skylta med vårt företagsnamn så får ni respektera det, men mitt namn går att använda. Då skriver man om det som säkerhetsexpert istället. Så absolut.
41	D - Ja men tack så mycket för att du ställde upp, det betyder mycket för oss.
42	SE - Ja men absolut, kopplat till vad vi pratade om GDPR så känner jag att det där hade jag nog lagt ett par timmar på. Mest för att förstå. Innan ni läser, vi pratar om 99 artiklar, med massa sub-paragrafer. Det ni måste göra innan ni sitter ner och skriver, så tror jag att jag hade satt mig ner och definierat frågan, varför ska jag läsa GDPR till det här. Jag vill ju veta vilka delar som kan ha en relevans. Vad är min bedömning här? Jag tror vi pratar personlig information..jag tror vi pratar om den här, okej, vad säger GDPR? Så läser ni de relevanta delarna. Läser ni nämligen bara GDPR så kan vi ses om ett år, så sitter ni fortfarande och läser den, och då fyller den inte syftet. Men att GDPR kommer till att ha en högst relevant inverkan på det ni skriver om är hundra procent. Tar man idag informationssäkerhet och kopplar den till personuppgiftslagen så finns det inga viteskrav men idag så pratar man om att ett företag kan få alltså fyra procent av sin bruttoårsinkomst max tio miljoner eller tjugo miljoner i euro. Så har man nu bara lite förståelse för denna marknad så förstår man ganska snabbt att det är ju företag som går i kull på det där, för att man inte hanterar informationssäkerhet och personuppgifter på korrekt sätt.
43	D - Precis.
44	SE - Så verkligen, ta med paragrafer till det här och koppla det till själva frågeställningen, begränsa det. Och här är ju det svåra, jag har själv suttit mycket med examensarbeten, ett antal och sagt att och så har man frågeställningen och

	sen börjar man justera den efter hand och sen så börjar man inse att det är lätt att flumma ut. Ni har min mailadress va?
45	D & A - Ja.
46	SE - Ställ gärna frågor fortlöpande också, om ni känner för det.
47	D & A - Absolut, tack så mycket.