LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Kommuners arbete med informationssäkerhet

med den mänskliga faktorn i fokus

Kandidatuppsats 15 hp, kurs SYSK02 i informationssystem

Författare: Nelly Karlsson Åhlén
Sofia Söderström

Handledare: Magnus Wärja

Examinatorer: Umberto Fiaccadori
Anders Svensson

Kommuners arbete med informationssäkerhet: med den mänskliga faktorn i fokus

Författare: Nelly Karlsson Åhlén och Sofia Söderström

Utgivare: Inst. för informatik, Ekonomihögskolan, Lund universitet

Dokumenttyp: Kandidatuppsats

Antal sidor: 74

Nyckelord: Policy och styrande dokument, utbildning och kompetensutbildning samt kontroll och uppföljning

Sammanfattning (Max. 200 ord):
Vi lever i en informationsekonomi där varje företag är beroende av informationstillgångar. Detta innebär att informationssäkerhet måste utvecklas för att skydda känsliga tillgångar. Ett av de största hoten för lyckad informationssäkerhet inom en organisation är de felaktiga åtgärder och beteende hos de anställda när de hanterar information. Myndigheten för Samhällsskydd och Beredskap genomförde år 2015 en enkätundersökning med syfte att ta reda på om kommuner arbetar systematiskt med informationssäkerhet. Denna undersökning ligger till grund för denna uppsats. De tre huvudområden som behandlas under uppsatsen är: policy och styrande dokument, utbildning och kompetensutveckling, samt kontroll och uppföljning.
Dessa kopplas till tre steg som Conner och Patterson (1982) pekar på att en anställd går genom för att anpassas till en organisatorisk förändring och inkluderar således den mänskliga faktorn. Syftet med uppsatsen är att undersöka hur kommuner arbetar med informationssäkerhet med de tre huvudområdena som perspektiv. Författarna har genom en kvalitativ undersökning intervjuat åtta kommuner i Sverige för att besvara forskningsfrågan *Hur arbetar kommuner med informationssäkerhet utifrån den mänskliga faktorn i fokus?* Det framgick att samtliga kommuner generellt sätt inte arbetar systematiskt med informationssäkerhet och inte inkluderar de anställda i det dagliga arbetet. Kommuner bör sträva efter att arbeta med informationssäkerhet kontinuerligt, med den mänskliga faktorn i fokus, för att uppnå så hög säkerhet som möjligt.

Innehåll

1 Introduktion 1
1.1 Bakgrund 1
1.1.1 En bild av kommuners informationssäkerhet 2015 2
1.2 Problemformulering 2
1.3 Forskningsfråga 3
1.4 Syfte 3
1.5 Avgränsningar 3
2 Litteraturgenomgång och teori 4
2.1 Myndigheter och kommuner 4
2.1.1 Myndigheten för samhällsskydd och beredskap 4
2.1.2 Kommuner och samhällsansvar 4
2.2 Vad är informationssäkerhet? 5
2.2.1 CIA-Triad 6
2.2.2 Den mänskliga faktorns påverkan på informationssäkerhet 7
2.3 Policy och styrande dokument 8
2.3.1 Information Security Policy 9
2.3.2 Vem ansvarar för utformandet av policyn? 10
2.4 Utbildning och kompetensutveckling 10
2.4.1 Information Security Awareness 11
2.4.2 ISA Program 11
2.4.3 Den mänskliga faktorn kopplat till ISA Program 12
2.4.4 Datorstödd informationssäkerhetsutbildning för anställda 13
2.4.5 NanoLearning via Junglemap 13
2.4.6 EU:s Dataskyddsförordning GDPR 14
2.5 Kontroll och uppföljning 14
2.6 Sammanfattning av teorin 15
2.6.1 Policy och styrande dokument 15
2.6.2 Utbildning och kompetensutveckling 15
2.6.3 Kontroll och uppföljning 15
2.7 Teoretiskt ramverk 16
3 Metod 18
3.1 Metodval 18
3.2 Urval 18
3.2.1 Geografisk plats 19
3.3 Utformning av intervjuguide 19

3.3.1 Teori kopplat till intervjuguide 20
3.3.2 Intervjuform 21
3.4 Undersökningskvalitét 22
3.4.1 Validitet 22
3.4.2 Reliabilitet 22
3.4.3 Etik 23
4 Resultat 24
4.1 Policy och styrande dokument 24
4.2 Utbildning och Kompetensutveckling 26
4.3 Kontroll och uppföljning 28
4.4 Övrigt 29
4.5 Sammanfattning av resultat 32
5 Analys och diskussion 33
5.1 Policy och styrande dokument 33
5.2 Utbildning och kompetensutveckling 35
5.3 Kontroll och uppföljning 36
5.4 Övrigt 37
6 Slutsats 39
6.1 Framtida forskningsmöjligheter 40
7. Bilagor 41
7.1 Intervjuguide 41
7.2.1 Transkribering av intervju: Kommun 1 (K1)
7.2.2 .2 Transkribering av intervju: Kommun 2 (K2)
7.2.3 Transkribering av intervju: Kommun 3 (K3)
7.2.4 Transkribering av intervju: Kommun 4 (K4)
7.2.5 Transkribering av intervju: Kommun 5 (K5)
7.2.6 Transkribering av intervju: Kommun 6 (K6)
7.2.7 Transkribering av intervju: Kommun 7 (K7)
7.2.8 Transkribering av intervju: Kommun 8 (K8)
7.3 Initialt e-postmeddelande
Referenser

Figurer

Figur 1: Illustration av Andress (2011) CIA-Triad 6

Figur 2: Teoretiskt ramverk anpassat från Conner och Pattersons (1982) teori angående en anställds anpassning vid en organisationsförändring 16

Tabeller

Tabell 1. Kommuner och intervjuobjekt 19

Tabell 2. Teori kopplat till intervjuguide 21

Tabell 3. Sammanfattning av resultat 32

Förkortningar

MSB: Myndigheten för Samhällsskydd och Beredskap
SKL: Sveriges Kommuner och Landsting

ISP: Information Security Policy
ISA: Information Security Awareness
ISA Program: Information Security Awareness Program
GDPR: General Data Protection Regulation

1 Introduktion

I detta kapitel beskrivs bakgrunden till uppsatsens ämne mer specifikt och problemområdet introduceras. Detta smalnas därefter ner till uppsatsens frågeställning samt syftet att besvara denna fråga. Slutligen beskrivs uppsatsens avgränsningar som gjorts runt frågeställningen.

1.1 Bakgrund

Vi lever i en informationsekonomi där varje företag är beroende av informationstillgångar. Detta i form av information, data, hårdvara, mjukvara samt network för att bara nämna några. Som ett resultat av denna förändring och framsteg inom informationsteknologimarknaden måste även informationssäkerheten utvecklas (Martins & Elofe, 2002). Betydelsen av informationssäkerhet har ökat som bevittnat av det ökande antalet IS-säkerhetshändelserna som organisationer stött på under de senaste åren. För att klara av ökandet av hot mot informationssäkerheten, så har olika säkerhetsåtgärder föreslagits. Allt från tekniska skyddsåtgärder till olika informationshanteringsstandarder, säkra systemmetoder och informationssäkerhetspolicy (Pahnila, Siponen & Mahmood, 2007).

Ett av de största hoten för en lyckad informationssäkerhet inom en organisation är de felaktiga åtgärder och beteende hos de anställda när de hanterar information (Thomson, von Solms & Louw, 2006). Värdet av att ha informationssäkerhetsutbildningar, träning samt medvetenhet hos de anställda förbises ofta inom organisationer (Amankwa, Loock & Kritzinger, 2014). De anställda följer emellanåt inte de korrekta säkerhetsprocesserna och teknikerna för säkerheten, vilket till följd kan sätta organisationens tillgångar och affärer i fara. En effektiv informationssäkerhet kräver därför inte bara att användarna är medvetna om vilka åtgärder som krävs, utan att de även följer dessa åtgärder och riktlinjer (Pahnila et al. 2007).

Det kan finnas standardiserade säkerhetskontroller såsom brandväggar, men om företagsstyrelsen inte hanterar dessa effektivt eller om användarna inte vet hur de på ett korrekt sätt använder sig utav dessa kontroller, så blir den mänskliga faktorn en vital påverkan och inte enbart teknologin. Varje dag integrerar användare med datorer och företagets resurser för olika anledningar. Denna interaktion representerar den svagaste länken inom informationssäkerhet (Martins & Elofe, 2002). Bulgurcu, Cavusoglu och Benbasat (2010) menar däremot att även om de anställda ofta anses vara den svagaste länken i informationssäkerhet, kan de även vara den största tillgången gällande att minska riskerna relaterade till ämnet. Anställda i organisationer, oavsett storlek och inriktning, måste vara medvetna om informationssäkerhet för att ha möjlighet att ta välformade val gällande säkerheten för att kunna prestera i deras dagliga arbete (Amankwa et al. 2014). Detta dock under förutsättningarna att rätt utbildning sker, samt inställningen hos de anställda.

1.1.1 En bild av kommuners informationssäkerhet 2015

På uppdrag av regeringen genomfördes år 2015 en enkätundersökning vid namn *En bild av kommuners informationssäkerhet 2015*. Denna enkätundersökning genomfördes av Myndigheten för Samhällsskydd och Beredskap (MSB), med samverkan av Sveriges Kommuner och Landsting (SKL). Enkätundersökningen skickades ut till Sveriges 290 kommuner varav 228 kommuner besvarade hela enkäten. Syftet med enkäten var att undersöka hur kommuner arbetar med informationssäkerhet, med utgångspunkt i hur kommunerna själva uppfattar att de arbetar med informationssäkerhet. Resultatet finns sammanställt i en rapport där grafiska diagram, procentsatser och tabeller används för att beskriva situationen som sådan. Utifrån enkätresultatet gjordes ett urval på 11 olika delar av systematiskt informationssäkerhetsarbete som analyseras i rapporten, vilket inkluderade: 1) Policy och styrande dokument, 2) Kontroll och uppföljning, 3) Ansvar och roller, 4) Leda och samordna informationssäkerhetsarbetet, 5) Informationsklassning, 6) Riskanalys, 7) Incidenthantering- och kontinuitetsplanering, 8) Teknisk infrastruktur, 9) Upphandling, 10) Samverkan, samt 11) Utbildning och kompetensutveckling (MSB, 2015).

1.2 Problemformulering

För att organisationer ska öka kvaliteten och förtroendet för sin verksamhet är en vital del det systematiska arbetet gällande informationssäkerhet (Kalmelid, 2015). Att uppnå en god informationssäkerhet är dock inte alltid enkelt och kräver mycket arbete på alla olika plan inom organisationen. Ett av de mest vitala problemen gällande informationssäkerhet är den mänskliga faktorn. Alla säkerhetssystem, oavsett hur välformade och genomförda de är, måste lita på användarna (Gonzalez & Sawicka, 2002). Ett av de största hoten gällande informationssäkerhet menar Thomson et al. (2006) är de felaktiga åtgärder och beteende hos de anställda när de hanterar information.

Conner och Patterson (1982) pekar på tre steg en anställd går genom med koppling till en organisatorisk förändring. Författarna menar att de anställda måste genomgå en process på tre steg för att vara medvetna om arbetet gällande informationssäkerhet och på så sätt eliminera den mänskliga faktorn som ett hot mot organisationen. Dessa tre steg är preparation, awareness och commitment. Layton (2005) menar att dessa tre steg kommer bidra att organisationer flyttar sitt fokus från att se informationssäkerhet som ett tekniskt problem, till att se det ut ett mänskligt perspektiv.

I MSB:s enkätundersökning *En bild av kommuners informationssäkerhet 2015* framgår det tydligt tre områden där arbetet bör förbättras. 67 av 242 kommuner har inte en informationssäkerhetspolicy beslutad av ledningen, 136 av 236 erbjuder inte utbildning och kompetensutveckling för de anställda, och 141 av 241 kommuner anger att de inte kontrollerar efterlevnaden gällande informationssäkerhet (MSB, 2015). Dessa tre områden går direkt att koppla till den mänskliga faktorn. Conner och Pattersons (1982) tre steg kopplas således till ett teoretiskt ramverk som presenteras senare i uppsatsen som inkluderar tre huvudområden: policy & styrande dokument, utbildning & kompetensutveckling samt kontroll & uppföljning. Alla dessa tre delarna är kopplade till den mänskliga faktorn och genom att flytta perspektivet från de tekniska till det mänskliga, menar Layton (2005) att färre säkerhetsincidenter kommer inträffa. Med ovanstående i

beaktning ämnar uppsatsen att undersöka dessa tre delar av enkäten, då det finns en tydlig röd tråd mellan områdena, samt en koppling till den mänskliga faktorn gällande informationssäkerhet. Då MSB:s undersökning enbart förser läsaren med statistiskt underlag, besvarar denna undersökning frågan "varför" genom en kvalitativ undersökning. Detta leder vidare till forskningsfrågan nedanför.

1.3 Forskningsfråga

Hur arbetar kommuner med informationssäkerhet utifrån den mänskliga faktorn i fokus?

1.4 Syfte

Syftet med uppsatsen är att undersöka hur kommuner arbetar med informationssäkerhet. Med hur avses tre perspektiv: policy & styrande dokument, utbildning & kompetensutveckling samt kontroll & uppföljning med den mänskliga faktorn i fokus.

1.5 Avgränsningar

Uppsatsen avgränsas till informationssäkerhet med den mänskliga faktorn som huvudfokus. Således behandlas människans interaktion med teknologin och informationssystem och hur denna interaktion kan förbättras genom användandet av: *policy och styrdokument*, *utbildning och kompetensutveckling* samt *kontroll och uppföljning*.

2 Litteraturgenomgång och teori

I detta kapitel presenteras befintlig litteratur med relevans inom området för uppsatsen. Inledningsvis förklaras fenomenen som myndigheter och kommuner för att sedan kopplas till varför dessa organ är beroende av informationssäkerhet. Vidare förklaras termen informationssäkerhet och dess beståndsdelar. Detta för att ge läsaren en strukturerad bild av arbetet. Slutligen presenteras de tre faktorerna som identifierats under problemområdet: policy och styrande dokument, utbildning och kompetensutveckling, samt kontroll och uppföljning. Till sist sammanfattas dessa delar i ett teoretiskt ramverk.

2.1 Myndigheter och kommuner

2.1.1 Myndigheten för samhällsskydd och beredskap

Myndigheten för samhällsskydd och beredskap (MSB) är en statlig myndighet som syftar till att hjälpa samhället med att förebygga och hantera diverse olyckor och kriser. MSB ansvarar för frågor gällande civilskydd, allmän säkerhet, nödhantering samt civilförsvar. Detta under förutsättning att ingen annan myndighet har ansvar över något av områdena. Arbetet sker med kommuner, landsting, myndigheter, men även andra organisationer. Vid en omfattande olycka eller kris ger MSB stöd till de ansvariga parterna för att lösa händelsen i fråga, men även för att lära dem arbeta förebyggande i framtiden med liknande situationer (MSB, 2017).

MSB arbetar genom kunskapsökningar, support, utbildning, övningar, reglering och tillsyn. Detta sker i nära samarbete med kommuner, landsting, andra myndigheter, den privata sektorn samt olika organisationer i Sverige. Detta görs för att uppnå bättre säkerhet på alla nivåer i samhället, både lokalt men även globalt. Anvisningarna som anger MSB:s ansvar och uppgifter kommer från den svenska regeringen. Regeringen styr MSB genom en uppsättning av instruktioner samt ett årligt anslag. Anslagen som regeringen tillhandahåller MSB specificerar målen samt rapporteringskraven, liksom de resurser som krävs för MSB-administrationen samt diverse aktiviteter (MSB, 2017).

2.1.2 Kommuner och samhällsansvar

I Sverige finns det 290 kommuner och 20 landsting (SKL, 2017a). Kommunerna i Sverige har ett av de mest komplexa uppdragen i samhället och omfattar allt från den dagliga omsorgen av äldre till att säkerställa att känslig infrastruktur fungerar (Goede, 2017). Kommunerna styrs av politiker som valts direkt av medborgarna. Detta innebär att medborgarna har stora möjligheter att både påverka och kontrollera hur kommuner utför sina uppdrag (SKL, 2017b). Kommunerna har det yttersta ansvaret gällande vuxna, ungdomar och barn som vistas i kommunen, samt att de får det stöd och hjälp som de behöver (SKL, 2017c). Kommunerna har även ansvar för en stor del av samhällsservicen. Detta innebär att några av kommunernas främsta uppgifter inkluderar förskola, skola, socialtjänst och äldreomsorg. Kommunerna är enligt lag skyldiga att bedriva vissa verksamheter. Andra verksamheter är frivilliga och beslutas av lokalpolitikerna (SKL, 2017a).

Kommunerna i Sverige styrs genom direktvalda politiska församlingar, så kallade kommunfullmäktige. Dessutom finns det politiska uppdrag inom kommunstyrelsen, i olika nämnder och utskott. Det finns drygt 38 000 förtroendevalda i landets 290 kommuner, varav merparten av dessa är fritidspolitiker. Detta innebär att dessa politiker sköter sina uppdrag vid sidan av annat arbete eller studier. Vart fjärde år får medborgarna rösta och på så sätt välja politiker till kommunfullmäktige, detta val sker samtidigt som riksdagsvalet. Det kommunala självstyret är en princip som är inskriven i regeringsformen, en av grundlagarna (SKL, 2017b). Detta innebär att kommuner och landsting har en självständig och fri bestämmanderätt. Staten reglerar delvis dessa ramar genom olika lagstiftningar, samt att de har övergripande ansvar för kommunerna. Detta innebär att de har ansvar att verksamheten utvecklas på ett sätt som är förenligt med en samhällsekonomisk balans (Regeringskansliet, 2017).

Likt andra organisationer är kommuner, landsting och regioner beroende av information och IT-stöd för att kunna bedriva sin verksamhet. I takt med satsningar på digitalisering inom den offentliga sektorn ökar även verksamhetens beroende av informationssäkerhet. Detta för att inte tappa förtroendet hos de boende på kommunen eller deras tillit när kommunen behandlar känslig information (SKL, 2017d). Sveriges kommuner hanterar betydelsefull information och är därför en kritisk del i samhällets informationssäkerhet. Arbetet gällande informationssäkerhet är vitalt inom kommuner för att säkerställa en hög nivå på säkerheten inom alla olika förvaltningar och bolag, det är även viktigt att denna säkerhet bedrivs metodiskt och långsiktigt (MSB, 2012).

2.2 Vad är informationssäkerhet?

Enligt Whitman och Mattord (2011) innebär säkerhet att ens tillgångar är skyddade och hot samt risker är eliminerade. I allmänhet kan säkerhet ses som ett tillstånd av trygghet, att vara fri från eventuella risker och således vara skyddade från motståndare vars handlingar är att med avsikt göra skada (Whitman & Mattord, 2011). Genom ett systematiskt arbete med informationssäkerhet kan organisationer öka kvaliteten och förtroendet för sin verksamhet (Kalmelid, 2015). Behovet av informationssäkerhet utvecklas dagligen och har tydligt gått från att ta itu med mindre och ofarligare säkerhetsbrott till att hantera de hot och risker som har stor påverkan på en organisations tillväxt samt säkerhet (Dlamini, Eloff & Eloff, 2009). Whitman och Mattord (2011) definierar informationssäkerhet som skydd av information och dess kritiska element, inklusive system och hårdvara som använder, lagrar och överför information.

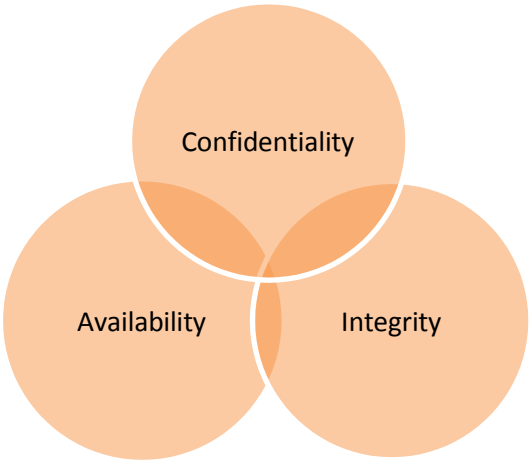
De organisationer som är starkt beroende av informationssystem är även starkt beroende av informationssäkerhet (Bulgurcu et al. 2010). Information på kommuner är värdefull och behöver skyddas efter behovs. Ett bra informationsarbete ger verksamheten förtroende och borgar för effektiv informationshantering (Kalmelid, 2015). Olika system inom organisationer kräver att riskerna som medförs hanteras så organisationen inte tar skada av eventuella risker och hot. Görs inte detta på ett ordentligt sätt kan det leda till allvarliga konsekvenser (Bulgurcu et al. 2010). Informationssäkerhet finns på organisationer för att skydda konfidentialitet, integritet och tillgänglighet av informationstillgångar (Whitman & Mattord, 2011). Information måste skyddas så att den alltid finns tillgänglig för rätt personer, samt att den är korrekt och således

inte manipulerad av obehöriga. Detta innebär att informationen måste skyddas så obehöriga inte kan få tillgång till den (Kalmelid, 2017). För att uppnå detta krävs det tillämpning av informationssäkerhetspolicys (ISP), utbildningar, medvetenhet hos de anställda samt användandet av teknologi (Whitman & Mattord, 2011). Kalmelid (2015) menar att informationssäkerhet handlar om att skapa en fungerande långsiktig process för att ge en organisations känsliga information det skydd den förtjänar.

Det är dock inte alltid enkelt för en organisation att uppnå den mest ultimata informationssäkerheten. Whitman och Mattord (2011) menar att även med den bästa planeringen och implementeringen är det omöjligt att få till en perfekt informationssäkerhet. Säkerhet kan inte vara absolut, utan är en process och inte ett mål en organisation kan uppnå. Genomförandet av informationssäkerhet inom en organisation måste börja någonstans och kan inte ske över en natt. Att säkra en organisations informationstillgångar är en process som kräver samordning, tid samt tålamod. Kalmelid (2015) skriver även att skyddet givetvis måste vara anpassat efter organisationens behov så det varken blir allt för klent, krångligt eller dyrt. Detta bör dock inte försummas med tanke på konsekvenserna som en bristande säkerhet kan leda till. God informationssäkerhet bör vara en självklarhet för alla organisationer. Som tidigare nämnt menar Whitman & Mattord (2011) att alla organisationer som hanterar information bör skydda denna genom konfidentialitet, integritet samt tillgänglighet, även förkortat till CIA-triad.

2.2.1 CIA-Triad

De tre grundläggande principerna för informationssäkerhet är: confidentiality, integrity och availability som fritt översatt blir konfidentialitet, integritet och tillgänglighet - även känd som CIA-triaden (Agarwal & Agarwal, 2011). Dessa tre element är sammankopplade för att förstå innebörden av informationssäkerhet. All sorts information kräver skydd, precis som alla tillgångar i organisationen. Detta menar Wylder (2003) är en grundläggande inställning alla inom organisationen måste ha för att förstå CIA-triaden och dess innebörd.



Figur 1, Illustration av Andress (2011) CIA-Triad

2.2.1.1 Konfidentialitet

Den första komponenten av de grundläggande principerna är konfidentialitet, även känt som sekretess. Konfidentialitet hänvisar till förmågan att skydda data från dem som inte är behöriga (Andress, 2011). Konfidentialitet syftar på att förebygga obehörig användning eller utlämnande av information (Wylder, 2003). Konfidentialitet kan genomföras på många nivåer av en process och kan äventyras av förlust av en dator bestående av vital och känslig data, om en person tittar över axeln när någon skriver sitt lösenord eller att ett mejl skickas till fel person (Andress, 2011). Konfidentialitet garanteras av nätverksäkerhetprotokoller, nätverksautentiseringstjänster, kommunikationssäkerhet samt intrångsdetektering (Agarwal & Agarwal, 2011).

2.2.1.2 Integritet

Den andra komponenten i CIA-triaden är integritet. Integritet hänvisar till att informationen ska vara korrekt, komplett och inte modifierad av obehöriga användare eller utomstående processer (Wylder, 2003). Med detta menas garantin att det meddelande som skickas är det samma som det mottagna meddelandet, vilket innebär att innehållet inte har altererats från sändaren till mottagare (Agarwal & Agarwal, 2011). Integritet avser förmågan att förhindra att en organisations data ändras på ett otillåtet eller oönskat sätt. För att upprätthålla god integritet inom organisationer krävs det inte enbart medel för att förhindra obehöriga ändringar i data, utan även möjligheten till att återkalla ändringar (Andress, 2011). Integritet garanteras av brandväggstjänster, kommunikationssäkerhet samt intrångsdetektering (Agarwal & Agarwal, 2011).

2.2.1.3 Tillgänglighet

Den tredje och sista komponenten är tillgänglighet. Tillgänglighet avser möjligheten att få tillgång till data och information när det behövs (Andress, 2011). Detta innebär även att tillgängligheten för konsumenten ska finnas i ett tidigt skede, fungera oavbrutet samt vara oberoende av användarens plats. Detta innebär att molninfrastruktur, säkerhetskontroller och nätverksanslutningar ska fungera korrekt. Tillgänglighet säkerställs genom tolerans, autentisering samt nätverkssäkerhet (Agarwal & Agarwal, 2011).

Alla tre delar i CIA-triaden går att direkt koppla till den mänskliga faktorn. De tre faktorer sammanfattar de aspekter som inkluderar att information ska skyddas från obehöriga, att informationen ska var korrekt samt tillgänglig för behöriga. Alla dessa faktorer kan äventyras på grund av den mänskliga faktorn, både genom misstag eller med uppsåt att skada. Som tidigare nämnt menar Agarwal och Agarwal (2011) att dessa tre element är sammankopplade för att organisationer ska förstå vikten av informationssäkerhet. Är en organisation således införstådda i detta och utbildar de anställda kommer risken för skadliga handlingar utförda av anställda minska.

2.2.2 Den mänskliga faktorns påverkan på informationssäkerhet

Alla säkerhetssystem, oavsett hur välformade och genomförda de är, måste lita på användarna. Det faktum att den mänskliga faktorn spelar en viktig roll i flertalet olyckor inom organisationer gällande information är ett oroande kännetecken. En organisation kan genomföra lämpliga tek-

niska lösningar, men det är fortfarande vanligt att misslyckas med hanteringen av den mänskliga faktorn. Det är därför viktigt att organisationer förstår innebörden att informationssäkerhet både inkluderar teknologi samt människor (Gonzalez & Sawicka, 2002). De teknologiska framstegen blir allt fler, samt mer imponerande, men det blir även mer tydligt att den mänskliga faktorn är en svag länk inom informationssäkerhet (Gonzalez & Sawicka, 2002). Mitnick (2000) menar att den mänskliga faktorn är ett av de största säkerhetshoten mot en organisation. Pengar som spenderas på mjukvaru- och hårdvarusäkerhet kan anses onödigt om en anställd exempelvis tappar bort en hårddisk, genomför ändringar utan tillåtelse eller om denne öppnar länkar som innehåller virus Mitnick (2000). En organisation behöver tydliga och väldefinierade säkerhetspolicys och strategier för att kunna minimera risken som är kopplad till den mänskliga faktorn. En anställd med felaktig behörighet kan av misstag radera eller modifiera vital information tillhörande organisationen (Gollmann, 2011).

Däremot menar Bulgurcu et al. (2010) att även om de anställda ofta anses vara den svagaste länken i informationssäkerhet, kan de även vara den största tillgången gällande att minska riskerna relaterade till ämnet. Detta för att de anställda är de som måste foga sig efter dessa policys samt regler, och därmed fyller de anställda en nyckelfunktion gällande informationssäkerheten. Organisationer som anser att teknik kan lösa alla dess problem, förstår enligt Gonzales och Sawicka (2002) varken problemet eller tekniken. Organisationer måste således se till att de drar nytta av sin mänskliga kapacitet, istället för att göra motsatsen (Bulgurcu et al. 2010).

För att lyckas dra nytta av den mänskliga kapacitet menar Conner och Patterson (1982), som tidigare nämnt, att en anställd måste gå genom olika steg för att slutligen rätta sig efter en organisatorisk förändring. Dessa steg kan sammanfattas till tre steg: preparation, awareness och commitment. Dessa steg fördjupas senare i mer detaljerade steg. *Preparation* kan jämföras med policy och styrande dokument, *awareness* med utbildning och kompetensutveckling och *commitment* med kontroll och uppföljning. Layton (2005) menar att dessa steg går att sammankoppla med Information Security Awareness (ISA) då huvudsyftet är att förändra slutanvändarnas beteende till mer självgående och förstående. Organisationer bör enligt författaren flytta sitt fokus från att se informationssäkerhet som ett tekniskt problem, till att se det ur ett mänskligt perspektiv. Genom detta hävdar Layton (2005) att färre säkerhetsincidenter skulle inträffa. För att lyckas flytta perspektivet till den mänskliga faktorn och dra nytta av den mänskliga kapaciteten måste de anställda vara införstådda med organisationens regler och policyn gällande informationssäkerhet. På så sätt blir de medvetna om arbetet som behövs utföras för att uppnå en så hög säkerhet som möjligt.

2.3 Policy och styrande dokument

En policy är grundprinciper för ett företags eller en organisations handlande (NE, 2017). I allmänhet definieras en policy som en plan eller en åtgärd som är avsedd att påverka och bestämma beslut, handlingar och andra frågor inom bland annat politiska partier, eller en organisation. En policy representerar det formella uttalandet av en organisations ledningsgrupp (Whitman & Mattord, 2008). En policy definierar ett beteende som antingen organisationen förväntar sig av

de anställda eller vad som är strikt förbjudet. En väl utformad policy definierar vem som förväntas att göra vad, detta innebär att en policy ställer kvar på en organisations anställda genom att specificera vad de kan eller inte är tillåtna att göra (LeVeque, 2006).

En policy är i de flesta fall svår att genomföra och vissa riktlinjer bör följas för att bidra till korrekt formulering av innehållet. En policy måste bidra till organisationens framgång, ansvarsfördelning inom ledningen måste tydliggöras samt att slutanvändarna måste vara involverade (Whitman & Mattord, 2008). Utöver det specifika innehåll en policy bör innehålla måste den även skräddarsys till organisationens specifika behov. LeVeque (2006) tar även upp att en organisation kan ha flera policys, detta beroende på olika organisationsenheter samt tekniska och administrativa sammanhang. För olika ändamål är olika policys tillämpliga. När det pratas om ISP kan det finnas en policy för slutanvändaren som tydligt beskriver befogade säkerhetsrutiner för dagligt systemanvändande. Vidare kan det finnas en mer tekniskt inriktad policy samt en policy som agerar på ledningsnivå där ledningens ansvar gällande informationssäkerhet definieras.

2.3.1 Information Security Policy

Det finns olika kontroller som bör genomföras inom en organisation för att säkerställa en effektiv informationssäkerhet. Dessa kontroller och åtgärder sträcker sig från tekniska lösningar och avtalsbestämmelser till den organisatoriska medvetenheten angående risker, hot och sårbarhet. Höne och Eloff (2002) skriver att en av de viktigaste kontrollerna när det kommer till informationssäkerhet är skapandet av en ISP. Däremot menar de att det finns svårigheter med att utveckla detta policydokument, då det inte är lätt att identifiera exakt vad som skall inkluderas.

En organisations ISP fungerar som ett styrdokument som ska styra riktningen inom organisationen mot en god informationssäkerhet (Höne & Eloff, 2002). Organisationens syfte vid skapandet av en ISP är att förse de anställda med riktlinjer som syftar till att säkerställa informationssäkerhet (Whitman, Townsend & Aalberts, 2001). Dokumentet bör diktera de anställdas beteende och fastställa vad som förväntas av dem, vilket inom sin tid blir en del av det dagliga arbetet (Martins & Elofe, 2002). Dokumentet bör även förklara behovet organisationen har av informationssäkerhet samt dess koncept för alla anställda. Detta innebär även att organisationens affärsmål bör finnas med samt reflektera ledningens villighet att driva organisationen på ett kontrollerat och säkert sätt (Höne & Eloff, 2002).

Gollmann (2011) menar att en ISP fungerar som en redogörelse för de olika säkerhetsmålen hos en organisation. Policyn måste inkludera vad som måste skyddas, men även hur detta skall göras i praktiken. Att skapa dessa riktlinjer och policys är enligt Bulgurcu et al (2010) en god början, men inte tillräcklig för att de anställda ska samtycka och tillämpa dessa policys. Vidare belyser författarna att nyckeln till detta samtycke är att identifiera och förstå vilka faktorer som motiverar de anställda att tillämpa policys. De anställda måste både vara medvetna, utbildade och tränade inom området (Martins & Elofe, 2002).

Ett vanligt problem är att de flesta ISP misslyckas med att påverka slutanvändarna. Anställda är ofta ignoranta gentemot sin organisations policy, samt att de inte förstår innehållet till fullo. Antingen är det för långt eller för tekniskt, och användarna ser inte relationen och sambandet mellan deras dagliga arbete och innehållet i organisationens ISP. Detta resulterar till att organisationens ISP blir ineffektiv och inte uppnår dess mål (Höne & Eloff, 2002). För att undvika detta beteende hos de anställda menar Höne och Eloff (2002) vidare att en effektiv ISP hjälper användarna förstå vad som är acceptabelt och vilket ansvar de har mot informationssäkerhet. Detta innebär att en effektiv ISP måste inkludera användarnas behov av korrekt och tillförlitlig information, samt organisationens behov av att uppnå deras strategiska mål. Om detta görs på ett korrekt sätt bör användarna förstå att informationssäkerhet inte är negativt och ansträngande, utan existerar för att rätt information ska vara tillgänglig för de anställda vid rätt tillfälle, och detta för att ta välgrundade affärsbeslut för att uppnå vinst och framgång.

För att undvika händelser likt vad Höne och Eloff (2002) beskriver, menar LeVeque (2006) att olika säkerhetspolicys bör utformas och tillämpas beroende på olika organisatoriska faktorer såsom storlek, organisationskultur och hierarki. Specifika policys skall således tillämpas på olika delar av organisationen. Höne och Eloff (2002) belyser även att det mest vitala när det kommer till att utforma en policy är att denna är skräddarsydd efter organisationskulturen. Riskerna för att slutanvändarna ignorerar policyns existens minskar och därmed arbetar de efter uppsatta riktlinjer. För att nå en så effektiv ISP som möjligt bör den vara ett förståeligt, meningsfullt och praktiskt dokument som adresserar användarna direkt och övertygar dem att använda informationsresurser på ett säkert sätt.

2.3.2 Vem ansvarar för utformandet av policyn?

Det är vitalt att rätt person eller avdelning utformar organisationens ISP. Många organisationer låter sina IT-avdelningar utforma den, vilket ger policyn i fråga en mycket teknisk synvinkel. Detta resulterar i policys som är svåra att förstå för den otekniske användaren. Därför är det vitalt att förstå vikten av att inkludera psykologiska aspekter vid utformandet av policyn, då detta skall gynna integreringen av policyn i organisationen (Layton, 2005). Oavsett vem som utformar policyn är det, som tidigare nämnt, viktigt att inkludera slutanvändarna (Höne & Eloff, 2002). Detta sker inte enbart genom att skapa en policy som inkluderar dem, utan även att organisationen erbjuder utbildning för att öka medvetenheten hos de anställda, och på så sätt öka deras kunskap gällande dess ISP och vikten av informationssäkerhet.

2.4 Utbildning och kompetensutveckling

Utbildning och medvetenhet gällande informationssäkerhet är en av de mest kritiska aspekterna när det kommer till att skydda känslig information inom organisationer (Amankwa, Lock & Kritzinger, 2015). För att lyckas med detta krävs både utbildning och träning inom organisationen. Detta innebär att inställningen gentemot informationssäkerhet är viktig för alla anställda. (Martins & Elofe, 2002).

2.4.1 Information Security Awareness

I varje organisation finns det en informationssäkerhetskultur som framgår och skapas utifrån hur de anställda ställer sig till företagets information och dess säkerhet. Ett av de största hoten för en lyckad informationssäkerhet inom en organisation är de felaktiga beslut och beteende hos de anställda när de hanterar information (Thomson et al. 2006). De processer de anställda arbetar med i deras dagliga arbete kan representera den svagaste länken inom informationssäkerhet (Martins & Elofe, 2002). För att kunna skyddas mot detta är det viktigt att de anställda blir utbildade och integrerade i informationssäkerheten och använder denna kunskap i deras vardagliga arbete (Thomson et al. 2006).

Termen Information Security Awareness (ISA) används för att referera till stadiet där användarna i en organisation både är medvetna och fullt engagerade i säkerhetsarbetet. ISA är av avgörande betydelse då informationssäkerhetstekniker och processer kan misskötas, misstolkas eller ignoreras av slutanvändarna, och således förlora dess riktiga värde och användbarhet. Ökad medvetenhet ska minimera användarrelaterade misstag, upphäva dessa i teorin och maximera effekten hos säkerhetstekniker och processer ur ett användarperspektiv (Siponen, 2000). Medvetenhet innebär även utbildning och träning. Det är viktigt att inställningen gentemot informationssäkerhet ska vara en del av organisationens kultur (Martins & Elofe, 2002). Det är viktigt att utbilda användarna och deras disciplin gällande informationssäkerhet. Deras beteende måste modifieras till den grad att de kan arbeta med deras dagliga arbetsuppgifter och aktiviteter med ett säkerhetstänk. Det är viktigt att detta beteende fungerar omedvetet under hela arbetsprocessen, detta innebär att de anställda alltid ska tänka ur ett säkerhetsperspektiv oavsett vilka uppgifter de utför (Thomson & von Solms, 1998).

Att införa informationssäkerhet som en del av en organisations kultur är ingen enkel uppgift, och kan ta upp mot flera år. Utmaningar såsom ISP, samt ISA måste adresseras av alla organisationer som vill utveckla en kultur som främjar skyddandet av deras informationstillgångar. Kulturen har att göra med hur saker och ting blir gjorda inom organisationen samt beteendet och inställningen hos de anställda. Detta innebär att även organisationens beteende har en påverkan på informationssäkerheten inom företaget (Martins & Elofe, 2002). För att förenkla arbetet gällande informationssäkerhet involvera detta i organisationen krävs det utbildningar för att öka medvetandet och kunskapen.

2.4.2 ISA Program

På grund av det intensifierade behovet av förbättrad informationssäkerhet har många organisationer etablerat ISA program. Idag ses användaren i de flesta fall som ett hot mot säkerheten, istället för att se användaren som en tillgång (Schlienger & Teufel, 2002). ISA program definieras till vilken grad varje anställd förstår innebörden av informationssäkerhet, vilken nivå på säkerheten som är passande för just deras organisation, deras individuella ansvar gentemot säkerheten samt att deras arbete alltid strävar mot detta (Kruger & Kearney, 2006). Enligt Layton (2005) kan det vara svårt att inkludera ett ISA program i en organisation, eftersom alla organisationer har olika affärsstrategier. För vissa organisationer handlar det endast om att efterfölja

informationssäkerhetslagar och regleringar, vilket gör det vitalt för organisationen att ha medvetna anställda. Layton (2005) menar således att denna medvetenhet främst handlar om att de anställda ska kunna efterfölja befintliga lagar, policys och regleringar. Vissa organisationer använder ISA program för att vinna konkurrensfördelar, medan andra nyttjar det för att kontrollera oförutsägbara kostnader och utgifter. Det är vitalt att samtliga anställda som hanterar information förstår sina roller och ansvarsområde i samband med sina arbetsuppgifter. Det är därför viktigt att de förstår organisationens informationssäkerhetspolicy och rutiner, samt ha tillräckligt med kunskap gällande de olika kontroller som krävs för att skydda organisationens resurser (Dewey & Shaffer, 2016).

ISA program används även för att utbilda de anställda gällande informationssäkerhetsfrågor, samtidigt som det ständigt påminner användarna om pågående problem samt nya problem som kan ha blivit relevanta. Målet med ett ISA program är att ändra de anställdas idéer och beteende gentemot informationssäkerhet, därför är det viktigt att programmet är strukturerat på så sätt att användarnas beteende och attityd modifieras så att deras handlingar är säkerhetsmedvetna (Thomson & von Solms, 1998). Detta för att försäkra sig om att de anställda är informerade och medvetna om de olika säkerhetsriskerna, och på så sätt skydda sig själva och företagets resurser (Kruger & Kearney, 2006). Skapandet och användandet av ett ISA program är att minimera slutanvändarnas fel gällande säkerhetsriktlinjer med ett systematiskt tillvägagångssätt (Siponen, 2000).

Vidare bör utbildning främja informationsäkerhetstänket och inkludera användarnas insikt i vitala frågor. Detta innebär att höja medvetenheten angående varför de anställda bör inkludera informationssäkerhet i deras dagliga arbete, och på så sätt även öka motivationen. Träning av de anställda bör inkludera att öka deras kompetent och förmåga kring ämnet gällande det dagliga arbetet och lära dem hur de bör arbeta för att uppnå hög säkerhet (Siponen, 2000). Detta innebär även att de anställdas handlingar och beteende är särskilt viktiga eftersom nästan alla lösningar gällande informationssäkerhet litar på den mänskliga faktorn (Thomson et al. 2006). Utbildningen bör inte enbart inkludera hur de anställda ska hantera känsliga resurser utan även tillse de anställda med färdigheter och kompetens för att försäkra sig om organisationens hållbarhet (Amankwa et al. 2015). Detta för att eliminera den mänskliga faktorn som ett hot mot organisationen.

2.4.3 Den mänskliga faktorn kopplat till ISA Program

I enlighet med Thomson et al. (2006) menar Layton (2005) att den viktigaste faktorn i ett ISA program är den mänskliga faktorn. Främst handlar det om deras attityd, beteende, handlingar, men även deras förmåga att skilja rätt från fel. Teknologi kan på egen hand inte lösa de utmaningar som organisationer möter som är kopplade till informationssäkerhet och att den mänskliga faktorn är d en sista pusselbiten för att effektivisera ISA program. Dessvärre kan människans beteende inte förutsägas till fullo, utan ledningen måste försöka förstå vilka steg en anställd går genom innan denne blir gynnsamt engagerad utan teknik. Organisationer bör således minska värdet av tekniskt baserade kontroller i ISA program och istället fokusera på att de

anställda verkligen är införstådda med informationssäkerhetsriskerna. Det finns olika ISA program samt utbildningar organisationer kan använda för att öka medvetenheten hos de anställda.

2.4.4 Datorstödd informationssäkerhetsutbildning för anställda

Det nya informationssamhället innebär att de flesta organisationer och anställda hanterar och därmed kommunicerar med större mängder information än tidigare. Denna utveckling gör det vitalt för de anställda inom en organisation att ha kunskap kring säkerhet och informationshantering. Alla organisationer i Sverige erbjuds en informationssäkerhetsutbildning för användare vid namn DISA (Datorstödd informationssäkerhetsutbildning för anställda). Detta är ett kostnadsfritt initiativ från MSB som finns tillgänglig på webben eller som fristående version. DISA är en kombination utav film, text och frågor som syftar till att enkelt och kostnadseffektivt höja nivån på informationssäkerheten inom en organisation. Detta för att samtliga anställda ska ha en förståelse för vikten av informationssäkerhetshantering. Med informationssäkerhet menas möjligheten att upprätthålla önskad sekretess, riktighet och tillgänglighet hos en organisations informationstillgångar. (MSB, 2011)

Utbildningen fungerar som en introduktion och består av tio avsnitt och tar ungefär 20 minuter att genomföra. Efter avslutad utbildning ska användaren ha funderat på vilken information som är mest skyddsvärd samt hur de bäst skyddar den. De olika avsnitten är: Lösenord, Mobila enheter, Skadlig kod, Sociala medier, E-post, Säkerhetskopiering, Spårbarhet och loggning, Smarta telefoner, Surfplattor, samt säkert beteende. Dessa områden är alla särskilt viktiga för den anställde att ha kunskap om. (MSB, 2011)

2.4.5 NanoLearning via Junglemap

NanoLearning via Junglemap är en pedagogisk metod som är anpassad till ett fragmenterat arbetsliv där utbildning och medvetenhet kring informationssäkerhet är något som är centraliserat. Kursen i informationssäkerhet erbjuder upp till 28 lektioner helt anpassat utifrån kundens krav och levereras därefter till valfritt antal anställda, inklusive nyanställda, inom organisationen. Leverans sker via e-post där användarna får en serie med korta lektioner på 2-5 minuter, som är fördelade på valfritt antal veckor eller månader. För att undvika informationsöverflöd får användarna en lektion i taget, där de i lugn och ro kan ta in informationen i fråga. Utbildningen är uppbyggd som så att användarna får relevant information gällande olika situationer, utmaningar och möjligheter i relation till informationssäkerhet (Olofsson, 2016). För att mäta effekten av utbildningen ges olika typer av analyser, undersökningar, reflektionsövningar och kunskapstester. Detta gör att lärandet blir en process istället för ett enskilt event. Att enbart ha ett särskilt event kan te sig riskabelt eftersom risker förändras kontinuerligt. Processarbetet ska enligt Junglemap maximera kunskapsinhämtandet och öka medvetenheten i längden hos de anställda (Junglemap, 2017a). Exempel på standardlektioner som erbjuds via informationssäkerhetskursen är: “Vem som helst kan bli en hackare!”, “Använd HTTPs”, “Var försiktig med sociala medier”, “Håll uppsikt över USB-minnet”, “Respektera sekretess” och “Ta kontroll över apparna” (Olofsson, 2016). Kurser som erbjuds genom NanoLearning för både chefer och anställda är: Informationssäkerhet för anställda och chefer samt EU:s Dataskyddsförordning (GDPR) (Junglemap, 2017a). Bland Junglemaps kunder inom GDPR och Informationssäkerhet

finns såväl kommuner, välkända försäkringsbolag, banker, telefonoperatörer, företag inom detaljhandel m.m. (Junglemap, 2017b).

2.4.6 EU:s Dataskyddsförordning GDPR

I april 2016 beslutade EU att ett nytt regelverk för behandling av personuppgifter ska börja tillämpas i de olika medlemsstaterna i maj 2018 (Datainspektionen, 2017a). Dataskyddsförordningen, även känd som GDPR (General Data Protection Regulation) innehållet regler om hur personuppgifter får behandlas. Förordningen ersätter den nuvarande personuppgiftslagen (PUL) (Datainspektionen, 2017b). Enligt Datainspektionen kommer denna förordning innebära en del förändringar för de som behandlar personuppgifter. Det nya regelverket består av två rättsakter, men den mest centrala av dessa är den allmänna dataskyddsförordningen som gäller för behandling av personuppgifter (Datainspektionen, 2017a). Vidare räcker det inte enbart med utbildningar för de anställda, efterlevnaden måste kontrolleras för att både undvika och förebygga problem kopplat till informationssäkerhet (MSB, 2015).

2.5 Kontroll och uppföljning

För att organisationer ska kunna arbeta löpande med informationssäkerhet är en nödvändig förutsättning att arbetet löpande följs upp och utvärderas. Detta för att arbetet gällande informationssäkerhet ska kunna anpassas till organisationen och uppnå de krav som krävs gällande säkerheten. Det är inte enbart viktigt för organisationer att ha en god informationssäkerhet som fungerar på alla plan samt i alla processer, åtgärderna måste även kunna utvärderas för att säkerställa att de möter de risker och eventuella hot som identifierats (MSB, 2015). För att kunna hantera de olika risker och incidenter som en organisation dagligen utstår underlättar det om organisationen använder sig utav en beprövad incidenthanteringsmodell. Detta för att organisationer ska kunna fortsätta bedriva sin verksamhet även i riskfylld miljö. Kontinuerlig planering inför säkerhetsarbetet bör även upprättas och införas på organisationer (MSB, 2016).

En central del i arbetet gällande uppföljning av säkerheten inom en organisation är ledningens utvärdering. Detta görs av den informationssäkerhetsansvarig i form av rapporter för att se hur ledningen arbetar med informationssäkerhet samt för att se hur arbetet fortlöper. Dessa rapporter kan innefatta en redogörelse över vilka incidenter som inträffat, väsentliga förändringar i riskbilden, det arbete som genomförts, resultat av egna och oberoende granskningar, förslag till bättre policy och riktlinjer samt förslag till beslut kring arbetets inriktning och finansiering framåt. Ett vanligt misstag som ofta sker i arbetet gällande rapportering är att se informationssäkerhet som en IT-fråga. Detta leder i de flesta fall att organisationer sätter en ansvarig från IT-avdelningen som ansvarar för informationssäkerheten (MSB, 2016). Detta medför i många fall komplikationer i form av att säkerhetsarbetet blir för präglat av it-fokus och arbetet blir således för tekniskt. Organisationer måste förstå att informationssäkerhet inte är detsamma som IT-säkerhet och arbetet måste därför ha ett bredare perspektiv och inte bara IT-inriktat. Informationssäkerhet rör all typ av informationshantering och inte enbart de tekniska aspekterna (MSB, 2016).

2.6 Sammanfattning av teorin

2.6.1 Policy och styrande dokument

En av de viktigaste kontrollerna när det kommer till informationssäkerhet är upprättandet av en policy. Dessvärre finns det svårigheter med att utforma en information security policy (ISP) eftersom det kan vara svårt att identifiera vad som skall inkluderas i den (Höne & Eloff, 2002). En ISP fungerar som en redogörelse för de olika säkerhetsmålen som en organisation har, men inkluderar även vad som skall skyddas och hur detta görs i praktiken (Gollmann, 2011). Vidare är det vitalt att reflektera över vem eller vilka som skall utforma denna policy. Det är vitalt att inkludera psykologiska aspekter vid utformandet av en policy och således inte bara tekniska synvinklar (Layton, 2005). För att en ISP ska fylla sin funktion bör dokumentet vara förståeligt och meningsfullt och dessutom adressera användarna direkt, samt övertyga användarna att använda sina informationsresurser på ett säkert sätt (Höne och Eloff, 22). Bulgurcu, et al. (2010) menar att de anställda måste samtycka med dessa policys för att tillämpa dem. Nyckeln till detta ligger i att identifiera och förstå vilka faktorer som motiverar de anställda. De anställda måste således vara medvetna, utbildade och tränade inom området (Martins & Elofe, 2002).

2.6.2 Utbildning och kompetensutveckling

De mest kritiska aspekterna gällande informationssäkerhet och skyddandet av känslig information, är utbildning och medvetenhet (Amankwa et al. 2015). Information security awareness (ISA) används för att referera till det stadiet som de anställda befinner sig i när de är både medvetna och fullt engagerade i säkerhetsarbetet. Ökad medvetenhet ska minimera misstag relaterade till användaren och således upphäva dessa misstag i teorin (Siponen, 2000). Det ökade behovet av en förbättrad informationssäkerhet har resulterat i skapandet av ISA program. Detta för att användaren i många fall ses som ett hot mot säkerheten istället för en tillgång (Schlienger & Teufel, 2002). Målet med införandet av ett ISA program är att förändra de anställdas inställning och beteende gentemot informationssäkerhet och därför är det viktigt att ISA programmet är strukturerat efter användarnas behov (Thomson & von Solms, 1998). Vidare bör ISA programmet främja informationsäkerhetstänket hos de anställda och således inkludera användarnas insikt och svar på frågan "varför", detta för att öka medvetenheten. Programmet bör även inkludera frågan "hur" som inkluderar träning och ökandet av kompetens (Siponen, 2000). Slutligen är vikten av utbildning och kompetensutveckling särskilt viktig eftersom nästan alla lösningar på informationssäkerhet idag vilar på att den mänskliga faktorn inte felar (Thomson et al. 2006).

2.6.3 Kontroll och uppföljning

För att organisationer ska kunna följa upp sitt arbete gällande informationssäkerhet är det nödvändigt att arbetet följs upp och utvärderas kontinuerligt. Arbetet gällande informationssäkerhet måste anpassas till organisationen och uppnå de krav som ställs på säkerheten. Enligt MSB (2016) görs detta på bästa sätt genom utvärdering och rapportering. Denna uppföljning av säkerheten bör ske av ledningen i form av utvärderingar. Uppföljningen görs i form av rapporter för att se hur ledningen arbetet med informationssäkerhet för att se hur arbetet fortlöper. Dessa rapporter kan innehålla olika delar som är väsentliga för fortsatt arbete gällande informationssäkerhet. De inkluderar bland annat redogörelser över vilka incidenter som inträffat, väsentliga

förändringar i riskbilden, det arbete som genomförts, resultat av egna och oberoende granskningar samt förslag på bättre policy och riktlinjer.

2.7 Teoretiskt ramverk

Det teoretiska ramverket grundar sig i Conner och Pattersons (1982) teori angående att en anställd går genom tre steg vid en organisatorisk förändring innan den anställda slutligen rättar sig efter förändringen i fråga. De tre största stegen är *preparation*, *awareness* och *commitment*. Layton (2005) kopplar dessa steg till ISA då huvudsyftet är att förändra användarnas beteende kring informationssäkerhet till mer självgående och förstående. Dessa steg har i denna uppsats kopplats till tre områden i MSB:s enkätundersökning från 2015: *policy & styrande dokument*, *utbildning & kompetensutveckling* samt *kontroll & uppföljning*. Uppsatsen grundas i MSB:s enkätundersökning med fokus på den mänskliga faktorn. Dessa tre område kan alla kopplas till den mänskliga faktorn och hur organisationer arbetar med att inkludera slutanvändarna i arbetet.

Figur 2. Teoretiskt ramverk anpassat från Conner och Pattersons (1982) teori angående en anställds anpassning vid en organisationsförändring.

För att uppnå en hög informationssäkerhet är det vitalt att de anställda är införstådda och förberedda *(prepared)* med de riktlinjer och regler som är satta på organisationen. Detta faller under området *policy & styrande dokument.* Det räcker inte enbart med att en organisation har etablerat dessa dokument, utan en vital del är att de anställda är införstådda med innehållet (Martins & Elofe, 2002). Är de anställda inte införstådda med de riktlinjer och regler som är satta inom en organisation ökar riskerna för att den mänskliga faktorn ska ha negativ påverkan på arbetet. Vidare är det vitalt att de anställda förstår hur de ska arbeta dagligen utan att riskera organisationens säkerhet (Thomson & von Solms, 1998). Här är *utbildning & kompetensutveckling* en viktig faktor som är av stor relevans för organisationer. Att ha kunskap gällande *styrande dokument och policy* är inte tillräckligt, om inte utbildning och medvetenheten finns *(awareness).* Andra delen i det teoretiska ramverket inkluderar därför utbildningen av de anställda. Erbjuder inte en organisation utbildning till sina anställda är det större risk att den mänskliga faktorn blir avgörande i arbetet och således riskera organisationens säkerhet.

Utöver att de anställda är införstådda med organisationens policy och styrande dokument samt har rätt utbildning för att utföra deras dagliga arbete krävs det *kontroll & uppföljning.* En organisations anställda kan arbeta med informationssäkerhet i deras dagliga arbetsuppgifter men

kontrolleras inte efterlevnaden är risker för eventuella hot och problem större (MSB, 2015). Detta kopplas till det sista steget *(commitment)* som innebär att samtliga i organisationen måste se arbetet med informationssäkerhet som en process. Utför inte en organisation detta arbete finns det stor risk att de anställda utför riskabla val i deras dagliga arbetsuppgifter. Dessa val kan i sin tur riskera informationssäkerheten och den mänskliga faktorn blir därmed avgörande.

Att koppla samman dessa tre steg ligger i linje med vad Layton (2005) belyser gällande att minska värdet av tekniskt baserade kontroller inom ISA program och istället fokusera på att de anställda är införstådda med informationssäkerhetsriskerna, det vill säga den mänskliga faktorn av informationssäkerhet. Med fokus på den mänskliga faktorn genom uppsatsen har detta teoretiska ramverk legat till grund för arbetet, och således ökat förståelsen för kopplingen mellan de tre huvudämnena och dess vikt på en kommuns arbete gällande informationssäkerhet.

3 Metod

Detta kapitel beskriver hur undersökningen har utförts och varför, med grund i litteraturen. Syftet med metodkapitlet är att beskriva tillvägagångssättet, vilka olika val som tagits i undersökningen och hur arbetet kring detta har skett.

3.1 Metodval

Enligt Jacobsen (2002) finns det två övergripande metodansatser att tillämpa gällande datainsamling vid en forskningsundersökning och dessa är kvalitativ eller kvantitativ. I denna uppsats har en kvalitativ metod tillämpats eftersom sociala fenomen undersöks. Med sociala fenomen syftar vi i detta fall till den mänskliga faktorn inom informationssäkerhet som belyses i tidigare avsnitt.

3.2 Urval

Jacobsen (2002) menar att en empirisk undersökning syftar till att undersöka hur verkligheten ser ut. Vidare beskriver författaren vikten av att komma i kontakt med personer som är korrekt anpassade för ändamålet och som således kan tillhandahålla den informationen som efterfrågas. I enlighet med Jacobsen (2002) beslutades det att kontakta personer med relevant bakgrund, alltså personer som aktivt arbetar med informationssäkerhet på något sätt, men helst inom en beslutsfattande roll. En förfråga skickades ut till 30 kommuner i Sverige, utan vidare eftertanke på storlek eller folkmängd. Allt för många intervjuobjekt är överflödigt när det kommer till en kvalitativ metod och därför bör 20 intervjuobjekt ses som en övre gräns (Jacobsen, 2002). Med detta i åtanke kontaktades enbart 30 kommuner i Sverige. Gällande storlek och folkmängd på kommunen menar MSB:s enkätundersökning (MSB, 2015) att detta inte har någon betydelse för undersökningen i fråga då inget samband identifierades i deras undersökning.

Av de 30 tillfrågade kommuner svarade 3 kommuner att de inte hade möjlighet att medverka, 5 kommuner vidarebefordra mailet till behörig person, 14 kommuner svarade inte alls och 8 kommuner kunde medverka i undersökningen. Som tidigare nämnt är de medverkande intervjuobjekten anpassade för ändamålet och har dessutom liknande befattning som de som deltagit i MSB:s enkätundersökning från 2015 (MSB, 2015). En intressant aspekt vid urvalsprocessen var att en kommun inte hade möjlighet att delta då de var mitt uppe i ett stort utvecklingsarbete inom informationssäkerhet, där bland annat information och utbildning för kommunens tjänstemän och förtroendevalda ingår. De ansåg därför inte att de hade tid att medverka. Nedan presenteras en tabell med de kommuner som intervjuats, befolkning inom kommunen, antal anställda samt vilken befattning intervjuobjektet har inom kommunen.

KOMMUN	BEFOLKNING	ANSTÄLLDA	BEFATTNING
K1	ca 30 000	ca 3050	Säkerhetssamordnare
K2	ca 13 000	1325	IT-chef
K3	ca 15 000	ca 1375	Trygghetsstrateg
K4	ca 17 000	ca 1375	Kris- och säkerhetssamordnare
K5	ca 18 000	ca 1775	IT-samordnare
K6	ca 77 000	ca 6600	Informationssäkerhetssamordnare
K7	ca 62 000	ca 4375	Kommunarkivarie
K8	ca 17 000	ca 1575	Kommunarkivarie

Tabell 1. Kommuner och intervjuobjekt

3.2.1 Geografisk plats

Andersson (1994) redogör för olika frågemetoder som kan delas in i muntliga och skriftliga metoder. Till de muntliga metoderna hör bland annat telefonintervjuer, vilket har varit tillvägagångssättet under denna undersökning. Detta beroende på att intervjuobjekten har befunnit sig på geografiska platser i Sverige som har hämmat möjligheten till en intervju öga mot öga. Jacobsen (2002) skriver att telefonintervjuer inte är lika kostsamma som intervjuer ansikte mot ansikte, eftersom dessa kräver fysisk förflyttning från plats till plats. Vidare exemplifierar författaren de båda tillvägagångssättens baksidor gällande hur påverkad intervjuobjektet blir av att intervjuas i samma rum eller via telefon. En av dessa nackdelar är det faktum att det inte finns möjlighet att känna av informantens kroppsspråk eller sinnesstämning över telefon.

3.3 Utformning av intervjuguide

För att kunna hålla en struktur genom en intervju och vidare kunna analysera den insamlade data krävs det en intervjuguide att utgå ifrån. Vidare är intervjuarens uppträdande avgörande när det kommer till resultatet av en intervju. En tillitsrelation mellan intervjuare och intervjuobjekt är vital för att uppnå en så öppen informationsutväxling som möjligt. Dock är denna tillit knepig att uppnå när en relation inte är etablerad sedan tidigare, vilket gör det mer komplicerat att få en öppen informationsutväxling (Jacobsen, 2002). Vidare menar författaren på att alla inte kan lära sig att uppträda lika bra under intervjuer, men att det finns några tips som alltid skall tillämpas. Först och främst ska intervjuaren inleda intervjun en snabb översikt där det framgår vem som intervjuar, vad ändamålet för intervjun är och hur informationen kommer att användas. Intervjuaren skall även öppna upp för eventuella frågor och funderingar under detta skede.

För att uppnå en god relation mellan intervjuare och intervjuobjekt har mailkontakten varit tydlig redan ett par veckor innan intervjuerna utfördes. Detta för att minska riskerna för missförstånd när intervjuerna väl utfördes, samt för att ge intervjuobjekten möjlighet att ställa motfrågor. Riktlinjerna gällande intervjuerna har tillämpats och syftet med intervjuerna har varit tydligt för intervjuobjekten redan i den inledande fasen.

När den huvudsakliga intervjun inleds är det vitalt att ställa öppna frågor. Intervjuaren skall inte heller styra samtalet vid uppstart, utan snarare låta intervjuobjektet styra intervjun. Genom dessa öppna frågor framgår det vad intervjuobjektet tycker är viktigt (Jacobsen, 2002). Vidare redogör författaren att intervjuaren inte skall avbryta, utan snarare lyssna noggrant och be intervjuobjektet utveckla svar som varit intressanta för undersökningen. Termer så som: "Hur menar du då?" och "Det du sa var intressant, skulle du kunna utveckla det lite?" kan användas för att få ut så mycket information som möjligt (Jacobsen, 2002). Intervjufrågorna har således inte varit ledande, utan snarare öppna för att intervjuobjekten själva ska styra samtalet och få berätta fritt om sitt arbete. Termerna som nämnts ovan har använts under intervjuerna för att få ut så mycket detaljrik information som möjligt.

Avslutningsvis menar Jacobsen (2002) att intervjun skall avslutas mjukt och inte tvärt. En idé kan vara att meddela intervjuobjektet att denne gett den informationen som behövs för undersökningen och avsluta med att fråga intervjuobjektet om denne vill tillägga något. Slutligen är det viktigt att hålla en god ton och tacka informanten för deltagandet. Ovanstående aspekter har tillämpats under intervjuerna genom att i slutet ställa en öppen fråga om intervjuobjekten till lägga till någonting, eventuellt ställa intervjuaren frågor. Detta för att förmedla en seriös bild av arbetet i fråga.

3.3.1 Teori kopplat till intervjuguide

Intervjuerna startade med öppna frågor som allmänt handlade om intervjuobjektets position på kommunen, hur involverad denne är i informationssäkerhetsarbetet, hur denne upplever att kommunen arbetar med säkerheten samt fråga om deltagandet i MSB:s enkätundersökning *En bild av kommunernas informationssäkerhetsarbete 2015*. Vidare delades intervjun upp i tre huvuddelar som matchar de tre koncepten: *policy och styrande dokument*, *utbildning och kompetensutveckling* samt *kontroll och uppföljning*. Intervjufrågorna som inkluderas i de tre olika koncepten är utformade med teorin som grund. Detta för att koppla svaren till teorin, både likheter samt skillnader.

Avslutningsvis ställdes öppna frågor till intervjuobjekten gällande den största utmaningen inom informationssäkerhet samt hur attityden ser ut hos de anställda gentemot informationssäkerhet. Detta för att få en avslutande bild över kommunens arbete inom informationssäkerhet, samt att ge intervjuobjekten chansen att prata mer öppet om hur de upplever attityden mot säkerheten på deras kommun. Nedan presenteras de tre koncept som varit huvudfokus genom uppsatsen, vilka författare som tagit upp detta ämne samt de intervjufrågorna som är kopplade till de specifika konceptet.

KONCEPT	FÖRFATTARE	INTERVJUFRÅGA
Policy & styrande dokument	Whitman & Mattord (2008), LeVeque (2006), Höne & Eloff (2002), NE (2017), Whitman, Townsend & Aalberts (2001), Martins & Elofe (2002), Gollmann (2011), Bulgurcu, Cavusoglu & Benbasat (2010), Layton (2005)	6. Har Ni etablerat en informationssäkerhetspolicy? 7. Vem eller vilken del av organisationen har i så fall utvecklat denna? 8. När skapades denna och när reviderades den senast? 9. Vem eller vilka är ansvarig(a) för policyn? 10. Hur arbetar Ni på kommunen för att Era anställda skall vara införstådda med er informationssäkerhetspolicy? 11. Hur har resultatet av MSB:s undersökning förändrat ert arbete gällande policy och styrande dokument?
Utbildning & kompetensutveckling	Amankwa, Loock & Kritzinger (2015), Martins & Elofe (2002), Thomson, von Solms & Louw (2006), Siponen (2000), Thomson & von Solms (1998), Schlienger & Teufel (2002), Kruger & Kearney (2006), Layton (2005), Dewey & Shaffer (2016), MSB (2011), Olofsson (2016), Junglemap (2017a), Junglemap (2017b), Datainspektionen (2017a), Datainspektionen (2017b), MSB (2015),	12. Hur arbetar ni med utbildning och kompetensutveckling för Era anställda? 13. Hur ser er generella utbildningsplan ut inom kommunen, och när sker denna utbildning? 14. Hur ser framtiden ut gällande utbildningsarbeten på Er kommun? 15. Hur har resultatet av MSB:s undersökning förändrat ert arbete gällande utbildning av anställda inom informationssäkerhet? 16. Enligt MSB:s enkätundersökning var det 136 stycken kommuner som inte erbjuder utbildning inom informationssäkerhet till sina anställda. Var ni en av dessa kommuner?
Kontroll & uppföljning	MSB (2015), MSB (2016)	17. Hur arbetar Ni med kontroll och uppföljning? 18. Hur har resultatet av MSB:s undersökning förändrat ert arbete gällande kontroll och uppföljning?

Tabell 2: Teori kopplat till intervjuguide

3.3.2 Intervjuform

Som tidigare nämnt valdes intervjuerna att utföras över telefon på grund av de geografiska platserna intervjuobjekten befann sig på. Före intervjuerna utfördes skickades intervjuguiden till samtliga objekt, detta för att underlätta för de som skulle intervjuas. Detta gav objekten möjlighet att tänka genom de olika frågorna och svar. Detta kan både ses negativt och positivt. Att objekten i förhand tilldelades en intervjuguide kan bidra till inövade svar och på så sätt inte helt sanningsenliga. Det kan även bidra till positiva resultat i form att de får tänka efter en extra gång och verkligen berätta allting istället för att i efterhand komma på väsentlig information som hade kunnat gynna undersökningen. Valet att skicka ut intervjuguiden på förhands togs mestadels på grund av att ämnet informationssäkerhet är ett känsligt ämne som kräver stor försiktighet.

Som tidigare nämnt menar Jacobsen (2002) att en nackdel med telefonintervjuer är det faktum att det inte finns möjlighet att identifiera intervjuobjektets kroppsspråk eller sinnesstämning över telefon. Frågor gällande informationssäkerhet och faktorer kring ämnet kan ses som känsliga för vissa organisationer. Att inte ha möjlighet att se intervjuobjekten och hur de påverkades av de ställda frågorna kan ses negativt för intervjuerna och hur de fortlöpte. Dock fick objekten tillgång till intervjuguiden i förhand och visste vilka frågor som skulle ställas och hade därför kontroll över intervjun och kunde avbryta eventuella svåra frågor om det skulle dyka upp. Detta var därför ingenting som påverkade undersökningen tydligt och telefonintervju var den mest ultimata intervjuformen för detta arbete.

3.4 Undersökningskvalitét

3.4.1 Validitet

Enligt Jacobsen (2002) finns det både intern och extern validitet. Den interna validiteten fokuserar på resultatens giltighet där begreppet intersubjektivitet används framför begreppet sanning. Intersubjektivitet är det närmsta vi kan komma sanningen genom att flera personer är ense om att någonting är en riktig beskrivning. Ju fler personer som är ense om detta fenomen, desto större sannolikhet att informationen är riktig. Med detta i baktanke har en responsvalidering genomförts, då intervjuobjektet fått ta del av transkriberingen för att lämna eventuella invändningar gällande resultatet av intervjun. Därmed har intervjuobjektet fått en möjlighet att korrigera innehållet om denne anser att något är felaktigt återgivet eller liknande. Denna validering har skett för att främja den interna validiteten, samt för att korrektheten skall vara så hög som möjligt.

Gällande extern validitet och överförbarhet handlar det om i vilken grad som resultaten från en undersökning kan generaliseras. En styrka i kvalitativa metoder ligger i att utveckla generella teorier om verkligheten och hur denna företer sig. (Jacobsen, 2002). För att presentera resultaten från intervjuerna har löptext skrivits under kapitlet resultat. Utöver texten där resultaten presenterats har det tagits ut specifika citat från de transkriberade intervjuerna som är relevanta för innehållet. Avslutningsvis presenteras en sammanfattning av resultatet i form av en tabell där specifika delar av intervjuerna valts ut. Både citaten och utdragen i tabellen är refererade till transkriberingarna, detta för att tydligt kunna se likheter och skillnader mellan kommunerna. Detta kan ses som generalisering, men enbart i en liten grad då inga antagande gjorts utan all fakta grundas i intervjuerna.

3.4.2 Reliabilitet

Jacobsen (2002) belyser vikten av att kritiskt granska reliabiliteten i själva undersökningen, med syfte att ta reda på om resultaten är tillförlitliga. Författaren menar på att alla undersökningar utsätter de undersökta objekten för olika stimuli och signaler som kan påverka slutresultatet. På grund av ovanstående är det enligt Jacobsen (2002) vitalt att granska effekter av dessa för att för att säkerställa tillförlitligheten i undersökningen. Denna punkt handlar främst om att ta reda på om det går att lita på den insamlade data, och i detta fall har främst två olika åtgärder vidtagits. Först och främst har intervjuobjektet intervjuats i en naturlig miljö istället för en artificiell sådan (Jacobsen, 2002). Detta eftersom intervjuobjektet har kunnat sitta på sitt kontor

under intervjun och därmed kunnat vara bekväm med situationen. För det andra har intervjun varit planerad, snarare än överraskande, då intervjuobjektet själv fått bestämma tid för intervju. Dessutom har intervjuobjektet fått en intervjuguide innan intervjun med syfte att kunna förbereda sig.

3.4.3 Etik

Jacobsen (2002) menar att etiska dilemman främst uppstår i situationer där avsikten med en undersökning döljs. Människor som vet att de är studerade tenderar att uppträda annorlunda än vad de skulle gjort i en vanlig situation och därför vill många dölja avsikten med en undersökning. Enligt författaren finns det inga klara direktiv gällande etik, men det finns tre grundkrav som en undersökning bör uppfylla. Bland dessa finns: informerat samtycke, krav på privatliv och krav på att bli korrekt återgiven. För att inte dölja avsikten med intervjun har, som tidigare nämnt, en preliminär intervjuguide skickats ut till intervjuobjektet, med syfte att intervjuobjektet ska kunna ta reda på fakta inom vissa områden på förhand. Detta var även ett önskemål från vissa intervjuobjekt. På grund av ovanstående har intentionen med telefonintervjun aldrig varit dold, utan snarare tydlig från första kontakt med intervjuobjektet.

I ett initialt mail (Bilaga 7.3) har objektet fått information gällande ändamål och i vilket syfte intervjun sker. Efter detta mail har objektet själv fått ta ställning till om denne vill delta eller ej. Dessutom har det funnits ett samtycke till inspelning av samtliga intervjuer och intervjuobjektet har fått information gällande syftet med inspelningen. Jacobsen (2002) menar att detta benämns som informerat samtycke, eftersom den som undersöks frivilligt deltar i undersökningen. Vidare förklarar författaren termen "krav på privatliv", där författaren bland annat skriver om rätten till anonymitet. Med anonymitet menas att det skall vara omöjligt att koppla information till den enskilda personens identitet. Detta kan dock te sig komplicerat när det inte finns så många uppgiftslämnare, och därmed måste kraven på anonymitet lättas, eftersom det är omöjligt att garantera den. Istället tillämpas olika krav på konfidentialitet, vilket gör det praktiskt möjligt att identifiera individer även om de anonymiserats. Gällande detta anonymitetskrav, har ingen anonymitets utlovats. Av etiska skäl har dock namnen på intervjuobjekten samt kommuner inte tagits med, utan enbart deras befattning på kommunen, samt kommunens befolkningsmängd och antal anställda. Detta gör det praktiskt möjligt att identifiera individerna trots att de är anonymiserade, men uppfyller krav på konfidentialitet.

4 Resultat

Nedan presenteras resultaten från de åtta telefonintervjuer som utförts. Resultaten presenteras med fyra underrubriker: policy & styrande dokument, utbildning & kompetensutveckling, kontroll & uppföljning samt övrigt. De tre första områdena har varit huvudfokus genom hela uppsatsen och återspeglas även i det teoretiska ramverket. Resultaten presenteras i löptext och kompletteras med specifika citat direkt tagna från de transkriberade intervjuerna. Vidare presenteras tabeller för att tydligare visa eventuella samband eller skillnader mellan de olika kommunerna.

4.1 Policy och styrande dokument

Samtliga kommuner som intervjuats har en informationssäkerhetspolicy (ISP), men endast 7 kommuner har en som är beslutad av kommunstyrelsen. K4 har en ISP, men den är inte beslutad av kommunstyrelsen än. Vidare nämner K3 att deras ISP är tio år gammal och därför inte är aktuell längre, intervjuobjektet säger: *"Jag har fått som hastigast någon form av genomgång på kommunens informationssäkerhet och det har funnits en policy. Det vi skrattade lite åt var att den var så gammal om vi säger så, den har säkert tio år på nacken. Den är ju inte aktuell längre men den finns och den har funnits, men den är inte uppdaterad."* (Bilaga 7.2.3, Rad 44-47).

Resterande sex kommuner har skapat sin ISP från åren 2012–2016. Samtidigt som K6 skapade sin ISP utvecklades även allmänna riktlinjer för informationssäkerhetsarbetet på kommunen. K2 är den enda av de åtta kommunerna som har en ISP bestående av två delar. Den första delen är mer övergripande och inkluderar vad förvaltningschefen har ansvar för osv. Den andra delen kallas för användarinstituition, där alla anställda kan ta del av mer detaljerad information kring vad de får och inte får göra samt vad de anställda ska tänka på i deras dagliga arbete kring informationssäkerhet. Intervjuobjektet nämner dock *"Den är väl helt okej, skulle kanske varit lite, göras bättre. Men det är en helt okej policy".*(Bilaga 7.2.2, Rad 77).

Variationen bland kommunerna angående vem som utvecklat deras ISP är stor. Fyra utav kommunernas ISP har skapats av kommunens säkerhetssamordnare. K2s ISP utvecklades av IT-chefen och K3s skapades av en anställd på IT-kontoret. K8s ISP utvecklades av deras kommunarkivarie tillsammans med kommunens jurist och K7s utvecklades av en projektanställt men intervjuobjektet hade ingen vetskap om den exakta befattningen.

Revideringen av kommunernas ISP skiljer sig åt beroende på hur kommunen arbetar med informationssäkerhet. K1 har en dokumentationsplan där de anställda på trygg- och säkerhetsenheten ansvarar för ett antal dokument. Dessa dokument gås igenom och revideras en gång per år. De reviderar även sin ISP vid behov samt om någon incident inträffat med koppling till säkerheten. Fem av de åtta kommunerna som intervjuades hade ingen vetskap angående när, eller om deras ISP är reviderad, när detta sker, eller under vilka förutsättningar. Dock nämner

K7 att deras ISP är i stort behov av en uppdatering då den inte fyller önskad funktion. Intervjuobjektet säger: *"Vi har en policy från 2014, sedan har det väl egentligen inte hänt så mycket mer med den, så det är egentligen hög tid att uppdatera den [...]"* (Bilaga 7.2.7, Rad 48-49). K6 är heller inte medveten om när deras ISP reviderades senast eller när den bör revideras, dock är det säkerhetssamordnarens ansvar att detta blir gjort på ett korrekt sätt och under rätt tillfällen. K5 reviderar sin ISP var tredje år och det skapades även en ny ISP i höstas som reviderades i Mars 2017.

Tre av åtta intervjuobjekt var inte medvetna om vem som ansvarar för deras ISP. K7 nämner att deras ISP enbart gäller till detta år, 2017, och att den sen måste skrivas om för uppdateringar. I dagsläget är det kommunkansliet som ansvarar för den. K3 är en av de tre kommuner som inte är medveten om vem som ansvarar för deras. Intervjuobjektet nämner dock att informationssäkerheten tillhör IT och ligger på den avdelningen, även fast detta inte alltid stämmer. Objektet menar att informationssäkerhet tillhör mer än bara de tekniska aspekterna. K8 nämner även att deras kommunjurist samt arkivarien, samma personer som skapade deras ISP, är även ansvariga för policyn. Det är dock en oklar situation då det i dagsläget inte är någon som konkret arbetar med informationssäkerhet på kommunen. Vidare är tre av de åtta kommunerna som intervjuades fullt medvetna om vem som ansvarar för deras ISP. Trygg- och säkerhetsenheten ansvarar för K1s policy, och på K4 samt K5 är det kommunens säkerhetssamordnare.

Fyra av intervjuobjekten tog upp att de inte arbetar med att de anställda ska vara införstådda i deras ISP. K3 nämner dock av egen erfarenhet att denne blev anställd i februari och har inte fått någon information gällande deras ISP, utan att det finns dokument de anställda själva kan söka upp på kommunens hemsida och således få information och kunskap gällande deras ISP. Intervjuobjektet säger "*[...] kan jag bara relatera till mig själv då jag började här den första februari och jag har inte fått någon information om informationssäkerhet så länge jag varit här. Dock vet jag att det finns dokument som man själv kan leta upp på hemsidan då. Men inte så att man, jag fick inte ta del av någonting när jag började."* (Bilaga 7.2.3, Rad 57-61). Intressant att tillägga är att K3 arbetar som trygghetsstrateg och i framtiden ska ansvara för informationssäkerhetsfrågor.

K7, en av de kommunerna som inte arbetar med anställdas förståelse för deras ISP nämner att deras policy enbart existerar och det inte finns något mer bakomliggande arbete. Intervjuobjektet önskar dock att kommunen arbetar mer med deras ISP och att den hade fyllt någon värdefull funktion. K4 fokuserar inte mycket på deras ISP utan riktar arbetet mer på den dagliga användningen och hanteringen av informationssäkerhet samt att utbilda i detta. Intervjuobjektet säger *"Ja, alltså man kan väl säga att vi inte fokuserar jättemycket på policyn, utan vi fokuserar mer på den dagliga användningen av att få informationssäkerhet på, alltså utbilda i det."* (Bilaga 7.2.4, Rad 42-43). De arbetar dock en del med att göra ledningsgruppen införstådd och medvetna om vad deras ansvar är samt vad behöver göras, men inte generellt med de anställda.

Likt K4, tar K1 upp att de arrangerar mindre informationskampanjer. Dessa är dock inte riktade till den enskilda medarbetaren, och deras ISP finns heller inte där för att hjälpa de anställda.

Intervjuobjektet säger *"Men policyn i sig skrevs ju på en väldigt hög nivå så att det är ju egentligen inte en större hjälp för den enskilde medarbetaren och det var inte syftet med den heller"*(Bilaga 7.2.1, Rad 58-60). Deras ISP togs fram för att enheten som ansvarar för den skulle få mandat att arbeta med frågor gällande informationssäkerhet ute i förvaltningen. Deras ISP finns även för att deras ledningsgrupp och förvaltningschef ska bli mer införstådda vad de har för antaganden. K5s arbete med deras ISP skiljer sig från de andra kommunerna. Först tas innehållet upp i deras chefsgrupper, när de gett sitt godkännande får varje chef sitt eget ansvar att vidare ta upp information på en arbetsplatsträff. De anställda ska läsa igenom alla vägledande råd och bestämmelser ("vrobbar") kopplade till informationssäkerhet, samt deras ISP. Vidare i processen ska de skriva under ett papper där de medger att de tagit del av utbildningen och förstått kontentan. Detta kontrakt förvaras det tillsammans med den enskildes personalakt. Deras ISP ligger även uppe på nätet för alla anställda att hitta. Således kan ingen anställd förneka att de inte är förstådda med innehållet i deras ISP, eller säga att de inte hittar eller har tillgång till den.

4.2 Utbildning och Kompetensutveckling

Gällande utbildning och kompetensutveckling, arbetar de olika kommunerna på olika sätt. K3 hade en nyanställd inom posten för informationssäkerhet, vilket gjorde att denne inte kunde svara på frågorna gällande detta område (Bilaga 7.2.3, Rad 9-20). Därför finns bara sju respondenter inom området utbildning och kompetensutveckling. Dessutom anger K8 att de inte arbetar med utbildning och kompetensutveckling i dagsläget, vilket gör att det enbart är sex kommuner som gett fullständiga svar.

Fyra kommuner anger att de erbjuder DISA som utbildningsmaterial till sina anställda, men det är oklart huruvida de andra fyra kommunerna använder sig utav DISA eller inte. Fyra kommuner anger dessutom att de börjat använda sig av ett nytt utbildningsverktyg vid namn NanoLearning via Junglemap. K1 anger att NanoLearning ger full kontroll över skapandet av lektioner och att resultatet kan följas upp i realtid, vilket resulterar i en bra statistik. Dessutom anger intervjuobjektet att medarbetarna får en påminnelse en gång i veckan angående utbildningen, vilket enligt K1 *"Detta påminner dem om att få in informationsäkerhetstänket i ryggraden"* (Bilaga 7.2.1, Rad 98-99). En annan kommun, K2, säger såhär om utbildningen: *"Alltså det är verkligen fokus på informationssäkerhet och lite sunt förnuft kan man säga."* (Bilaga 7.2.2, Rad 135-136).

Gällande arbetet med DISA anger K1 att de från år 2014 har utvecklingssamtal mellan anställd och chef gällande utbildningen i DISA. Däremot uttalar sig K1 följande angående DISA-utbildningen: *"[...]jag ska väl inte säga utbildning, för DISA är väl mera för att höja medvetenheten iallafall"* (Bilaga 7.2.1, Rad 80-81). Även K5 recenserar DISA enligt följande: *"Alltså inte såhär stenåldersfrågor som jag tycker att DISA har litegrann"* (Bilaga 7.2.5, Rad 178-179). Hos K5 finns DISA tillgängligt för alla anställda på intranätet sedan 6-7 år sedan tillbaka och utan godkänt resultat på DISA får de anställda inte tillgång till kommunens nät.

Förutom DISA och NanoLearning som utbildningsunderlag använder sig K5 av så kallade "Vrobbar" (Vägledande råd och bestämmelser) som måste läsas och skrivas under utav de anställda, för att visa att de förstått och tagit till sig informationen. Dessutom måste informationssäkerhetspolicyn läsas genom samtidigt, för att även den undertecknas. K2 erbjuder alla nyanställda att delta på en introduktionsdag, där ett pass under dagen behandlar informationssäkerhet. Vidare nämner K6 att de lutar sig på IIS (Internetstiftelsen i Sverige) där material som inkluderar utbildning och kurser, finns upplagt. Av de kommuner som varken anger DISA eller NanoLearning som utbildningsverktyg finns bland annat K4 som istället har utbildat alla kommunens chefer inom informationssäkerhet, och i framtiden hoppas de göra ytterligare en sådan utbildning med cheferna, men också för de anställda.

Gällande framtida utbildningsplaner anger alla kommuner förutom två att det inte finns några specifika planer kopplat till utbildning och kompetensutveckling just nu. K8 anger att de ska göra ett stort projekt till hösten som kommer att inkludera väldigt mycket utbildning, men som främst kommer handla om att försöka formulera krav på IT-verksamheten (Bilaga 7.2.8, Rad 56-59). Gällande framtidsplaner hos K4 säger intervjuobjektet *"[...]vi kommer till hösten köra för cheferna och förhoppningsvis kommer vi ha en bra webbutbildning också i höst, men vi kanske kommer igång i början av nästa år"* (Bilaga 7.2.4, Rad 54-56). K7 nämner att de vill utvärdera NanoLearning som utbildningsverktyg innan de börjar fundera på framtida utbildningsplaner, då de knappt arbetade med utbildning för de anställda innan NanoLearning.

Något annat som lyfts fram inom området är den nya dataskyddsförordningen, GDPR, som enligt K5 tagit fokus från resterande informationssäkerhetsarbete. *"[...]den träder ju i kraft snart och därför måste vi lägga lite krut på utbildning inom det då. Och då blir det kanske att informationssäkerheten ligger lite mer bakom än så länge. Eftersom vi måste satsa jättemycket på den här GDPR:en."* (Bilaga 7.2.5, Rad 109-111). Även K7 menar att den nya dataskyddsförordningen tagit fokus från informationssäkerhetsarbetet: *"Som sagt ligger ju då vårt fokus rätt mycket nu på dataskyddsförordningen. Så vi håller ju på med det och har skickat alla då som kan vara berörda av det arbetet på kurser. Från alla förvaltningar och bolag. Detta är ju en informationssäkerhetsfråga man hanterar"*(Bilaga 7.2.7, Rad 72-74). Förutom dessa kommuner nämner även K2 och K6 GDPR kortfattat.

Huruvida MSB:s undersökning förändrat utbildningsarbetet på kommunerna eller inte så var svaret, hos de som svarade, att arbetet inte förändrats i och med resultatet av undersökningen. K2 menar att undersökningen främst används som ett argument när informationssäkerhetsfrågan ska lyftas fram, mer som statistikunderlag. Gällande vad resultatet av undersökningen gett kommunen uppger K1: *"Jag kan väl inte påstå att vi är så styrda av vad alla andra gör [...] mer att ha som en reflektion till kanske hur man står sig i förhållande till andra"* (Bilaga 7.2.1, Rad 109-111).

4.3 Kontroll och uppföljning

Utav de åtta kommuner som intervjuades var det enbart ett av intervjuobjekten som med säkerhet kunde säga att de arbetar med kontroll och uppföljning. K4 har gjort många informationsklassificeringar den sista tiden, det tas även upp att när dessa klassificeringar är färdigställda är det en del som behöver åtgärdas. Dessa olika faktorer som behövs åtgärdas tas upp och analyseras för att se hur saker och ting görs samt hur det fungerar. Detta gås genom manuellt men under sommaren kommer den läggas in i verksamheten. På så sätt kommer arbetet kunna följas genom ledningssystemet.

Resterande av kommunerna som intervjuades erkände att de inte hade bra koll på kontroll och uppföljning. K1 nämnde att de fortfarande är tidigt ute i arbetet gällande informationssäkerhet och har inte arbetat sig runt hela varvet till kontroll, uppföljning och utvärdering. Kommunen är fortfarande bara i början av implementeringen i utbildning av säkerhet och därför finns det heller inget att följa upp och utvärdera. Både K2 och K5 säger att kontroll och uppföljning inte är deras starkaste del och därför blir arbetet gällande denna del sämre. Intervjuobjektet på K5 tycker personligen att arbetet går att göra mycket bättre. K2 tar dock upp att när det gäller kontroll och uppföljning angående de olika verksamhetssystemen så ligger ansvaret ute på varje förvaltning och inte under avdelningen för IT. Likt K5 tar intervjuobjektet för K2 upp: *"Men generellt vågar jag nog ändå hävda att där finns en del att göra. Det finns säkert inte framtagna rutiner överallt på hur saker och ting ska följas upp. Undantagsvis omsorgen, de är duktiga på det!"* (Bilaga 7.2.2, Rad 171-174).

Tre av kommunerna nämner även att deras arbete med kontroll och uppföljning inte startas förrän en eventuell incident inträffar. K3 erkänner att denne har för dålig koll för att egentligen besvara frågorna angående detta ämne, men tar upp att det finns kontroller inom datasystem och liknande, men inte inom informationssäkerhet. Kommunen utför inget arbete förrän någonting går fel. Likaså tar K5 upp att de enbart kontrollerar och följer upp om någon incident har inträffat, detta räknas dock inte som förebyggande arbete. Detta då K5 anser att om incidenten redan har inträffat så är det varken kontroll eller uppföljning, utan någonting de alltid utreder, men inte i ett förebyggande syfte. Sist tar K7 upp att de inte har något arbete riktat mot just informationssäkerhet som helhet. Intervjuobjektet säger *"[...] vi har ju ingen plan så för att följa upp informationssäkerheten, nä, det har vi inte."* (Bilaga 7.2.7, Rad 98-99) Likt K3 och K5 framgår det i citatet att K7 inte har någon plan att följa upp informationssäkerhetsarbetet utan arbetar efter incidenter.

Fyra utav de kommuner som intervjuades arbetar med kontroll och uppföljning fast med andra direktiv än enbart riktat mot informationssäkerhet. K1 använder sig utav en utbildning som kallas NanoLearning. Denna utbildning följs upp genom statistik som påvisar hur många som utfört utbildningarna osv. K1 följer upp denna statistik och intervjuobjektet säger *"[...] och det blir då en möjlighet att följa upp och kolla vad kan vi göra för att öka eller få förbättrade resultat och på så vis. Men det är bara på ett område."* (Bilaga 7.2.1, Rad 125-126). K5 använder sig utav interna kontroller som kollar upp behörigheten på de som är inloggade i deras system. Intervjuobjektet nämner även att det är svårt med kontroll och att deras medarbetare

verkligen följer redan utsatta riktlinjer. De anställda har skrivit under ett kontrakt där de lovat dyrt och hederligt att följa kommunens regler och riktlinjer. Mer än det anser K5 att de inte kan göra, förutom de interna kontrollerna som redan utförs. Intervjuobjektet uttrycker sig *"Och jag vet inte, alltså det ät jättesvårt att kontrollera det här. Att våra medarbetare verkligen följer det. Har de skrivit på ett papper och lovat dyrt och hederligt att de följer det, ja men då kan vi inte göra så mycket mer."* (Bilaga 7.2.5, Rad 117-119).

K6 kontrollerar enbart efterlevnaden genom att alla deras anställda ska ha genomgått utbildningen DISA, därefter nämner intervjuobjektet inte mer hur de arbetar med kontroll och uppföljning med informationssäkerheten i fokus. K7 har inget samlat begrepp om informationssäkerhet utan olika delar inom kommunen följs upp på olika sätt. Exempelvis så tar intervjuobjektet upp att IT-avdelningen följer upp och kontrollerar säkerheten gällande IT osv. Utöver detta har deras kommunarkivarie tillsyn över arkivering och dokumenthantering.

4.4 Övrigt

Avslutningsvis ställdes två frågor i slutet av intervjuerna för att få ut mer av intervjuobjektens egna åsikter och tankar kring informationssäkerhet. Den första frågan handlade om vilka de största utmaningarna kommunen i fråga står inför gällande informationssäkerhet. K1 tog upp att det fanns flera saker som denne såg som en utmaning. Den största utmaningen anser K1 vara att nå ut i organisationen. Detta menas med att de olika förvaltningarna har sitt eget kärnarbete och informationssäkerhet kan därför vara en liten del att förhålla sig till. K1 tog även upp att det är viktigt att få till en plan över hur kommunen kontinuerligt bör arbeta för att nå den punkt där det utförs kontroller och uppföljningar.

När frågan gällande den största utmaningen ställdes till K2 svarade intervjuobjektet *"Det tycker jag är... Att få fram ett lagom. Att hitta rätt ambition på vad vi ska göra."*(Bilaga 7.2.2, Rad 187). Med detta menar intervjuobjektet att arbetet angående informationssäkerhet kan göras jättestort, eller kan det ignoreras och väljas bort. K2 nämner även att det kan vara lätt att säga att en kommun sköter sig när det gäller informationssäkerhet. Att informationen klassificeras samt att riskanalyser utförs. Dock måste det finnas stöd i detta arbete, så kommunen är införstådd i vem som ska utföra vilket arbete. Därför krävs det även att en lagom ambitiös plan tas fram samt utbildning kring detta ämne utförs. Detta anser K2 vara en av de största utmaningarna. Intervjuobjektet tar även upp att arbetet bör starta med de små delarna för varje användare och uttrycker sig: *"Väldigt mycket intrång görs ju. Man kan ju hindra det med teknik och så, men den största anledningen, det är ju egentligen användaren själv som drar in saker och ting för att den inte vet att den inte ska klicka på det ena och det andra."* (Bilaga 7.2.2, Rad 204-206). Med detta sagt menar K2 att en av utmaningarna är att påverka slutanvändarna och avslutar med citatet *"Det spelar ingen roll hur stort, och långt och komplext lösenord du har om du ändå inte låser datorn när du lämnar den."* (Bilaga 7.2.2, Rad 214-215).

Likt K2 anser K4 att en av de största utmaningarna är att utbilda användarna så de är medvetna om hur de ska arbeta gällande informationssäkerhet. Detta inkluderar både att användarna ska veta vilket arbete som ska utföras samt vara införstådda i vilket arbete som krävs om någonting

blir fel. K4 nämner även att det är enkelt att skriva dokument, skapa policys och göra olika rutiner, men är inte slutanvändarna med på detta kommer resultatet bli lidande. Intervjuobjektet uttalar sig: *"Det är nog mer implementeringen ut i vardagsanvändandet som jag nog tycker är mest kritiskt."* (Bilaga 7.2.4, Rad 70-71).

K5 tar upp aspekten kontroll och efterlevnad som en av de största utmaningarna och nämner *"Och det spelar ju egentligen ingen roll hur mycket policys, och "vrobbar" och riktlinjer och det vi gör och de lovar, men ja. Nä, det är jättesvårt att följa upp det överhuvud taget, så det är största utmaningen. Definitivt."* (Bilaga 7.2.5, Rad 135-137). K6 går från slutanvändarnas perspektiv och tar upp ledningen som en av de största utmaningarna och att få med dem på banan. Intervjuobjektet tar upp att innan denne började arbeta på kommunen så bedrevs det inget systematiskt arbete överhuvudtaget med informationssäkerhet. Under de fem åren då intervjuobjektet varit anställd har de skaffat en plattform som inkluderar arbetet med just informationssäkerhet. Intervjuobjektet anser därför att kommunen kommit en bra bit på vägen, men att de inte är fullt medvetna om allt som kvarstår inom arbetet.

Även K7 går från perspektivet på slutanvändarna och anser att få de olika verksamheterna att avsätta den tid och resurser som krävs för att arbeta med informationssäkerhet är en av de största utmaningarna. Intervjuobjektet menar att det är svårt att hitta utrymme för att aktivt arbeta med de frågorna, samt att de som innefattar kompetens arbetar med andra område och har således inte tiden, och avslutar med *"Jag tror att viljan finns, men inte riktigt möjligheterna"* (Bilaga 7.2.7, Rad 109-110). K7 menar således att det finns mycket kommunen vill göra, men har inte resurser till det.

Vidare ställdes frågan hur den generella attityden hos de anställda gällande informationssäkerhet såg ut på kommunen. K1 ansåg att attityden är väldigt bra, men att kunskapsnivån i de flesta fall är väldigt låg och att användarna inte har tillräckligt hög medvetenhet. Dock om frågan väcks bland de anställda får K1 känslan att det är en diskussion som de är intresserade att medverka i. K1 trycker på att kunskapsnivån måste lyftas och således kommer även medvetenheten att växa och på så sätt se vilka behov som finns inom kommunen. Likt K1 nämner K4 att de anställda generellt är medvetna om informationssäkerhet, men att det fortfarande finns en stor okunskap. Denna okunskap faller under hanteringen av sekretess och känsligt material. K4 tar dock upp att det finns en stor förståelse hos de anställda, men att okunskapen tar över och uttrycker sig: *"Vi har, istället för att göra det komplicerat försökt göra metoden väldigt enkel"* (Bilaga 7.2.4, Rad 82-83).

K7 och K8 belyser även den positiva inställningen hos de anställda. K7 nämner att inställningen hos de anställda på kommunen är överlag positiv och att de anställda tycker informationssäkerhet är viktigt och att de vill göra rätt. Dock anser K7 att informationssäkerhet inte alltid prioriteras så som denne önskar. K8 tar således även upp att de anställda anser att arbetet med informationssäkerhet är viktigt och att medvetenheten finns, men att det saknas redskap för att hantera detta. Till skillnad från K7 och K8, anser K5 att den generella attityden på kommunen är negativ och säger *"Man tycker att ´det är ingenting man orkar lägga tid eller resurser på'"*

(Bilaga 7.2.5, Rad 140-141). Dock har en ny kommunchef anställts på den kommunen och sedan dess har attityden sakta börjat ändras och de anställda börjar inse hur viktig informationssäkerhet faktiskt är.

K6 tar upp att de tar lite väl lätt på informationssäkerhet. K6 menar att de har de anställdas ögon och öron och att de är öppna för ämnet men att det fortfarande finns saker som är svåra att hantera. K6 säger angående de anställdas inställning *”Ja, allmänt är det fortfarande lite väl beige och, men det är definitivt inte ointresse”* (Bilaga 7.2.6, Rad 67). Till sist tar K2 upp att inställningen hos deras anställda går att dela upp beroende på vilket perspektiv man kollar genom. De anställda genomgår en introduktionsutbildning där intervjuobjektet går genom arbetet gällande informationssäkerhet och har således en öppen dialog med de anställda. Då anser K2 att arbetet varken är stort eller svårt och att de anställda är väldigt engagerade och positiva att lära sig nya saker samt att de har även nytta av kunskapen privat.

Däremot anser K2 att det blir stort och svårt när det handlar om klassificering av information, genomförandet av riskanalyser och inte veta hur detta ska utföras. Överlag tror dock K2 att det inte är så stort och ansträngande på användarnivå. Intervjuobjektet nämner även att informationssäkerhet absolut kan vara tekniskt ibland, men att det i grunden inte är ett tekniskt ämne. K2 avslutar sedan med att säga *”[…] men det är ju mer sunt förnuft och man måste förstå, liksom lyfta olika scenarion så man får möjlighet att bara inse att ’jaha, gör jag bara såhär så skyddar jag faktiskt informationen bättre’”* (Bilaga 7.2.2, Rad 238-240). Med detta menar K2 att kommunen måste höja både medvetenhet och kunskap hos de anställda för att uppnå en så bra informationssäkerhet som möjligt.

4.5 Sammanfattning av resultat

	K1 (bilaga 7.2.1)	K2 (bilaga 7.2.2)	K3 (bilaga 7.2.3)	K4 (bilaga 7.2.4)	K5 (bilaga 7.2.5)	K6 (bilaga 7.2.6)	K7 (bilaga 7.2.7)	K8 (bilaga 7.2.8)
KONCEPT: POLICY OCH STYRANDE DOKUMENT								
Existens av policy beslutad av kommunstyrelsen	Ja, 2014 (r46)	Ja, 2013 (r83)	Ja, 2007 (r46)	Ja, 2017 *(inte beslutad, hoppas göras i maj)* (r32)	Ja, 2002; men gjordes en ny 2016 (r69-71)	Ja, 2015 (r15)	Ja, 2014 (r48)	Ja, 2016 (r25)
Policy reviderad?	Vid behov (r51)	Nej (r83)	Vet ej (r49)	Nej (r32)	2017 (revideras vart 3e år) (r70)	Vet ej	Nej (r48)	Oklart
Vem har utvecklat?	Säkerhetssamordnare (r43)	IT-chef (r80)	IT-kontoret (r52)	Säkerhetssamordnare (r36)	IT-samordnare/ Informationssäkerhetssamordnare (r65)	Informationssäkerhetssamordnare (r18)	Oklart: personen var projektanställd (r52)	Kommunarkivarie/Kommunjurist (r14-15)
Vem ansvarar?	Säkerhetssamordnarens avdelning (r54)	Otydligt (r85)	Oklart	Säkerhetssamordnare (r38)	IT-samordnare/ Informationssäkerhetssamordnare (r74)	Informationssäkerhetssamordnare (r18)	Kommunkansliet (r53)	Oklart (r28-29)
Hur arbetar kommunen för att de anställda ska vara införstådda med ISPn?	Mindre informationssäkerhetskampanjer. *(men dessa är inte till så stor hjälp för den enskilde användaren)* (r58-60)	En ISP som är anpassad för slutanvändare och en för högre ledning (r91-97)	Oklart, men intervjuobjektet har inte fått ta del av någon info (r57-61)	Fokuserar mer på dagliga användningen av informationssäkerhet än själva policyn (r42-43)	Policyn tas upp i chefsgruppen, således har varje chef ansvar att ta upp policyn på ett APT (r77-78)	Oklart	Ingenting, den finns bara (r58-59)	Ingenting just nu (r32)
KONCEPT: UTBILDNING OCH KOMPETENSUTVECKLING								
Utbildningsplan?	- DISA (r76) - NanoLearning (r85)	- NanoLearning (r128) - Introduktionskurs inom informationssäkerhet för nyanställda (r119)	Vet ej (r64-65)	Utbildat kommunens chefer (r50)	-DISA (r163) -NanoLearning (r31) -"Vrobbar" (r81)	- DISA (r34) - IIS (Internetstiftelsen i Sverige -Andra riktlinjer (r28)	-NanoLearning (r65)	Ingenting (r35)
Framtid?	Inget annat än NanoLearning. Vill höja säkerhetsnivån på bred front (r94-97)	Inget annat än det som redan finns (r143)	Vet ej (r69)	Utbilda cheferna mer, och förhoppningsvis webbutbildning för resterande anställda (r54-55)	Ingenting planerat förutom NanoLearning (r101)	Oklart	Inga planer just nu, förutom att utvärdera NanoLearning senare (r80-82)	Stort projekt till hösten som inkluderar utbildning (r56-57)
KONCEPT: KONTROLL OCH UPPFÖLJNING								
Arbete med kontroll och uppföljning?	Inte kommit dit än (r119)	Vågar hävda att det behövs göras ett o annat (r171-172)	Vet ej (r90)	Informationsklassificeringar (r59)	Det är faktiskt dåligt, men har intern-kontroller (r116)	Kontrollerar efterlevnaden av DISA (r33-34)	Ingenting riktat mot informationssäkerheten (r93)	Ingenting just nu (r37)
KONCEPT: ÖVRIGT								
Största utmaningen?	Ta fram en plan för att kunna arbeta med informationssäkerhet kontinuerligt (r134)	Att få fram ett "lagom", hitta rätt ambition (r187)	Informationen ut ska vara rätt och riktig (r97)	Implementeringen ut i vardags-användandet är mest kritiskt (r70)	Kontroll och efterlevnad (r133)	Att få ledningen på banan (r46)	Få de olika verksamheterna att avsätta tiden (r104-105)	Övergången till Google (r40)
Anställdas attityd	Bra, men kunskapsnivån låg (r140)	Engagerade, men ändå tveksamma när det blir för "stort och jobbigt" (r223-225)	Oklart	Det finns en stor okunskap (r74-75)	Generellt sätt dåligt då "man inte orkar lägga ned tid på det" (r140-141)	"Beige", men inte omtrisse (r67)	Generellt sett positivt – de vill göra rätt (r117-118)	"man tycker det är viktigt" (r50)

Tabell 3. Sammanfattning av resultat

5 Analys och diskussion

I denna del kommer resultatet av den empiriska data som samlats in analyseras och diskuteras och vidare kopplas till de teorierna som presenterats tidigare i uppsatsen.

Likt det teoretiska ramverket som redovisades under § 2.7 behöver en anställd enligt Conner och Patterson (1982) gå genom tre steg under en organisatorisk förändring innan denne rättar sig efter förändringen i fråga. Dessa tre steg jämförs i det teoretiska ramverket under § 2.7 med uppsatsens tre huvuddelar; *policy & styrdokument*, *utbildning & kompetensutveckling* och *kontroll & uppföljning*.

5.1 Policy och styrande dokument

För att uppnå det första steget i en organisatorisk förändring krävs enligt Conner och Patterson (1982) preparation, som jämförs med policy och styrdokument i det teoretiska ramverket (§2.5).

Enligt Höne och Eloff (2002) är en ISP en av de viktigaste kontrollerna när det kommer till informationssäkerhet och detta är något som samtliga kommuner har anammat, då alla har en ISP på kommunen. Whitman et al. (2001) menar att organisationens syfte med skapandet av en ISP bör vara att förse de anställda med riktlinjer som syftar till att säkerställa informationssäkerhet. I enlighet med författarna skapade bland annat K6 allmänna riktlinjer för informationssäkerhetsarbetet i samband med utformandet av policyn för att tydliggöra dem ytterligare.

Vidare hävdar LeVeque (2006) att en organisation kan ha flera policys med olika tillämpningsområden. Likt Leveque (2006) har K2 delat upp sin ISP i två olika delar, där den ena är på en mer övergripande nivå och främst anpassad för chefer, medan den andra är mer riktad till användarna. Detta ligger i linje med det LeVeque (2006) menar är optimalt då författaren påstår att det ska finnas en policy som lämpar sig till ledningen och en som beskriver dagligt systemanvändande för slutanvändarna. En kommun som ställer sig i motsats till detta är K1 som beskriver att deras ISP skrevs på en väldigt hög nivå, och därmed inte är till hjälp för den enskilde användaren. Denna utformning kan, enligt LeVeque (2006), vara missgynnande då tekniska och administrativa sammanhang skall skiljas åt.

Gällande utformandet av policyn och vem som bör utforma den, menar Layton (2005) att en ISP helst inte skall utformas utav IT-avdelningen eftersom det ger policyn en teknisk synvinkel och därmed inte lämpar sig till slutanvändarna som kanske inte är lika tekniska. Kommuner har som tidigare nämnt ansvar för en stor del av samhällsservicen, vilket innebär att de är beroende av information och IT-stöd för att bedriva sin verksamhet. I och med digitaliseringen ökar behovet av informationssäkerhet hos den offentliga sektorn (Thorslund, 2017). De anställda på kommunen ansvarar för allt från omsorg av äldre till att säkerställa att känslig infrastruktur fungerar (Goede, 2017) och med dessa olika utbildningsbakgrunder hos de anställda måste policyn vara lättförståelig för såväl en förskollärare, till en medarbetare på IT-avdelningen.

I linje med vad Layton (2005) hävdar, bör en IT-avdelning således inte utforma ISP, eftersom den då tenderar att bli för teknisk för den otekniske slutanvändaren. I tabellen (Tabell 3) från resultat framgår det att minst tre kommuner låtit sin ISP utvecklas utav en anställd från IT-avdelningen, vilket kan leda att policyn i fråga har fått en för teknisk vinkel. Intressant är dock att K3, som är en av de kommuner som låtit sin IT-avdelning utforma deras ISP, är medvetna om problematiken som Layton (2005) påpekar angående vem som utformar en ISP. K3 menar att informationssäkerhet tillhör mer än bara de tekniska aspekterna. Detta påstående ligger i linje med Gonzalez och Sawicka (2002) som menar på att informationssäkerhet inkluderar både teknologi och människor. Vidare menar författarna att den mänskliga faktorn är en svag länk inom informationssäkerhet om den inte handskas med på rätt sätt. I motsats till detta menar Bulgurcu et al. (2010) att de anställda även kan vara den största tillgången gällande att minska riskerna relaterade till den mänskliga faktorn av informationssäkerhet. Därför borde kommunerna se över vem som utformar kommunens ISP, så att denna inte bara är anpassad efter ledningen eller de mest tekniska användarna, utan även den potentiellt otekniske slutanvändaren.

För att vidare kunna arbeta med utformningen och anpassningen av policyn till de anställda är revidering en vital del. Detta för att en organisations policy ska vara uppdaterad och uppnå de krav som ställs. Likt detta belyser Höne och Eloff (2002) att det är vitalt att en ISP är skräddarsydd efter organisationskulturen. För att uppnå detta bör revidering av policyn utföras. Arbetet gällande revidering inom kommunerna skiljer sig åt beroende på hur de arbetar med informationssäkerhet. Fem av åtta kommuner hade inte kunskap angående när deras ISP revideras eller under vilka förutsättningar. Dock nämner K7 att deras ISP är i stort behov av en uppdatering och är således inte skräddarsydd efter organisationskulturen som Höne och Eloff (2002) belyser är vitalt. Skilt från de andra kommunerna reviderar K5 sin ISP var tredje år för att ständigt vara uppdaterade och anpassade till organisationen.

Gällande arbetet med att få de anställda införstådda med kommunens ISP anger fyra kommuner att de inte arbetar med att få de anställda införstådda i policyn, vilket kan vara problematiskt då Höne och Eloff (2002) hävdar att anställda är ignoranta mot sin organisations ISP för att de inte förstår den till fullo. Detta ignoranta beteende menar författarna kan motverkas genom att skapa en mer effektiv ISP som hjälper användarna att förstå vad som är acceptabelt och vilket ansvar de har gentemot informationssäkerhet. K1 arbetar som tidigare nämnt med mindre informationssäkerhetskampanjer relaterade till kommunens ISP, vilket troligtvis kan motverka användarnas ignorans mot kommunens ISP eftersom användarna då förstår att informationssäkerhet inte är negativt och ansträngande (Höne & Eloff, 2002). K7 tar upp att deras ISP enbart existerar och att det således inte finns mer bakomliggande arbete. Detta går inte i linje med Whitman och Mattord (2008) som menar på att en policy ska bidra till organisationens framgång, både genom ledningens samt slutanvändarnas involvering.

K4 fokuserar inte allt för mycket på deras ISP, utan riktar arbetet mer på den dagliga användningen och hanteringen av informationssäkerhet. Martins och Elofe (2002) belyser att en policy bör diktera de anställdas beteende och fastställa vad som förväntas av dessa, vilket i sin tur blir en del av det dagliga arbetet. Likt vad författarna förespråkar, arbetar K4 med att involvera

informationssäkerhet i det dagliga arbetet, men de bör även inkludera information kring sin ISP för att öka medvetenheten hos de anställda ytterligare.

5.2 Utbildning och kompetensutveckling

I enlighet med Conner och Patterson (1982) är det andra steget i processen att få en anställd att rätta sig efter en organisatorisk förändring (awareness). Detta steg kopplas i det teoretiska ramverket (§2.7) till utbildning och kompetensutveckling.

Amankwa et al. (2015) hävdar att den mest kritiska aspekten när det kommer till att skydda känslig information inom organisationer är utbildning och medvetenhet. Detta ligger i linje med vad Conner och Patterson (1982) hävdar vara det andra steget gällande att få en anställd att acceptera en organisatorisk förändring (awareness). För att en anställd ska förstå organisationens ISP och rutiner, samt för att denne ska ha tillräckligt med kunskap gällande de olika kontroller som krävs för att skydda organisationens resurser krävs utbildning för de anställda (Dewey & Shaffer, 2016). Enligt Siponen (2000) ska ökad medvetenhet hos de anställda minimera användarrelaterade misstag samt upphäva dessa i teorin. Detta leder även till maximerad effekt hos en organisations säkerhetstekniker och processer ur ett användarperspektiv. För att uppnå en så hög medvetenhet som möjligt för de anställda och att öka kunskapen arbetar kommunerna på olika sätt.

Tre kommuner erbjuder DISA som utbildningsverktyg och fyra kommuner anger att de använder sig utav NanoLearning. Dessa verktyg kan jämföras med ISA Program då Thomson och Von Solms (1998) menar att ISA Program används för att utbilda de anställda gällande informationssäkerhetsfrågor, samtidigt som det hela tiden påminner de anställda om pågående samt nya problem kopplade till informationssäkerhet. NanoLearning är uppbyggd som så att användaren ska få relevant information angående olika situationer, utmaningar och möjligheter kopplat till informationssäkerhet (Olofsson, 2016). Denna utbildning ligger därmed i linje med vad Thomson och von Solms (1998) hävdar är kriterium för ISA Program. De menar att målet med ett ISA program är att ändra de anställdas idéer och beteende gentemot informationssäkerhet. Det är därför vitalt att användarnas beteende och attityd modifieras så att deras handlingar är säkerhetsmedvetna. För att lyckas med ovanstående menar Junglemap (2017a) att lärandet ska fungera som en process istället för ett enskilt event och därmed bestå av olika typer av analyser, undersökningar, reflektionsövningar och kunskapstester. I motsats till vad Junglemap (2017a) hävdar gällande att se inlärningen som en process, så erbjuder K2 en introduktionsdag, likt ett event, inom informationssäkerhet för alla nyanställda. Detta är ett enskilt event som inte gynnar det systematiska informationsäkerhetstänket. Dock är K2 är en av kommunerna som både erbjuder DISA och Junglemap som ISA program, vilket kompenserar detta enstaka event. Hade de enbart erbjudit ett introduktionsevent inom informationssäkerhet hade det varit annorlunda, men i K2s fall bör eventet endast ses som en bonus som främjar informationssäkerhetsarbetet. Användningen av DISA som ISA Program verkar detta inte fylla samma funktion som NanoLearning, då K5 bland annat säger att den inkluderar "stenåldersfrågor". Vidare menar K1 att DISA inte bör kallas för en utbildning, då den snarare syftar till att höja medvetenheten.

De kommuner som erbjuder utbildning till sina anställda har större chans att uppnå hög ISA inom organisationen. Enligt Siponen (2000) används termen ISA för att referera till det stadiet då alla användarna i en organisation är både medvetna och fullt engagerade i informationssäkerhetsarbetet. För att uppnå detta krävs det enligt Martins och Elofe (2002) medvetenhet hos de anställda, vilket uppnås genom utbildning och träning. De kommuner som erbjuder utbildning har således större chans att uppnå hög ISA. En kommun som enbart arbetar begränsat med utbildning är K4. De erbjuder enstaka event som enbart är till för att utbilda cheferna. Detta motsäger termen ISA och det som Siponen (2000) samt Martins och Elofe (2000) belyser. K4 uppnår således inte hög ISA inom organisationen vilket kan skada organisationen genom att de anställda fattar felaktiga beslut, vilket enligt Thomson et al. (2006) är ett av de största hoten för en lyckad informationssäkerhet.

Alla kommuner förutom två anger att det inte finns några specifika framtidsplaner kopplade till utbildning och kompetensutveckling. Ovanstående beror enligt K5 på att den nya dataskyddsförordningen, GDPR, som införs i maj 2018 (Datainspektionen, 2017a). Intervjuobjektet menar på att de på kommunen måste lägga resurser på utbildning inom dataskyddsförordningen, vilket leder till att andra frågor inom informationssäkerhet hamnar i bakgrunden. Detta ligger även i linje med K7 som menar på att deras fokus förflyttats till att skicka berörda parter på kurser inom den nya dataskyddsförordningen istället för att utbilda de anställda generellt inom informationssäkerhet. Thomson et al. (2006) belyser att ett av de största hoten för en lyckad informationssäkerhet inom en organisation är de felaktiga beteendet hos de anställda när de hanterar information. På grund av ovanstående finns det grund till att utbilda sina anställda inom GDPR också, men att utesluta den allmänna utbildningen inom informationssäkerhet kan vara en risk då Thomson et al. (2006) menar att anställda måste bli utbildade och integrerade i informationssäkerheten i sitt dagliga arbete.

Om utbildningen hamnar på is under en period riskerar kommuner att inte uppnå hög ISA. Detta kan således riskera att de processer de anställda arbetar med i sitt dagliga arbete blir lidande och Thomson et al. (2006) belyser att detta enbart går att skyddas mot genom utbildning av anställda och att integrera dem i informationssäkerhetsarbetet.

5.3 Kontroll och uppföljning

Det sista steget en anställd måste gå igenom innan denne rättar sig efter förändringen är commitment (Conner & Patterson, 1982). I det teoretiska ramverket (§2.7) är detta steg kopplat till kontroll och uppföljning. Detta steg syftar både på att de anställda måste förstå och anpassa sig efter de policys som finns inom organisationen, samt arbeta vidare med informationssäkerheten i form av kontroll och uppföljning.

Arbetet med kontroll och uppföljning är näst intill icke-existerande hos de åtta kommunerna, då det enbart är en kommun som med säkerhet kunde säga att de arbetar med kontroll och uppföljning av informationssäkerhet. Enligt MSB (2015) är kontroll och uppföljning en nödvändig förutsättning för att organisationer ska kunna arbeta löpande med informationssäkerhet. Eventuella hot och risker ska kunna utvärderas så att åtgärder kan tas för att undvika skador

mot organisationen. Tre av kommunerna nämner att deras arbete gällande kontroll och uppföljning enbart startar när en eventuell incident inträffar. Detta motsäger det MSB (2015) belyser med att en organisation bör utvärdera eventuella risker och hot innan de inträffar. Dock belyser MSB (2016) att en organisation kan hantera de olika risker och incidenter som de dagligen utstår genom användandet av en incidenthanteringmodell. Detta var dock inget kommunerna hade kunskap om och generellt sett arbetar därför enbart efter eventuella incidenter inträffat.

I linje med MSB (2016) som menar att organisationer måste kunna bedriva sin verksamhet även i en riskfylld miljö arbetar K4 med kontroll och uppföljning genom informationsklassificeringar. Detta innebär att K4 utför klassificeringar för att identifiera vad som behövs åtgärdas, vilket är en hel del. De tar även upp att de faktorer som behöver åtgärdas analyseras för att identifiera hur saker och ting blir gjorda samt hur detta fungerar i praktiken. MSB (2016) belyser även att det är vitalt att kontinuerligt planera säkerhetsarbetet, vilket K4 utför genom regelbundna klassificeringar. I dagsläget sker detta arbetet manuellt, men ska till sommaren automatiseras och kunna följas genom ledningssystemet. MSB (2016) tar upp att en central del i arbetet gällande uppföljning är ledningens utvärdering. Detta innebär att ledningen utför rapporter för att analysera hur arbetet med utvärdering och kontroll utförs. Även om K4 inte är där ännu är de på god väg dit.

De kommuner som inte arbetar med kontroll och uppföljning riskerar sitt arbete gällande informationssäkerhet. Enligt MSB (2015) är det vitalt att arbetet följs upp för att en organisation ska kunna arbeta löpande med informationssäkerhet. Denna undersökning visar dock på att enbart en kommun följer de riktlinjer som finns gällande kontroll och uppföljning och att de andra sju inte är där ännu.

5.4 Övrigt

Avslutningsvis ställdes två frågor i intervjuerna som inkluderade största utmaningen inom informationssäkerhet samt den generella inställningen hos de anställda gällande informationssäkerhet. Angående den största utmaningen tog K2 upp att det är knepigt att få fram ett "lagom" och att hitta rätt ambition på arbetet. Objektet nämner att det kan vara enkelt för en kommun att säga att de sköter sig gällande informationssäkerhet, dock måste det finnas stöd och förståelse för att utföra arbetet. Wylder (2003) belyser tre grundläggande principer som är sammankopplade för att organisationer ska förstå innebörden av informationssäkerhet. Dessa tre element är konfidentialitet, integritet och tillgänglighet - även känd som CIA-triaden. K2 nämner även att arbetet bör starta med de små delarna för varje användare och uttrycker sig att incidenter kan hindras med teknik, men att den största anledningen till eventuella fel i arbetet är användarnas handlingar. Detta går i linje med CIA-triaden där Agarwal och Agarwal (2011) belyser att dessa tre principer är sammankopplade med informationssäkerhet. Alla tre delar går att direkt koppla till den mänskliga faktorn då de sammanfattar de aspekter som inkluderar att information ska skyddas från obehöriga, att informationen ska vara korrekt samt tillgänglig för behöriga. Alla dessa faktorer kan äventyras på grund av den mänskliga faktorn och stämmer således överens med K2s oro gällande användarnas handlingar. Är kommunen införstådd med de tre elementen

i CIA-triaden och utbildar de anställda inom det ökar chansen att utesluta att användarnas handlingar blir skadliga för organisationen.

Likt K2, anser K4 att en av de största utmaningarna är att utbilda användarna så de är medvetna om hur de ska arbeta gällande informationssäkerhet och uttrycker sig att implementeringen ut i vardagsanvändandet är det mest kritiska. Gonzalez och Sawicka (2002) belyser att alla säkerhetssystem, oavsett hur välformade och genomförda de är, måste lita på användarna. Den mänskliga faktorn spelar stor roll i flertal olyckor relaterade till informationssäkerheten och organisationer måste därför lära sig hantera den mänskliga faktorn. Detta bevisar både K2s och K4s oro gällande slutanvändarna och att detta är ett problem många organisationer står inför. För att en organisation ska kunna arbeta sig vidare från perspektivet att den mänskliga faktorn är ett hot mot säkerhet bör de enligt Bulgurcu et al. (2010) se de anställda som den största tillgången gällande att minska riskerna relaterade till ämnet. En organisation måste således dra nytta av den mänskliga kapaciteten istället för att göra motsatsen.

Ovanstående kan dock vara problematisk inom organisationer beroende på hur de anställdas inställningar mot informationssäkerhet ser ut. Majoriteten av kommunerna antydde att inställningen hos deras anställda generellt är väldigt bra, men att kunskapsnivån i de flesta fall är för låg. K7 tar dock upp att informationssäkerhet inte alltid prioriteras så som denne önskar. K8 nämner att det saknas redskap för att hantera problemet med kunskap och medvetenhet, vilket stämmer överens med både K1 samt K4. Som tidigare nämnt ökar en användares kunskap genom utbildning och träning (Martins och Elofe, 2002). Författarna belyser även att de anställdas beteende måste modifieras till den grad att de kan arbeta med deras dagliga arbetsuppgifter med ett säkerhetstänk. Detta bevisar att det inte är de anställdas problem att kunskapen inte finns, deras inställning bevisar att ämnet intresserar dem men att utbildningen måste förbättras för att få in tänket i det dagliga arbetet.

Skilt från vad Martins och Elofe (2002) belyser angående att modifiera inställningen hos den anställde, tar K5 upp att den generella attityden på kommunen är negativ. K5 uttrycker att det inte är någonting som organisationen lägger tid eller resurser på. Detta innebär även att de anställda inte följer det som Thomson och von Solms (1998) belyser genom att den anställdes beteende ska fungera omedvetet under hela arbetsprocessen genom att alltid tänka ur ett säkerhetsperspektiv oavsett vilka uppgifter de utför. Att införa informationssäkerhet som en del av organisationskulturen är enligt Martins och Elofe (2002) ingen enkel uppgift och kan ta upp mot flera år. Ett vitalt steg är därför att ha de anställdas acceptans och vilja på organisationens sida, vilket majoriteten av kommunerna ändå har då de flesta anger att attityden mot informationssäkerhet generellt sett är positiv.

6 Slutsats

Detta kapitel presenterar slutsatserna som kommit fram under analys & diskussion. Vidare presenterar även framtida forskningsmöjligheter relaterade till ämnet.

Forskningsfrågan som ställdes inledningsvis var:

- *Hur arbetar kommuner med informationssäkerhet utifrån den mänskliga faktorn i fokus?*

Till att börja med har kommunerna som intervjuats i denna studie, generellt sett, inte arbetat systematiskt med informationssäkerhet särskilt länge. Denna slutsats dras genom vetskapen av att flera kommuner själva nämnt att de ser informationssäkerhet som en relativt ny fråga. Dessutom är det flera kommuner som fortfarande inte har en utsedd person på kommunen som specifikt har exempelvis rollen informationssäkerhetssamordnare. Inom vissa kommuner är arbetet med informationssäkerhet något som beskrivs enligt följande: *”[...]och därför är jag involverad under tiden tills det utses någon som skall ha det ansvaret så har jag ryckt in och driver detta litegrann då jag tycker att frågan är viktig och då hjälper jag till med den.”* (Bilaga 7.2.2, Rad 44-46). Vidare nämner ett annat intervjuobjekt*: ”Jag tror att det kommer förändras, alltså kommunerna har ju klarat sig ganska lindrigt undan om man kollar på de krav som finns, alltså lite tuffare krav.”* (Bilaga 7.2.1, Rad 158-159).

För att kommuner ska kunna arbeta systematiskt med informationssäkerhet med den mänskliga faktorn i fokus krävs det att kommunen tillämpar de tre steg som Conner och Patterson (1982) menar på att en anställd måste gå igenom innan denne anpassar sig efter en organisatorisk förändring. Dessa tre steg sammanfattas som *preparation*, *awareness* och *commitment*, som i denna uppsats kopplats samman med tre områden i MSB:s enkätundersökning från 2015. Dessa tre områden är, som tidigare nämnt: *policy och styrande dokument, utbildning och kompetensutveckling*, samt *kontroll och uppföljning*. Kommunerna behöver således ta sig igenom alla dessa tre steg för att slutligen nå den fasen då den anställde är rättar sig efter förändringen i fråga.

När det kommer till arbetet med policy och styrande dokument (preparation) behöver kommunerna ha i åtanke att enbart en ISP inte är nog såvida den inte är anpassad för hela organisationen. Det första steget som behöver tas är skapandet av flera ISP, anpassade till olika delar av organisationen. Vidare bör dessa vara anpassade efter olika kunskapsnivåer och inte bara ha en teknisk vinkel. Således räcker det inte att en ISP finns, utan kommunerna bör arbeta med att göra de anställda införstådda med den. Gällande utbildning och kompetensutveckling som står för nästa steg (awareness) arbetar många kommuner med ISA Program. Däremot är det flera kommuner som hävdar att de inte alls arbetar med utbildning för de anställda, inom informationssäkerhet. För att uppnå en hög ISA och därmed minska misstag relaterade till användaren krävs utbildning för de anställda oavsett kunskapsnivå.

Det sista steget, kontroll och uppföljning (commitment), är något som kommunerna generellt sett inte arbetar med. Kommunerna måste kunna bedriva sin verksamhet även i en riskfylld miljö för att således kunna uppnå hög informationssäkerhet. För att uppnå detta krävs det inte enbart att kommunens anställda är införstådda med deras ISP och har rätt utbildning, de måste även vara engagerade. Detta uppnår kommuner genom att arbeta kontinuerligt med uppföljning av arbetet gällande informationssäkerhet, och inte bara vid särskilda incidenter.

Avslutningsvis kan det tyckas att denna studie genomförts med en dålig timing då många kommuner vänt sitt fokus till att anpassa sig efter den nya dataskyddsförordningen som träder i kraft i maj 2018. Flera kommuner menar att denna går i första hand just nu, vilket har gjort att det dagliga arbetet med informationssäkerhet hamnat i skymundan. Detta har en negativ påverkan eftersom arbetet med informationssäkerhet bör ses som en ständig process. Kommuner bör därför sträva efter att arbeta med informationssäkerhet kontinuerligt, med den mänskliga faktorn i fokus, istället för att se informationssäkerhetsarbetet som ett tillfälligt projekt.

6.1 Framtida forskningsmöjligheter

Uppsatsen har enbart utgått från åtta kommuner i Sverige, där samtliga intervjuobjekt haft relevant koppling till informationssäkerhet i deras roll på kommunen. Framtida forskningsmöjligheter kan därför vara att intervjua anställda på kommuner med mindre kunskap om ämnet, som i sin tur kan ge målande svar på hur medvetna de är om informationssäkerhet. Att höra med de anställda skulle ge ett annat perspektiv på frågeställningen. Således skulle forskningsfrågan kunna vara:

- Hur upplever de anställda på kommuner att de jobbar med informationssäkerhet?

7. Bilagor

7.1 Intervjuguide

Bakgrund

1. Berätta kort om din roll inom kommunen
2. Hur involverad är du i informationssäkerhetsarbetet?
3. Hur upplever du att Ni arbetar med informationssäkerhet på Er kommun?
4. Har Ni varit en del av MSB:s enkätundersökning: En bild av kommunernas informationssäkerhetsarbete, 2015?
5. Har du tagit del av resultatet från ovanstående undersökning?

Policy och styrande dokument

6. Har Ni etablerat en informationssäkerhetspolicy?
7. Vem eller vilken del av organisationen har i så fall utvecklat denna?
8. När skapades denna och när reviderades den senast?
9. Vem eller vilka är ansvarig(a) för policyn?
10. Hur arbetar Ni på kommunen för att Era anställda skall vara införstådda med er informationssäkerhetspolicy?
11. Hur har resultatet av MSB:s undersökning förändrat ert arbete gällande policy och styrande dokument?

Utbildning och kompetensutveckling

12. Hur arbetar ni med utbildning och kompetensutveckling för Era anställda?
13. Hur ser er generella utbildningsplan ut inom kommunen, och när sker denna utbildning?
14. Hur ser framtiden ut gällande utbildningsarbeten på Er kommun?
15. Hur har resultatet av MSB:s undersökning förändrat ert arbete gällande utbildning av anställda inom informationssäkerhet?
16. Enligt MSB:s enkätundersökning var det 136 stycken kommuner som inte erbjuder utbildning inom informationssäkerhet till sina anställda. Var ni en av dessa kommuner?

Kontroll och uppföljning

17. Hur arbetar Ni med kontroll och uppföljning?
18. Hur har resultatet av MSB:s undersökning förändrat ert arbete gällande kontroll och uppföljning?

Avslutande frågor

19. Vad upplever du är den största utmaningen när det kommer till arbetet med informationssäkerhet på kommunen?
20. Hur anser du att den generella attityden mot informationssäkerhet är hos de anställda på kommunen?

7.2 Transkribering

7.2.1 Transkribering av intervju: Kommun 1 (K1)

Datum: 2017-04-28 13:00
Intervjuobjekt: K1
Intervjuare: S (Sofia Söderström)
Metod: Telefonintervju, inspelning av intervjun och transkribering efteråt.

K1: Hallåja!
S: Ja hejsan, är det xx?
K1: Ja det stämmer det!
S: Perfekt, hej jag heter Sofia och du har haft kontakt med Nelly Karlsson Åhlén på mejl angående vår kandidatuppsats.
K1: Jajamensan!
S: Vi är väldigt glada att du vill medverka på en intervju det är jätteroligt.
K1: Ja det tycker jag med!
S: Ja vad roligt. Har du någon fråga innan vi startar eller ska jag bara köra igång?
K1: Vi kan tuta och köra faktiskt, ni får styra och ställa så försöker jag hjälpa er så gott det går.
S: Ja men perfekt! Kan du berätta lite kort om din roll inom kommunen först?
K1: Ehm, jag jobbar som säkerhetssamordnare. Och vi är tre stycken totalt inom xx kommun. En utav oss jobbar med krishantering kan man väl säga och en jobbar med det förebyggande och sen jobbar jag egentligen med all övrig säkerhet och där är informationssäkerhet en del utav arbetet.
S: Okej, hur involverad är du då i just informationssäkerhetsarbetet?
K1: Ja tyvärr är jag nog den som mer eller mindre driver det arbetet idag.
S: Hur upplever du att ni arbetar med informationssäkerhet på er kommun?
K1: Vi ligger i startgroparna kan jag ju säga, på flera fronter. Jag anställdes här för 3,5 år sedan och jag anställdes egentligen för kompetensen med informationssäkerhet, så att aktivt har vi inte jobbat med mer än kanske, ah lite drygt 3-3,5 år.
S: Vi skickade ju även med MSBs enkätundersökning ”En bild av kommunernas informationssäkerhetsarbete 2015”. Var ni en del av den undersökningen?
K1: Jaa
S: Så ni var en av de kommunerna som besvarade frågorna?
K1: Ja
S: Har du i efterhand tagit del av resultatet?
K1: Ja, jag tog faktiskt… När ni påminde mig här hade jag glömt bort den nu men jag har läst den förut, men jag ögnade igenom det igår lite och drog mig till minnes lite.
S: Okej! Intervjun kommer vara så att vi har tre huvuddelar med lite frågor och första delarna handlar om policy och styrande dokument. Har ni etablerat en informationssäkerhetspolicy inom kommunen?
K1: Ja, det var faktiskt bland de första uppgifterna jag gjorde här när jag började.
S: Vem eller vilken del av organisationen har utvecklat, är det du då?
K1: Ja egentligen är det jag personligen, och jag jobbar alltså på kommunledningskontoret i kommunen. Alltså inom kommunstyrelsen, alltså central förvaltning kan man säga.
S: Skapades policyn för 3,5 år sen då eller?
K1: 2014 var den godkänd, jag kommer inte ihåg vilken månad men 2014 klubbades den igenom i kommunfullmäktige.
S: När reviderade ni den senast?

K1: Vi har en dokumentationsplan så att säga så att min, våran enhet här heter trygg- och säkerhetsenheten. Och vi ansvarar för ett antal dokument, så vi går igenom dom dokumentet en gång per år. Och i policyn så är det skrivet att den ska gås igenom eller revideras vid behov om någonting har hänt.

S: Nu i efterhand, vem är det då som är ansvarig för policyn?

K1: Själva dokumentet är våran enhet ansvarig för även om innehållet i sig är kommunfullmäktige i kommunstyrelsen. Men dokumentet är vi ansvariga för att hantera.

S: Hur arbetar ni i kommunen för att era anställda också ska vara införstådda med policyn?

K1: Ja vi har haft mindre informationskampanjer i början. Men policyn i sig skrevs ju på en väldigt hög nivå så att det är ju egentligen inte en större hjälp för den enskilde medarbetaren och det var inte syftet med den heller. Utan den skrev i mångt och mycket för att våran avdelning skulle få mandat att jobba med frågorna ute i förvaltningarna. Så därför togs den fram, men vi kommer lite längre fram nu in på den utbildning så då kommer den upp igen här att den ska marknadsföras lite mer men inget så att man kan få så mycket dagligt stöd i den utan egentligen för att förvaltningschefen ska bli mer införstådd vad dom har för antagande på en högre nivå så att säga.

S: Okej, som en slutfråga i detta avsnitt. Har resultatet av MSB:s undersökning förändrat ert arbete gällande policyn?

K1: Nej.

S: Nej, utan den är som vanligt?

K1: Aaa.

S: Andra delen då om utbildning och kompetensutveckling. I dagsläget, hur arbetar ni med utbildning och kompetensutveckling för era anställda?

K1: Ja man kan titta lite på vad vi har gjort centralt. Det är inte jättemycket men jag tror att från och med 2014 då införde vi en process att när man har sitt personliga samtal med chefen, alltså utvecklingssamtal eller liknande då skulle man ha med sig ett diplom från en kurs som MSB låg bakom, DISA.

S: Ja, den har vi hört talas om.

K1: Ja, och då skulle man alltså gå in och ha gjort det här testet, det är ett ganska så enkelt och då kan man trycka ut ett diplom och det skulle man ha med sig till sitt utvecklingssamtal som ett bevis på att man i alla fall en gång om året hade genomfört någon form utav, jag ska väl inte säga utbildning, för DISA är väl mera för att höja medvetandet i alla fall. Sen vad det gäller kompetensutveckling, det har inte skett så mycket från centralt håll utan det har nog förvaltningar och enheter gjort i den mån dom har velat. Men dit har vi inte nått, att kunna driva något centralt egentligen. Än så länge, förens faktiskt nu när vi började ett annat verktyg som heter NanoLearning.

S: Hade du kunnat berätta lite mer om det verktyget?

K1: NanoLearning är ett utbildningsverktyg som samtliga medarbetare får via ett mejl en gång i veckan. Och då är det en utbildning eller en kort kurs mellan 2–4 minuter i ett specifikt ämne. Det här verktygen äger vi själva egentligen så att vi har full kontroll över både hur vi skapar våra lektioner men vi kan också följa kurserna som genomförs i realtid vilket gör att vi får en väldigt bra statistik att följa upp framöver.

S: Är det detta ni satsar på i framtiden eller hur ser framtiden ut gällande utbildningsarbetet?

K1: Ja precis, det här är våran handlingsplan så att säga att på bred front höja säkerhetsnivån och framförallt försöka förändra ett beteende på lång sikt, för det tar tid. Och enda sättet för oss att göra det som vi har tänkt och så, det är därför vi fastnade men det, att man får en påminnelse en gång i veckan. Även om det är olika ämnen varje gång så blir man påmind att

"gör det", eller "gör inte så" eller "tänk såhär" eller" har du tänkt på det här?". Detta påminner dem om att få in informationssäkerhetstänket i ryggraden. Alltså att man har med sig det när man kanske är ute och surfar eller hur man hanterar sin information eller vad man nu gör. Att få in det här tänket att man alltid tänker efter lite.

S: Lite nyfiken, enligt MSB:s enkätundersökning så var det 136 stycken kommuner som inte erbjuder utbildning inom informationssäkerhet till sina anställda. Var ni en av dem?

K1: Nej vi körde Disa då!

S: Tycker du att ni har ändrat ert arbetssätt gällande utbildning av anställda efter undersökningen?

K1: Nej, och generellt så kan jag väl säga att jag inte tror att vi har förändrat någonting i och med resultatet som kom ut. Jag kan väl inte påstå att vi är så styrda av vad alla andra gör utan vi har nog försökt haft ett eget tänk vart vi vill så det var väl mer att ha som en reflektion till kanske hur man står sig förhållande till andra. Det var inte sätt för oss att vi skulle göra några större förändringar.

S: Okej! Då går vi in på sista delen som handlar om kontroll och uppföljning. Hur arbetar ni med kontroll och uppföljning?

K1: Ja du menar inom informationssäkerhet förstår jag?

S: Ja precis. Mer om ni kanske har utvärderingar, där ni utvärderar arbetet, eller väntar ni till någon incident inträffar eller har ni kontinuerligt arbete där ni kontrollerar att informationssäkerheten fungerar så ultimat som möjligt?

K1: Nä, jag tror att eftersom vi är ganska så tidigt ute i startblocket ändå att börja jobba med det så har vi liksom inte egentligen kommit varvet runt till just kontroll, uppföljning och utvärdering osv utan vi är början i cirkeln av implementering och utbildning och allt det här så jag tror att vi har liksom ingenting att följa upp och utvärdera än om jag ska vara ärlig. Utan det blir till exempel om man tar det här verktygen med NanoLearning så kommer statistik på hur många procent som har genomfört vissa utbildningar, detta kan man göra kvartalsvis eller hur man vill, och det blir då en möjlighet att följa upp och kolla vad kan vi göra för att öka eller få förbättrade resultat och på så vis. Men det är bara på ett område.

S: Toppen. Har då arbetet förändrats efter MSB:s undersökning?

K1: Nej.

S: Lite avslutande frågor. Vad upplever du är den största utmaningen när det kommer till arbetet med informationssäkerhet?

K1: Jaa, det är väl flera saker egentligen. Om jag pratar från en kommunal nivå så är det ju alltid svårt att nå ut i organisationen eftersom dom olika förvaltningar har sitt kärnarbete och då är kanske informationssäkerhet en liten del av deras arbete att förhålla sig till. Så att jag tror att få till en plan hur man ska arbeta med det kontinuerligt och att komma till en punkt där man kanske kontrollerar, följer upp och så vidare, man ska implementera det i en kommunal miljö där vi också har, ja det är ju en politisk organisation där det ska gå den svängen också, det är en utmaning.

S: Hur anser du att den generella attityden mot informationssäkerhet är hos de anställda? Är det någonting du lägger märke till i ditt dagliga arbete?

K1: Nej jag tror att attityderna är väldigt bra, däremot är kunskapsnivån väldigt låg ibland eftersom man inte är medveten. Men när man väcker frågan så är det ofta väldigt intressant att diskutera. Jag tror att det är just kunskapsnivån, att lyfta den. Och då tror jag även att det kommer växa, man ser vilket behov som finns och lite sådär.

S: Okej, toppen! Sen är vi lite nyfikna, vet du hur många anställda det är på kommunen?

K1: 2000 ungefär. Det kan ni nog kolla på nätet exakt, det står på hemsidan på första sidan.

S: Vi har sett från 2014 vi ville bara veta om det hade förändrats. Det var de frågorna vi hade, jättesnällt att du ville hjälpa oss! Men innan vi avslutar, är det någonting du vill tillägga eller fråga? Eller någonting vi kanske har glömt fråga dig om?

K1: Ja, hur kommer det sig att ni valde just dessa områden?

S: I och med att vi har MSB:s undersökning som vår grund för att utveckla denna vidare och ställa frågan varför inte kommuner inte erbjuder utbildning. Detta är vårt primära fokus. Desto mer teori vi läste insåg vi att policy och styrande dokument stämde in med utbildning samt kontroll och uppföljning. Därför valde vi dessa tre delarna. Och utöver detta så valde vi det tekniska och informationssäkerhet för vi läser Systemvetenskap. Vi är båda väldigt intresserade av säkerhet och kommuner hanterar väldigt mycket information.

K1: Jag tror att det kommer förändras, alltså kommunerna har ju klarat sig ganska lindrigt undan om man kollar på de krav som finns, alltså lite tuffare krav. Många myndigheter och så har ju mycket starkare kravbild än vad kommunen har idag. Jag tror att det kommer förändras framöver och då kommer man se en helt annan attention på just informationssäkerhet generellt inom kommuner än hur det är idag. Ni får gärna skicka över ert arbete sen också. Det skulle vara kul att läsa vad ni kom fram till eller hur det ser ut hos de andra ni intervjuar.

S: Ja självklart! Vi skickar transkribering av intervjun så fort den är färdig, sen kommer uppsatsen vara färdig i slutet av maj kanske och då skickar vi jättegärna den till dig.

K1: Ja jättekul!

S: Tack så mycket för vi ville medverka!

K1: Tack själv och lycka till nu!

7.2.2 Transkribering av intervju: Kommun 2 (K2)

Datum: 2017-04-28, 13:30
Intervjuobjekt: K2
Intervjuare: N (Nelly Karlsson Åhlén)
Metod: Telefonintervju, inspelning av intervjun och transkribering efteråt.

K2: xx, IT-enheten xx kommun
N: Hej xx, jag heter Nelly och jag ringer ju från Lunds Universitet.
K2: Jaa, hej Nelly. Jag visste ju att du skulle ringa, men du var lite tidig här men jag var på plats (skratt)
N: Jaa, det var ju bra haha
K2: Jag ska bara avsluta den chatten jag var inne i här då, vänta lite då så ska vi se.. Då ska jag stänga ned den så jag är koncentrerad på det jag ska tänkte jag!
N: Det låter bra!
K2: Sådär å den, å där, så ska vi se. Jag chattar med en förvaltningschef här som inte är så van på att chatta men nu fick han ju öva lite på det så det var ju bra!
N: Jaa, det är bra att lära dem!
SW: Ja, vad bra. Nu är jag redo för dig!
N: Så bra. Har du haft tid att läsa igenom den preliminära intervjuguiden som vi skickade till dig igår?
K2: Jaaa, men det har jag gjort
N: Jamen, vad bra. Toppen! Sedan är det ju inte meningen att vi utgår helt utifrån guiden, men ändå så att du skulle ha något hum om vad vi skulle prata om på förhand.
K2: Jamen just det, precis. Men du stället väl de frågor som du vill och jag försöker svara utefter bästa förmåga.
N: Toppen! Har du några frågor innan vi startar intervjun, eller ska vi köra igång med det samma?
K2: Nejdå, vi kan köra igång rakt av!
N: Toppen, då först vill jag bara att du ska berätta lite kort om din roll inom kommunen mer än att du är IT-chef och hur länge du har jobbat, och sådär.
SW: Ja, då får du styra in mig på rätt spår så att jag håller mig till saken eftersom jag inte riktigt vet vad de andra har svarat, men jag jobbar som IT-chef här på kommunen, och jag har gjort det i 3 år och jag är inne på mitt fjärde år nu. Jag kommer närmast ifrån Vattenfall tidigare där jag har jobbat länge inom IT. Jag är väl ingen traditionell IT-chef ur det perspektivet man tänker lite mer IT-drift, som är det föråldrade sättet att se det ur enligt mig då att se på saken. Och jag jobbar ju inte så. Jag jobbar kanske mer med verksamhetsutveckling och en del kanske benämner det som IT-strateg kanske. Men jag är ju även IT-chef och har en grupp här med åtta stycken medarbetare.
N: Okej.
K2: Jaa!
N: Men hur involverad är du då i själva informationssäkerhetsarbetet vill du säga då?
K2: Eehh, ja alltså man kan ju säga såhär då att ett informationssäkerhetsarbete generellt ska ju inte ligga på en IT-enhet, utan det bör ju ligga i verksamheten eftersom det är de som ansvarar för sin information, men så funkar det ju inte riktigt här.. och därför är jag involverad under tiden tills det utses någon som skall ha det ansvaret så har jag ryckt in och driver detta litegrann då jag tycker att frågan är viktig och då hjälper jag till med den. Så jag är involverad och är det någon som är involveras på kommunen så är det jag.
N: Okej, men hur upplever du då att ni arbetar med informationssäkerhet på er

kommun eftersom, ja.. du kanske låter lite tveksam till att just du är ansvarig så att säga.

K2: Njaae. Det beror ju på hur man ser det eftersom det finns ett reglemente som.. eller ja, man önskar ju att det ska finnas en roll inom en kommun som har, innehar rollen informationssäkerhetssamordnare. Och det är ju inte alla kommuner som har det och vi är ju också en ganska liten kommun, men jag tänker väl under tiden som de funderar på vem och vad som skulle kunna göra det så kan man ju inte stå stilla med arbetet. Men jag tycker nog ändå att det fungerar ganska bra här, jag tycker att jag får gehör för att det här är viktigt och så vidare, så på sätt funkar det bra, men det är klart det finns mycket att göra, men från det vi var för några år sedan går det ständigt framåt.

N: Förresten, var ni med i den här undersökningen som MSB genomförde, alltså den här: "En bild av kommuners informationssäkerhetsarbete, 2015"?

K2: Mmhm!

N: Ni var alltså med och deltog i den?

K2: Mm, jag vill minnas att jag var med och deltog i. Det är väl en sådan som skickas ut till alla, såsom en enkät vill jag minnas, som är ganska omfattande enkät.

N: Precis, ja de fick ganska mycket svar..

K2: Mmm, jaa.. Jag har gjort. Jag har varit med där.

N: Har du tagit del av resultatet som de skickade ut efter det också eller var du bara med på själva enkäten?

K2: Mm, nä jag har alltså läst den också. Men inför det här mötet gick jag in på deras sida och läste den igen då och skummade igenom den, men jag har läst den innan. Absolut.

N: Okej. Den här intervjun tänkte vi dela in i tre delar för att vår uppsats utgår utifrån tre olika delar från den här enkäten. Så att vi har ju mest fått statistik nu, utifrån denna enkät, så att hur många som har svarat ja eller nej på vissa frågor, så att vi vill mer veta varför det är så. Så att den första delen handlar om policys och styrande dokument, så min fråga till dig är: Har ni en informationssäkerhetspolicy eller hur ser det ut där?

K2: Ja... Vi har en informationssäkerhetspolicy som är beslutad av kommunstyrelsen. Ehhh... Och den är väl helt okej, skulle kanske varit lite, göras bättre. Men det är en helt okej policy, jag har läst igenom den. Men ett kort svar på frågan. Vi har en och den är beslutad, ja.

N: Okej, men jag hörde inte riktigt vem som hade utvecklat denna, kan du upprepa det?

K2: Jaa, jag vet att det är IT-chefen som var anställd här innan jag som jobbade fram dokumentet, men den är beslutad av kommunstyrelsen.

N: Okej, jag förstår. När skapades den, och när reviderades den senast?

K2: Den skapades 2013 och den är inte reviderad därefter.

N: Okej. Och då är det alltså ni på IT som är ansvariga för den policyn antar jag då?

K2: Ehh njaae, det är väl lite otydligt då. Jag tror att det är här det är.. inte klart.. nä. Jag kan inte påstå att det är IT som är ansvarig för det, jag vet faktiskt inte vem som ansvarar för att ta upp den för revision. Förmodligen så kan jag väl ana att man borde få en.. en omfråga och säga att det är dags att revidera den, men den ligger inte på mitt ansvar egentligen.

N: Okej... Till vem är den här policyn lämpad, alltså kan anställda ta del av den och förstå den, eller är det på högre plan som den är lämpad till?

K2: Nääej, men den består utav två delar. Och den första är lite mer övergripande. Där det står vad förvaltningschefen ansvarar för osv, på lite mer övergripande nivå. Men vi har även en, man skulle kunna säga att det är en användarinstutition som är kopplad till den här. Och den kan alla… Ja, ett: alla kan ta del av policyn, det är inget konstigt, men om du tänker vad den riktar sig mot, så är policyn kanske mer övergripande, men sen har vi ju en användarinstution med mer detaljerad information om vad man får göra och vad man inte ska göra och vad man ska tänka på.. Och DEN har jag skrivit.

N: Okej, men det låter ju ändå bra att den är lite blandad. För vi har fått lite olika svar.. Att den kanske bara finns men kanske inte varför liksom. Så det är ju intressant.

K2: Ja, just det. Och själva riktlinjen och policyn är väl lite av den traditionen. Alltså att den finns och att vi ska ha en sån och vi har den, men jag kan ändå tycka att användarinstutitionen är kopplad dit och gör den mer levande då. Och det är väl så det är med policy, den ska inte ändras så ofta.

N: Okej. Hmm. Men tycker du att det här resultatet från den här MSB-undersökningen har förändrat arbetet kring era policydokument, eller har ni någon framtidsplan på hur det ska se ut, på grund av svaren från den enkätundersökningen?

K2: Ehhh, näää. Alltså, det är ju.. Det kom ju egentligen inte fram något nytt alltså. Det är ju ett område.. Informationssäkerhet är ju ett område som det finns mycket att göra åt på vår kommun och på andra kommuner, så att det var väl inte några nyheter som kom upp. Eh, kan jag väl inte tycka. Men det är ju klart att man kan ju ha den som utgångspunkt i när man ska planera framöver, "Vad är det vi behöver ta tag i?" och på så sätt så fungerar den ju..

N: Mmm, okej.. Ska vi gå vidare till nästa del då?

K2: Det tycker jag!

N: Det handlar om utbildning och kompetensutveckling, men främst då för era anställda då, så jag undrar hur ni arbetar med det idag med utbildning och kompetensutveckling, men främst för era anställda?

K2: Eh ja, inom området informationssäkerhet?

N: Precis.

K2: Ja, då har vi för alla nyanställda som börjar på kommunen blir inbjuden till en introduktionsdag, en heldag. Ehmn, en jag är med och anordnar dagen och ett pass på denna dagen och ett pass på denna dagen, lite drygt en timme så pratar jag om informationssäkerhet. Så alla får med sig det, alla nyanställda som anmäls till den. Det är ju inte så att alla nyanställda går den, men många gör det. Den är väldigt populär och de är faktiskt ganska nöjda med denna dag. Och då fångar man ju in en del, dvs alla nya. Och sen har vi alla som jobbat på kommunen så många år som inte går informationsutbildningen, eller ja introduktionsutbildningen och dom, ja vi har en informationssäkerhetsutbildning som vi startade för två veckor sen som riktar sig till alla anställda. Och den görs eh, ja man kan säga att den är webbaserad, man får en lektion i veckan under 29 veckor tror jag mer kort information som man behöver veta om informationssäkerhet. Riktigt trevlig liten utbildning faktiskt!

N: Okej, vad är det för slags information som är inkluderad i den? I dessa avsnitt?

K2: Jaa, det kan vara vad man ska tänka på när man klickar på länkar i ett mail, hur man ska tänka om någon ringer och försöker få ut lösenord.. vilka appar, vad man ska tänka på när man laddar ned en app på sin mobiltelefon.. Och hur man ska skydda sin dator när man jobbar mobilt osv, det är behörighet. Alltså det är verkligen fokus på informationssäkerhet och lite sunt förnuft kan man säga. Vad är det jag som användare behöver tänka på? Mm, vi anlitar en.. Det är inte vi som har satt ihop kursen från början, utan vi har anpassar den, vi har köpt in den.

N: Mm, men det låter ju bra.

K2: Mycket bra!!

N: Följdfråga till den då. Hur ser då framtiden ut gällande era utbildningar, är det detta som är på agendan eller har ni något annat i görningen?

K2: Nej, det är absolut detta som är på agendan. Introduktionsdagen är uppdaterad. Ehmn, Gjordes om i denna befintliga formen för lite drygt ett år sedan och den funkar bra, så det ska vi köra vidare på! Och den här befintliga utbildningen i webben, som jag sa nu, vi har ju precis startat den. Vi har bara kört två lektioner. så det är årets fokus är informationssäkerhet

med den utbildningen, så ja årets fokus är detta inom informationssäkerhet. så ja, det är våran plan just nu!

N: Du sa innan att den här MSB-undersökningen inte egentligen kom fram till något nytt så, men har ert arbete förändrats efter den, gällande just utbildning och så?

K2: Äsch, jag skulle vilja påstå att jag kanske mer använder den som ett argument när jag vill lyfta informationssäkerhet på kommunen och få fram hur viktig den är.

N: Okej så mer då som statistikunderlag och så?

K2: Jaa, så kan jag ta fram information därifrån och visa hur det ser ut. Jag har inte gjort en handlingsplan utifrån den undersökningen, nej. Däremot så.. nää aa det kanske kan komma sen kanske, det var mitt svar på den..?

N: Okej, eeh eller nä du ville nästan lägga till något där, lät det som? Eller?

K2: Jag tänkte säga att en annan sak som vi gör, som eventuellt fanns med i den rapporten, men det minns inte jag och det var därför jag blev lite osäker. Men vi bör ju, vi skall ju klassificera våran information i våra verksamhetssystem och det tas säkert upp i rapporten och det har vi börjat göra med hjälp av Sveriges Kommuner och Landsting (SKL):s, verktyg "klassa".

N: Okej, ja men då till sista delen av intervjun som då. Den handlar om kontroll och uppföljning och det var också en del som var med i MSB:s enkätundersökning, så jag undrar mest hur ni just nu arbetar med kontroll och uppföljning. Inom informationssäkerhet, såklart då.

K2: Ah. Där.. Det är väl inte den starkaste delen vågar jag nog påstå. Nu svarar jag ju för en stor del av kommunen där jag inte ens. Jag har ju inte koll på allting. För att, när de gäller de olika verksamhetssystemen så ligger ju ansvaret ute för varje förvaltning, så det ligger inte här hos mig på IT, så jag kan ju inte det, så jag får nog kolla upp det. Men generellt vågar jag nog ändå hävda att där finns en del att göra. Faktiskt. Det finns säkert inte framtagna rutiner överallt på om hur saker och ting följs upp. Undantagsvis omsorgen, de är duktiga på det!

N: Okej, men då vet du ingenting om den här MSB-undersökningen har förändrat arbetet kring det då, antar jag?

K2: Nää, och där vågar jag nog påstå att det har den inte och att alla har tagit del av den undersökningen. Utan det är jag som, och sen så med förvaltningschef, och andra som jag har lyssnat. Det är inte ute på varje förvaltning, så det vågar jag påstå att den inte har påverkat dem. Mer att de är påverkade av den nya dataskyddsförordningen som kommer ut nästa år, för det är lite mer spritt.

N: Ja precis, GDPR tänker du på då?

K2: Aa, precis, jajamän.

N: Okej, men då kan vi lämna det området då så kan vi gå in på lite mer avslutande frågor? Så jag undrar mest vad du upplever är den största utmaningen när det kommer till informationssäkerhetsarbetet på kommunen?

K2: Det tycker jag är.. Att få fram ett lagom. Att hitta rätt ambition på vad vi ska göra. Man kan göra det här superstort, och man kan välja att inte göra det alls naturligtvis. Och det är ju inte bra. Men man behöver ju ta fram en modell.. Det är lätt att säga att man ska sköta sig när det gäller informationssäkerhet. Att man ska klassificera sin information, att man ska göra riskanalyser. Men man kan ju inte bara säga så, för att man måste ju ha stöd i det, så man vet vem som ska göra allt. Till exempel systemansvarig. Och då behöver man ju ta fram en lagom ambitiös plan och utbildning kring hur man ska göra det och det tycker jag är en utmaning. Det blir lätt väldigt, väldigt stort och komplext och då är det ingen som orkar och då blir det inte gjort.

N: Ja, och som du nämner kan det ju vara små saker som att man går igenom olika program om hur man gör ett lösenord eller hur man inte ska klicka på länkar i mail. Det behöver ju inte vara större än så egentligen, liksom.

K2: Nej! Exakt!! Och det är det här jag tror är framkomlig väg, för det är väldigt många, tror jag, som inte tänker sig för och får de bara veta lite så vill de ju göra rätt. Men jag tror ändå att man kan göra det parallellt, men att man börjar med de här små grejerna för varje användare istället för att säga att nu ska vi klassificera alla 70 system och det ska vara gjort på ett halvår. Det blir ju inte gjort! Det förstår man ju, det är för stort! Men börjar man här i den andra änden.. För vet du? Det är ju också att.. Väldigt mycket intrång görs ju. man kan ju hindra det med teknik och så, men den största anledningen, det är ju egentligen användaren själv som drar in saker och ting för att den inte vet att den inte ska klicka på det ena och det andra. Och börjar vi i den änden så är det ju faktiskt ett ganska stort steg fram med det. Jag försöker avdramatisera det här lite.

N: Ja, men det är ju jättebra och det är ju ungefär det här vår uppsats riktar sig till också. Att det är mera att du kan ha hur bra verktyg och så som helst, men om dina anställda inte arbetar rätt kring det så spelar det ju ingen roll.

K2: Nej! Det spelar ingen roll. Jag brukar säga till om det. Jag visar och talar om olika metoder för att hitta bra lösenord, för att det ska vara enkelt att komma ihåg, för att det ska vara enkelt osv, men jag säger det att.. Det spelar ingen roll hur stort, och långt och komplext lösenord du har om du ändå inte låser datorn när du lämnar den. Du kan ju ha en miljon siffror i den och sen så funkar det ju ändå inte för datorn inte är låst och då är den ju öppen ändå. Det behöver inte vara så himla komplicerat.

N: Nej precis.. Men då till min sista fråga då: Hur anser du då att den generella attityden är mot informationssäkerhet? Är det att folk tycker att det är för stort, eller att de inte förstår innebörden? Eller hur är attityden?

K2: Eh, jag tror att man kan dela upp den. När jag har introduktionsutbildningen och går igenom den och verkligen pratar med de som är där och har dialog, då tycker de inte att det är stort eller svårt, utan då är det väldigt engagerade och är glada för att faktiskt få lära sig lite, för det har de ju dessutom nytta av privat också, faktiskt haha. Ehm, det som blir stort och känns jobbigt är nog mer det här med att man ska klassificera information, att det ska göras riskanalyser, att man inte vet hur man ska göra. Alltså mer det. På användarnivå tror jag man inte tycker att det är så stort och jobbigt. Det tror jag inte, aa.

N: Det håller jag nog med dig om, så. Men då har nog jag fått det jag behöver, men om inte du vill lägga till någonting som du känner är viktigt gällande det här ämnet?

K2: Nä, jag hade skrivit upp några punkter, men dem har jag nog fått fram. Jag, eh, det går ju ganska snabbt och jag pratar ju ganska mycket så.. Ja, jag är nöjd! Jaa, men jag tycker att detta är ett väldigt intressant ämne detta, jag tycker det är väldigt roligt alltså.

N: Det tycker vi med! Vi kände det när vi skulle välja ämne till uppsats, att det vi läser ändå är ett väldigt tekniskt ämne så var det såhär att nä, det vi egentligen lär oss är att du kan ha hur bra grejer som helst, men sålänge inte interaktionen funkar mellan människan och datorer så spelar det ingen roll liksom.

K2: Ja, och det här är ju inget tekniskt ämne egentligen, informationssäkerhet. Utan jag.. Det kan ju vara teknik inblandat, absolut. till viss del, men det är ju mer sunt förnuft och man måste förstå, liksom lyfta olika scenarion så man får möjlighet att bara inse att "jaha, gör jag bara såhär så skyddar jag faktiskt informationen bättre". Och då kommer man långt, så jag tycker att det är ett stort ämne och det är jättekul tycker jag!

N: Absolut! Ja men då får jag nog tacka för mig så får du ha en trevlig helg, så återkommer jag senare med transkriberingen och såklart också om du vill ha uppsatsen när den är klar sen, så kan jag skicka den också.

K2: Du, den vill jag gärna ha! Det kan jag säga från början. Det är jag jätteintresserad av att läsa. Det kan du notera!
N: Tack! Då skickar vi den någon gång i juni skulle jag tro. Då är den nog helt klar.
K2: Det ser jag verkligen fram emot, det blir jättebra det! Trevlig helg!

7.2.3 Transkribering av intervju: Kommun 3 (K3)

Datum: 2017-05-02, 10.00
Intervjuobjekt: K3
Intervjuare: S (Sofia Söderström)
Metod: Telefonintervju, inspelning av intervjun och transkribering efteråt.

S: Vi kan börja om du vill berätta lite kort om din roll inom kommunen?
K3: Jaa då kan jag väl säga såhär mycket som att jag började första februari i år så det är ju precis tre månader jag varit på kommunen nu, och anledningen till varför jag fick den här tjänsten, och det kallas ju för trygghetsstrateg den tjänsten som jag har, och jag kommer från polisen innan så jag har ju varit polis innan och sen dök den här möjligheten upp. Anledningen till att den finns, den här tjänsten, är att man har valt att se, man tar det på allvar det här med trygghetsarbetet i kommunen. Så jag tillsammans med två andra jobbar med säkerhet och trygghet och då blir det väldigt brett och då någonstans på vägen där strax innan jag började och framför allt när jag började så blev en av dessa stora puckarna också informationssäkerhet. Som då helt plötsligt skulle falla på detta område och det är inte konstigt egentligen men därav min okunskap inom detta område än så länge. Jag har inte hunnit ta tag i det, eller sätta mig in i det. Jag har ingen kunskap heller, men den ligger på den här rollen och innan låg den på en helt annan position.
S: Hur involverad är du då egentligen i informationssäkerhetsarbetet?
K3: Ja, tanken är nog egentligen att att den här tjänster, att jag ska bli den som ansvarar för informationssäkerhet inom kommunen, att det ska ligga på den här tjänsten och på mig. Men just nu är det då en annan som har den här rollen då kan man säga och som då ska "jacka" ur den, han ska göra någonting annat, så det var som jag sa här om dagen: om man ska gå in i ett rum som har informationssäkerhet så står jag fortfarande utanför tröskeln och tittar in om man säger så. Jag har inte klivit in riktigt än utan håller fortfarande bara på att sätta mig in i det, vad innebär det? och vad är det? och vad kommer krävas av mig? Men så småningom när jag kliver in i rummet så kommer allting att hamna på mig, men just nu är jag fortfarande utanför och tittar in i rummet.
S: Vet du om ni var en del av MSB:s enkätundersökning "En bild av kommunernas informationssäkerhetsarbete 2015"?
K3: Ja jag tittade på den fråga och jag tror, eller jag kan nästan säga till 100% att vi var det. För dom hade fått en fel "bustning" där för det var en del som behövde göras och det vill jag hävda att det var just den uppsättning som sa att det var en del.
S: Såhär i efterhand, har du läst genom undersökningen? Har du tagit del av resultatet?
K3: Njae, säger jag ja så ljuger jag. Men jag säger ja då för jag har bläddrat genom den och tittat på den och det var massa annat också kring informationssäkerhet så jag har inte läst hela MSB:s undersökning, det har jag inte gjort.

S: Intervjun kommer iallafall att vara lite i tre delar men lite olika fokusområden, varav det första området handlar om policy och styrande dokument. Vet du om ni har etablerat en informationssäkerhetspolicy?
K3: Ja det gör det. Jag vet, jag har fått som hastigast någon form av genomgång på kommunens informationssäkerhet och det har funnits en policy. Det vi skrattade lite åt var att den var så gammal om vi säger så, den har säkert kanske tio år på nacken. Den är ju inte aktuell längre men den finns och den har funnits, men den är inte uppdaterad.

S: Aha, du vet inte när den reviderades senast?

K3: Nä, det vågar jag faktiskt inte svara på, men jag sitter med datorn och kan blippa lite under tiden vi pratar för att se om jag hittar det.

S: Vet du vem eller vilken del av organisationen som har utvecklat policyn?

K3: Ja den mannen som har den här rollen nu han sitter ju på, ja det kallas nog IT-kontoret och där jobbar de med IT och all data inom kommunen. Informationssäkerhet tillhör ju IT-teknik, även fast det inte alltid stämmer är det där de valt att lägga det. Så där har det legat innan.

S: Vet du om ni arbetar på något sätt för att de anställda ska vara införstådda i policyn?

K3: Man kan nog säga såhär då, för när jag kollade på frågorna så tänkte jag att det här kan jag bara relatera till mig själv då jag började här den första februari och jag har inte fått någon information om informationssäkerhet så länge jag har varit här. Dock vet jag att det finns dokument som man själv kan leta upp på hemsidan då. Men inte så att man, jag fick inte ta del av någonting när jag började. Jag fick en data och en telefon sen var det så.

S: Okej, då går vi vidare till utbildning och kompetensutveckling. Hur arbetar ni med utbildning och kompetensutveckling för era anställda gällande informationssäkerhet?

K3: Detta är en fråga som jag nästan inte vågar svara på. Det har jag ingen aning om, jag har inte koll på det.

S: Ingen fara, då har du kanske inte heller koll på eventuell utbildningsplan eller framtida planer? Du kan väl berätta lite om din vision och hur du vill ha det i framtiden?

K3: Ja men som sagt, jag står utanför tröskeln fortfarande men någon form av tankar och visioner kan man ju ha ändå. Och ja, informationssäkerhet idag tror jag att man tänker IT-säkerhet, man tänker data, virusprogram och man tänker brandväggar och sånt. Men där tror jag kanske att jag har varit själv under många många år och vanligt folk, om man nu kan säga så, tror jag har den bilden "jaja har vi en bra brandvägg så klarar vi oss". Börjar man studera informationssäkerhet så förstår man ju ganska snart att det är rätt så mycket mer. Och med den tekniken vi har idag men mobiltelefoner och appar och man måste tänka mycket bredare, och appar man tar hem, man blinkar liksom inte utan man bara tar hem sånt och tror att det är okej. Där tror jag att man måste ha någon form av basic nivå så att folk förstår att telefonen, värdehandlingar eller datorn man bär runt på kan komma i orätta händer. Och det behöver inte vara innebära att dom blir stulna. Utan det kan innebära att någon lyssnar av den och får då tillgång till viktiga dokument som man kanske inte alls ska ha del av. Och samma sak med informationen att den är rätt och riktig, för det har ju poppat upp fakta i samband med valet i USA. Information som man läser idag, är det verkligen sant och var kommer den ifrån och så vidare. Man tror det är sant när man läser det, men det finns ju folk som vill ändra ens åsikter och skickar därför ut falsk information. Så där tror jag även att man måste vara mer, man måste göra folk mer medvetna om att vi är lättpåverkade av den informationen som kommer. Så där är någon form av vision iallafall, det kan vara enkla och lätta insatser att informera folk men sen måste ju var och en ta tiden.

S: Nu går vi in på kontroll och uppföljning gällande informationssäkerhet. Hur arbetar ni med detta?

K3: Jag känner att jag nog har lite för dålig koll för att svara. När man tänker på datasystem och sånt så finns det ju en kontroll men vi pratar ju mer om informationssäkerhet. Och då tror jag nog att spontant så gör man nog ingenting förens det har blivit något tokigt. Men jag kan inte säga något mer om det.

S: Det är ingen fara! Lite avslutande frågor då. Vad upplever du är den största utmaningen när det kommer till arbetet just gällande informationssäkerhet?

K3: Ja, ehm, ja vad ska jag svara på det egentligen. Största utmaningen? Ja, dels så är det ju att man, den informationen som kommer ut verkligen är rätt och riktig. Idag är det så mycket konstigheter som florerar just på facebook och twitter och det informationsflödet som finns där är ju så stort. Och att man där måste sålla vad som är rätt och riktigt och det tror jag är svårt för folk är ju inte direkt, har man bara läst det tillräckligt många gånger eller är det många som gillar det då är det ju sant fast det kanske inte är det egentligen. Och det kan vara likadant inom en kommun då. Det kan florera en massa olika informationsbudskap som egentligen inte stämmer och med den snabba tekniken vi har idag så helt plötsligt kan alla som jobbar på kommunen tro på någonting som inte alls stämmer. Så det tror jag är en utmaning idag. Att verkligen, vad är källan till informationen. Är den sann eller är den inte sann?

S: Det var de frågorna jag hade. Men innan vi avslutar, finns det någonting du vill tillägga eller fråga mig?

K3: Nej, jag tror inte det. Hade jag som sagt påläst och verkligen i denna världen hade jag säkert haft massa mer. Men nu är jag ju så ny i detta, så du kanske står för det proffsiga i detta. Men det kanske är bra för då förstår man att det fungerar olika.

S: Precis! Tack så mycket för att vi fick intervjua dig!

K3: Det är ingen fara, det var bara roligt.

S: Vi återkommer, och tack ännu en gång.

K3: Tack så mycket!

S: Hejdå!

K3: Hej!

7.2.4 Transkribering av intervju: Kommun 4 (K4)

Datum: 2017-05-02, 13:00
Intervjuobjekt: K4
Intervjuare: S (Sofia Söderström)
Metod: Telefonintervju, inspelning av intervjun och transkribering efteråt.

S: Har du någon fråga eller vill du att vi bara kör igång?
K4: Vi kan köra igång! Jag har skrivit ut det material som du skickade så jag har lite koll på ungefär vilka frågor ni vill ställa.
S: Vill du börja berätta lite kort om din roll på kommunen?
K4: Jag är ju säkerhetssamordnare och jobbar strategiskt på kommunövergripande kan man säga, på kommunledningsförvaltningen. Och har egentligen det strategiska ansvaret när det gäller säkerhet i hela kommunen. Där informationssäkerhet är en del av det här då.
S: Hur länge har du arbetat på kommunen?
K4: Jag är inne på mitt 4,5 år har jag varit här. Så vad blir det då? 2013 kanske.
S: Hur involverad är du i informationssäkerhetsarbetet?
K4: Jag är ju den som är ansvarig för informationssäkerhetsarbetet. Alltså det är jag som håller i metoder, processer och hur vi ska gå tillväga och det är jag som håller i de klassificeringarna vi gör utifrån informationsäkerhetssystem, eller informationssystem. Så att man kan säga att det är jag som har det övergripande ansvaret för att jobba med det, men däremot så är det varje verksamhet som är informationsägare, eller vad man ska säga, också ansvariga.
S: Var ni en del av MSB:s enkätundersökning "En bild av kommunernas informationssäkerhetsarbete 2015"?
K4: Jag vet inte riktigt, jag tror jag brukar svara på den enkäten men jag är inte hundra på det. Och om man säger så, jag känner inte riktigt igen mig i det i så som de beskriver det. Men det är ju för att vi har jobbat väldigt mycket med informationssäkerheten det sista 1,5 året.
S: Har du tagit del av resultatet?
K4: Ja jag har bläddrat, jag har läst den delvis men inte i detalj.
S: Nu kommer vi gå in på mer specifika områden, där den första är policy och styrande dokument. Har ni etablerat en informationssäkerhetspolicy på kommunen?
K4: Vi har en, men den är inte beslutad än utan den ligger i, ehm, den kommer beslutas i nästa månad tror jag det blir. Så att den är på gång. Vi har en gammal också, men den lämpar sig inte riktigt, så vi har en ny på gång.
S: Okej, vem eller vilken del av organisationen har utvecklat den nya policyn?
K4: Det är då jag tillsammans med verksamheterna kan man säga. Men det är mest jag då.
S: Är det även du då som är ansvarig för den?
K4: Ja. Eller ja det är ju jag som är ansvarig tjänsteman för den kan man säga och den beslutas ju i fullmäktige så den är ju politisk.
S: Arbetar ni på något speciellt sätt så de anställda är införstådda med innehållet i policyn?
K4: Ja, alltså man kan väl säga att vi inte fokuserar jättemycket på policyn, utan vi fokuserar mer på den dagliga användningen av att få informationssäkerhet på, alltså utbilda i det. Däremot så jobbar vi ju en hel del med att eh, med vår ledningsgrupp för att dom ska vara medvetna om vad deras ansvar är och vad dom behöver göra.
S: Perfekt! Lite frågor om utbildning och kompetensutveckling. Hur arbetar ni idag med utbildning och kompetensutveckling för era anställda?

K4: Idag så är det väldigt dåligt ska jag säga. Men efter, och det är, vi har ju kört ett omtag och vi har inte kommit till en bra process kring det idag. Det vi har gjort det är att vi har utbildat att alla kommunens chefer, en kort genomgång per chef då. Men planen är att vi ska göra ytterligare en sån för chefer, och sen kommer det även blir en utbildning för alla anställda.

S: Så det är så framtiden ser ut gällande utbildningen då?

K4: Ja närmsta, om man säger så, vi kommer till hösten köra för cheferna och förhoppningsvis kommer vi ha en bra webbutbildning också i höst men vi kanske kommer igång i början av nästa år.

S: Vi går vidare till kontroll och uppföljning. Arbetar ni med kontroll och uppföljning och isåfall hur?

K4: Vi gör ju mycket, vi har gjort väldigt många informationsklassificeringar nu den sista tiden. Och dom, i dom, när man är klar med dom så är där ju en del som behöver åtgärdas. Det tar vi upp och tittar på hur dom, hur det går och det gör vi ju, idag gör vi det manuellt men under sommaren här så kommer vi även lägga in det i vår verksamhet, eller vårt ledningssystem så att man kan se det i vårt ledningssystem.

S: Okej. Lite avslutande frågor då. Vad upplever du är den största utmaningen när det kommer till arbetet med informationssäkerhet?

K4: Största utmaningen tror jag, som allting annat, vi jobbar med eh, det är väldigt lätt att man skriver dokument och gör policy och gör olika rutiner men det viktiga i det här är ju ändå att vi utbildar och så att användarna att dom som sitter och jobbar med sekretesshandlingar osv att dom vet hur dom ska göra, och att dom liksom är införstådda i vad som kan hända om dom gör fel. Det är nog mer implementeringen ut i vardagsanvändadet som jag nog tycker är mest kritiskt.

S: Har du någon åsikt hur du anser den generella attityden mot säkerheten är hos de anställda?

K4: Jag skulle nog säga så att generellt så är alla medvetna om det, men det är en stor okunskap. Det är okunskap att det här är, hur man ska hantera sekretess och hur man ska hantera känsligt material men man har stor förståelse för att det är viktigt.

S: Innan vi avslutar, har du någonting du vill tillägga eller fråga mig som jag kanske ha missat?

K4: Nä, alltså vi har, kommunen har haft fördelen att vi har jobbat med informationssäkerhet i 1,5 år. Vi har fått ett projekt att starta upp och nu har vi gått in i en vardag så att säga. Så vi har ju kommit ganska långt i arbetet. Men just fördelen på det sättet som vi har jobbat med det är att vi har gjort det enkelt. Vi har, istället för att göra det komplicerat försökt göra metoden väldigt enkel.

S: Toppen! Något annat?

K4: Nä det var allt. Hoppas det har gett er lite svar.

S: Absolut, vi är tacksamma att du ville ställa upp på en intervju. Vi kommer skicka tillbaka den transkriberade intervjun så att du får godkänna den innan den läggs in i uppsatsen.

K4: Ja det går jättebra!

S: Annars var det allt. Jag tackar så mycket!

K4: Tack själv, hej!

S: Hejdå!

7.2.5 Transkribering av intervju: Kommun 5 (K5)

Datum: 2017-05-02, 14:30
Intervjuobjekt: K5
Intervjuare: N (Nelly Karlsson Åhlén)
Metod: Telefonintervju, inspelning av intervjun och transkribering efteråt.

N: Ja, vi glömde bort att det var röd dag igår så vi skickade ut guiden till dig igår, så jag vet inte om du har hunnit att läsa igenom den?
K5: Jodå, men det har jag gjort.
N: Jamen toppen, då har du iallafall lite kött på benen inför intervjun hoppas jag!
K5: Ja.
N: Såå ska vi börja då?
K5: Gör så.
N: Då vill jag först bara att du ska berätta lite kort om dig själv och vad du har för roll inom kommunen och vad du gör där.
K5: Oj…
N: Ja, mest då inom informationssäkerhet såklart, men..
K5: Ja, jag är anställd som IT-samordnare. Sedan har det här med informationssäkerhet, IT-säkerhet, men även PUL, ja, GDPR, dataskyddsförordningen hamnat på mig. Så sedan i höstas är jag även informationssäkerhetssamordnare då.
N: Så då antar jag att du är ganska involverad i informationssäkerhetsarbetet?
K5: Japp!
N: Hur upplever du att ni jobbar med informationssäkerhet på er kommun?
K5: Eh, vi säger såhär att den föregående säkerhetschefen gick hem i höstas. Och efter sen hon gick hem så vart det mycket bättre. Då tog kommunchefen över som information, eller säkerhetschef. Och han tillsatte ju mig direkt under honom, som informationssäkerhetssamordnare. Och det tas på mycket större allvar det här med informationssäkerhet. Han tar upp det på varje chefsträff, en gång i månaden. Vi har köpt in utbildningar och ja.. Det är helt annan.. Det är skillnad än vad det har varit tidigare.
N: Okej, jag förstår. Vad är det för utbildningar som ni har köpt in?
K5: Vi har köpt in den här NanoUtbildningen från "Junglemap", dels på informationssäkerhet, men även på GDPR. Och då får man ju en utbildning i veckan som går ut till ALLA våra anställda som har en mailadress.
N: Är det den utbildningen som är på 29 veckor?
K5: Ja, precis. Det stämmer och sedan går det rapporter till kommunchefen och deras respektive förvaltningschef som de diskuterar en gång i månaden.
N: Vilka är det som gör den här utbildningen?
Ja, alltså de heter Junglemap.
N: Nej, förlåt. Jag menar vilka som genomgår utbildningen på er kommun.
K5: Jaha, ja det är alla anställda som får den.
N: Jaha, toppen!
K5: Jaa.. Alla som har en mailadress, så jag tror det var 1800 stycken och vi har 1300 anställda, så att.. hehe??
N: Jaha, oj. Det är ju jättebra ju.
K5: Ja. Och det är jag som har gått igenom frågorna då och kontrollerat så att det är relevanta frågor för xx kommun då.

N: På tal om annat, vet du om ni var en del av den här MSB-undersökningen: En bild av kommuners informationssäkerhetsarbete, 2015?
K5: Njaae, jag vet faktiskt inte. Det är iallafall ingenting som jag har varit inblandad i. Men har enkäten kommit fram till säkerhetschefen, då har hon gjort den.
N: Ja, alltså det var ganska många medverkande, så om ni ändå jobbar aktivt med informationssäkerhet så kan jag väl tänka mig att ni kan ha varit en av dessa kommuner som svarade.
K5: Jaa
N: Men har du tagit del av resultatet från undersökningen?
K5: Ja, det har jag. För den fick vi dessutom utskickad på en länk av er, så jag var in och laddade ned den från MSB, så att ja.
N: Vår uppsats utgår ju från tre olika delar från den undersökningen då vi valt att främst fokusera på policy och styrande dokument, men även utbildning och kompetensutveckling mest, och till sist då kontroll och uppföljning. Så att intervjun kommer att vara indelad i dessa tre kategorier. Så med det sagt vill jag bara fråga om ni etablerat en informationssäkerhetspolicy på er kommun?
K5: Japp, det har vi.
N: Vet du vem eller vilken del av organisationen som har utvecklat den?
K5: Ehh, ja.. Det var väl jag, inofficiellt för 15 år sedan. Fast den låg under säkerhetschefen då. Från och med i höstas då ligger den under kommunchefen och mig som informationssäkerhetssamordnare då. Det är ju vårat ansvar att hålla iordning på den.
N: Så den skapades för 15 år sedan då?
K5: Första gången ja, gjordes den då. I början på 2000-talet. Sedan har den reviderats vart tredje år och jag gjorde en helt ny i höstas och så reviderade jag den nu i mars. Så den är helt ny. Helt ny och omgjord.
N: Jättebra. Är det du som lite då har huvudansvar för den eller alltså, att få den reviderad så att säga.
K5: Ja. Och så lämnas den till kommunstyrelsen då för beslut.
N: Okej. Hmm. Hur arbetar ni på kommunen för att era anställda ska införstådda med policyn, eller vilka är det som tar del av denna policy hos er på kommunen?
K5: Jadu, dels från dess att den blivit beslutad från kommunstyrelsen så tas den ju upp i chefsgruppen. Och där får ju varje chef sitt ansvar att ta upp den på ett APT, en arbetsplatsträff då. Och är det så att de inte anser att de kan klara av det själv, då kommer jag gärna och hjälper dom. Och då är det meningen att de anställda ska läsa igenom alla "vrobbar" som vi kallar det: Ett vägledande råd och bestämmelser, plus informationssäkerhetspolicyn då. Och så ska de skriva på ett papper helt enkelt, att de har tagit del av det och förstått. Och det pappret förvaras sedan i personalakten då på "löner". På varje medarbetare då. Och sen ligger policyn ute på intranätet sen, så att de inte kan säga att de inte hittar den, eller inte hade tillgång till den eller nått sånt där, utan den finns tillgänglig året om.
N: Okej, tycker du att det här resultatet av MSB-undersökningen har förändrat ert arbete gällande policy och styrande dokument, eller hade ni det bra redan innan?
K5: Nä, det kan jag inte säga eftersom jag inte visste om att den hade gjorts. Så att nej, vi har inte jobbat någonting efter den. Nä.
N: Hm okej. Då tänkte jag att vi skulle gå vidare till nästa del av intervjun som handlar om utbildning och kompetensutveckling. Så jag tänkte börja med att fråga hur ni arbetar med utbildning och kompetensutveckling för just era anställda på kommunen, förutom det här nu som du har gått in på, men du får ju såklart gärna gå in på det mer detaljerat om du vill?

K5: Ja, jag vet inte om det går att säga något mer just om det. Dels att det är de här "vrobbarna" som vi går igenom på ett möte och den så får dom den här utbildningen utskickad på mail en gång i veckan. Ja, det är det vi har just nu.

N: Så det är det som är i görningen just nu, ni har inga andra framtidsplaner som ska hända mer inom informationssäkerhet?

K5: Nej.. nää.

N: Och då antar jag att MSB-undersökningen inte har förändrat erat arbete, eftersom du redan svarat nej på en liknande fråga innan?

K5: Nej, precis. Ingen ändring.

N: Okej, jag förstår.

K5: Sedan blir det ju också, det är ju så att det är en ny dataskyddsförordning som ersätter PUL.

N: GDPR menar du?

K5: Jaa, och den träder ju i kraft snart och därför måste vi även lägga lite krut på utbildning inom det då. Och då blir det kanske att informationssäkerheten ligger lite mer bakom än så länge. Eftersom vi måste satsa jättemycket på den här GDPR:en.

N: Ja, det förstår jag. Men hur arbetar ni med kontroll och uppföljning då? Är det något ni arbetar med gällande informationssäkerhet?

K5: Eh ja, det är faktiskt dåligt. Hehe, det måste jag få säga. Nej, men jag vet inte riktigt.. Jag personligen tycker att det går att göra mycket-mycket bättre. Vi har dom därа avtalen då som de får skriva på, att de har tagit del utav det. Vi har intern-kontroller på behörigheter och loggar vilka som har varit inne i systemen. Och jag vet inte, alltså det ät jättesvårt att kontrollera det här. Att våra medarbetare verkligen följer det. Har de skrivit på ett papper och lovat dyrt och hederligt att de följer det, ja men då kan vi inte göra så mycket mer. Ja, mer än dessa internkontroller då. Men det säger ju inte allt, för jag menar, vi kan ju ha oturen att kontrollera någonting som är jätte-jättebra och sedan så finns det någonting som är vägg-i-vägg som inte alls är jättebra. Som vi inte ser. Så det är jättesvårt att hålla kontroller och uppföljning på det då, väldigt svårt.

N: Ja, det är många som nämner att man mest arbetar med det vid incidenter, alltså om det är något specifikt som har hänt så kanske man kontrollerar och uppföljer vad som gick fel.

K5: Ja, det gör vi ju såklart, men då är det ju liksom ingen förebyggande kontroll. Då har det ju redan hänt, så att.. Men det gör vi ju naturligtvis också, OM det råkat hända någonting. Då utreder vi ju allting. Men, det tycker inte jag är en kontroll, för då har det redan hänt.

N: Nä, precis. Då vet jag. Men då till lite avslutande frågor då. Vad upplever du är den största utmaningen när det kommer till arbetet med informationssäkerhet, hos er på er kommun?

K5: Ja, det är ju faktiskt det här med kontroll då. Och att det efterlevs. För att som sagt var då, vi har ju 3000 människor inne i kommunen dagligen och vi kan ju inte garantera att alla dom följer det som dom ska följa. Och det spelar ju egentligen ingen roll hur mycket policys, och "vrobbar" och riktlinjer och det vi gör och de lovar, men ja. Nä, det är jättesvårt att följa upp det överhuvud taget, så det är största utmaningen. Definitivt.

N: Hur tycker du att attityden hos de anställda är gentemot informationssäkerhet hos er?

K5: Ja, säg såhär generellt sett har det varit ganska dåligt. Man tycker att "det är ingenting man orkar lägga tid eller resurser på". Men sedan vi fick ny kommunchef och han tagit upp det i chefsgruppen så har man börjat ändra lite attityd. Och man inser att det här är någonting som är jätteviktigt. Så får vi bara hålla på ett år till så kanske det blir bra.

N: Tycker du att attityden har förändrats också sedan ni har infört, till exempel den här nano-utbildningen? Har ni fått någon feedback på det?

K5: Jaa, det tycker jag. Och likadant, jag har haft jättediskussioner med folk som mailar personuppgifter. Och jag blir helt stortokig. För det är något som de absolut inte får göra. Och de förstår inte varför de inte får göra det. Och så tror jag att det är många gånger. Man förstår inte att man gör fel och att man kanske gör någonting som är olämpligt. Men när man förklarar, då verkar de som att de förstår.

N: Ja, jag diskuterade detta med en annan kvinna på en kommun här om dagen, att det är så många som tror att informationssäkerhet är så tekniskt, att det bara inkluderar brandväggar och ha med sådant att göra, medan det kan vara så mjuka värden. Och därför blir folk rädda för det. Att utbildning kan göra mycket inom detta område.

K5: Ja. Det gör det verkligen. Och när man läser detta frågor nu, eller dessa lektioner som man nu skickar ut då, ja. De som jobbar med informationssäkerhet och har det framför ögonen hela dagarna, de kommer ju tycka att "det där är ju jättelöjligt, varför engagera sig med det där?" Men, som kommun har vi så skilda människor som jobbar. Det är vårdbiträden, det är lärare, det är förskolelärare, det är vaktmästare. Och då kan man ju inte begära att de ska veta någonting om informationssäkerhet. Så att vi måste ju utbilda dem och informera dem så att de ska kunna förstå.

N: Precis. Har du förresten hört talas om en utbildning som heter DISA?

K5: Jadå, den har vi på intranätet.

N: Okej, är det något som många har genomfört?

K5: Ja, gud hur många år sen är det? 6-7 år sedan som vi la ut den på intranätet och då hade vi som krav att alla skulle genomföra den. Annars fick de inte tillgång till kommunens nät. Då stängde vi av dem. Men det är ju många som har bytts ut som ändrats efter det och vi sa ju det också, att alla nya som kommer in ska ju genomföra den också. Men däremot så tycker jag ju inte han är bra. Jag tycker han är jättedålig.

N: Jaa, alltså jag har faktiskt varit inne och gjort den själv och den var väl lite.. Låg nivå på kan man tycka?

K5: Ja, precis. Jag vet inte om han ger så mycket så därför har jag inte tjatat så mycket om honom.

N: Ja, jag ville ändå bara fråga för det är många som har tagit upp den som ett utbildningsmaterial som de har använt sig av. Men då är det intressant också att det finns andra utbildningsvägar att gå så att säga.

K5: Ja, så då tror jag att den här nano-utbildningen kommer att ge mycket mycket mer, och den är mer relevant och mer moderna frågor. Alltså inte såhär stenåldersfrågor som jag tycker att DISA har litegrann.

N: Men jättebra, tack så mycket för din hjälp! Jag tror faktiskt att jag har fått det som jag behöver nu, om inte du vill tillägga någonting inom området?

K5: Nej. Det är ett jobbigt område *skratt*

N: ja, det finns ju mycket inom området och speciellt har det kommit fram mycket nu när man pratar med olika personer från olika kommuner. Det kommer fram lite allt möjligt som är intressant, så man kan ju gå hur brett som helst.

K5: Japp. Så är det.

N: Men tack så jättemycket att du tog dig tid att vara med på detta så återkommer vi sedan med det transkriberade materialet till dig, så får du godkänna det också.

K5: Ja, vad bra.

N: Du får ha en bra eftermiddag!

K5: Jaa, du med. Tack hej!

7.2.6 Transkribering av intervju: Kommun 6 (K6)

Datum: 2017-05-03, 10:00
Intervjuobjekt: K6
Intervjuare: N (Nelly Karlsson Åhlén)
Metod: Telefonintervju, inspelning av intervjun och transkribering efteråt.

På grund av tekniska problem med inspelningen blev enbart 15/28 minuter inspelade. Det handlar om den sista delen utav intervjun. Olyckligtvis blev således inte fråga 1-16 inspelade och därför finns bara anteckningar från intervjun att tillgå.
Sammanfattningvis berättade intervjuobjektet att han arbetade på IT-avdelningen som informationssäkerhetssamordnare, vilket han har gjort de senaste 5 åren. Han arbetar för hela kommunen, men befinner sig på IT-enheten. Intervjuobjektet har varit en del av MSB:s enkätundersökning och således svarat på enkätfrågorna och dessutom tagit del av resultatet av undersökningen. Gällande informationssäkerhetspolicy så har kommunen en sådan som skapades 2015. Vidare skapades även riktlinjer för informationssäkerhet samtidigt som denna informationssäkerhetspolicy. Det finns inga planer på att revidera informationssäkerhetspolicyn. Däremot finns det planer att komplettera riktlinjerna med "Riktlinjer för Systemägare och Systemförvaltare" Intervjuobjektet var med vid skapandet av den och ansvarar även för att ta upp policyn för revision.

Gällande utbildning använder sig kommunen utav MSB:s verktyg DISA, men ingenting annat. Däremot menar intervjuobjektet att dessa riktlinjer som nämndes tidigare finns som stöd. Dessutom har användningen DISA förbättrats sedan införandet av "certifikat" och bevis kom till. Dessa bevis skickades till ledningscheferna när en anställd genomfört utbildningen och klarat den med godkänt resultat. Detta fanns enligt intervjuobjektet inte tillgängligt för mer än ett år sedan.

Vidare tar kommunen hjälp från IIS (Internetstiftelsen i Sverige) där en specifik person har lagt upp material som inkluderar utbildning och kurser. Intervjuobjektet tipsade oss om att kolla upp henne då hon är en "ikon" inom informationssäkerhet.

Fr.o.m fråga 17:
K6: Bra.. Eh, alltså vi betraktar efterlevnaden i just det kravet att alla anställda ska ha genomgått DISA. Det har vi lyckats med. I övrigt så tror jag inte vi skiljer oss från kommunerna i allmänhet, vi.. Även om systemförvaltning inte finns med som affärskapitel i ja, standarder för informationssäkerhet och betraktas som en självklar förutsättning för att drifta IT-stöd, och i verkligheten får jag arbeta mycket med att etablera systemförvaltning, se till så att det finns utsedda systemförvaltare och att systemförvaltarna vet vad de ska göra. Så att i praktiken så uppfyller det en stor del av mitt arbete, alltså att få ordning på systemförvaltningen. Och den är ju bara ett måste. Och det betraktar jag också som en del utav vårt sätt att följa upp att man arbetar systematiskt och kontinuerligt. Det går ju inte att arbeta med systemförvaltning utan att man ska behöva ta ställning till en hel del informationssäkerhetskrav. Alltså det vill jag också räkna in i vårt jobb.
N: Så lite avslutande frågor då: Vad upplever du är den största utmaningen när det kommer till arbetet med informationssäkerhetsarbetet på just eran kommun?
K6: Ja, det är ju fortfarande att få ledningen på banan. Att ha möjligheter att finnas med på styrelsemöten och annat och berätta om viktiga punkter och att ge utbildningar på hur det

faktiskt ser ut och vad som återstår att göra. Nu har väl jag turen att ha en tämligen intresserad IT-chef och det är inte alltid att det ser ut så, men IT-chefen tycker jag.. att han gör det han kan för att få upp vissa saker. Och eh, så att ja. Det innebär att vi jobbar inte i ett vakuum, utan vissa saker kommer faktiskt gå när iallafall kommunledningsförvaltningens chefer träffas. Dom cheferna; alltså vi pratar om bl.a. kansli, ekonomi och personal osv.. Där är det tämligen, då går det undan. Det är enkelt att få till informationsträffar. Det är lite besvärligare med våra traditionella nämnder alltså. Som skola. Men, De är en stor skillnad jämfört med fem år sedan när jag började. Innan jag började så bedrevs ju inget systematiskt arbete överhuvudtaget med informationssäkerhet. Så att vi har jobbat, skaffat en plattform under de här fem åren. Vi betraktar det att vi har kommit en bra bit på vägen, men självklart är vi ju medvetna om allt som återstår. Det som jag har lyckats också rätt bra med är att få till en, ja, att hantera informationskrav, då risk-och sårbarhetsanalyser inför stora förändringar när man gör en upphandling av IT-system. Det, och nu också sedan en månad tillbaka så har vi lanserat en checklista som ska följas vid upphandling och där har vi lagt in mängder av informationssäkerhetskrav. Detta räknas vi nog att det ska finnas med i upphandlingarna framöver. Vi betraktar det som ett extra förkontroll och även upphandling.

N: Det är jättebra. Och då slutligen till sista frågan: hur anser du att attityden mot informationssäkerhet är hos de anställda: till exempel när de ska utföra utbildningar såsom DISA. Vad har de för attityd mot informationssäkerhet?

K6: Ja, allmänt är det fortfarande lite väl beige och, men det är definitivt inte ointresse. Alltså jag tycker nog att vi kan säga att vi har de anställdas ögon och öron, de är öppna, vi har deras ögon, men många saker är ju så svåra att hantera. Så att man kanske tar lite väl lätt på informationssäkerheten. Men jag vill nog ändå mena att vakenhet är mycket mycket större, som de allra flesta kommuner har vi råkat ut för fishing-attacker och några har åkt dit varje gång och somd det har varit större attacker. Dessa attacker har inte bara drabbat de enskilda och deras dokumentation, utan även har drabbat kommunens grejer och det är faktiska händelser som inträffat som har höjt vakenheten. Men, ja alltså jag kan inte påstå att det finns ett motstånd att tänka informationssäkerhet, men det finns fortfarande en ovana att tänka mer systematiskt. Så vill jag svara generellt på den frågan.

N: Ja, men det tyckte jag ändå var ett väldigt klart svar på den frågan. Är det någonting som du känner att du vill tillägga till intervjun eller känner du dig nöjd med dina svar? …….För att jag är väldigt nöjd iallafall.

K6: Ja, det är väl det att jag tycker att det är bra att MSB äntligen börjar intressera för kommunerna också. Eftersom det är ju egentligen ingen skillnad i det fallet på offentlig verksamhet och. jag har väl tidigare tyckt (och tycker fortfarande) att MSB:s uppdrag har varit inte så sällan helt avgränsade till de statliga myndigheterna. Jag betraktar ju MSB definitivt som en myndighet som bör arbeta nationellt, och då kan man inte plocka bort 75-80% av Sverige och verksamheterna. Jag hoppas att de kommer att få lite utökad mandat så att det även ingår (I MSB:s uppdrag) att både följa, kontrollera och i vissa fall leda informationssäkerhetsarbetet i både landsting och kommun.

N: Ja, det är ju väldigt mycket som händer nu också i och med nya dataskyddsförordningen och så som man även måste få koll på inom kommuner också.

K6: Ja, jag räknar ju dataskyddsförordningen som enbart någonting positivt. Självklart för individerna. Men det hjälper till att pressa kommunens arbete och ja, insikter i vad som krävs för att uppfylla GDPR. Så den förändringen är bara en positiv grej.

N: Det tycker jag också! Men du, tack så mycket xx för att du ville ställa upp på en intervju. Vi kommer att återkomma till dig med det transkriberade materialet sedan så att du får godkänna allt du har sagt också. Så att du känner dig bekväm med det.

K6: Jadå.

N: Så, då skulle jag nog vilja tacka för mig.
K6: Ja, tack själv! Väldigt bra område som ni har valt att skriva om..
N: Ja, jag tycker också att det är väldigt intressant. Det finns så mycket inom det så att det blir nästan svårt att hamna på en tillräckligt smal nivå nästan.
K6: Jag förstår det. Informationssäkerhet är så gigantiskt och omfattande. Mm, jag hoppas också att ni hinner med några kommuner, för det finns ju några att välja emellan. Så man skaffar en överblick på vart kommuner befinner sig, men det är inte så lätt.
N: Nej verkligen inte, men tack återigen för din hjälp så hörs vi på mail snart då.
K6: Ha det!
N: Ha en bra dag!
K6: Detsamma.

7.2.7 Transkribering av intervju: Kommun 7 (K7)

Datum: 2017-05-04, 10:00
Intervjuobjekt: K7
Intervjuare: N (Nelly Karlsson Åhlén)
Metod: Telefonintervju, inspelning av intervjun och transkribering efteråt.

K7: Nu är jag redo
N: Har du hunnit läsa igenom den här intervjuguiden som vi skickade ut?
K7: Yes, det har jag,
N: Super, ska vi sätta igång då?
K7: Japp, absolut kör!
N: Då vill jag att du berättar kort om din roll inom kommunen, vad du gör och hur involverad du är i informationssäkerhetsarbetet och vad du vet om det?
K7: Mm, ja. Jag jobbar då som kommunarkivarie så jag sitter på kommunkansliet på kommunstyrelsens förvaltning. Så jag har ju inget, om man ska säga så, utpekat ansvar för informationssäkerheten i min tjänst, men jag jobbar ju med dokumentationsfrågor i stort och då har det ju blivit naturligt för mig att komma in i det jobbet. Så nu har det blivit så att jag blivit sammankallande för en grupp där vi träffas olika personer inom kommunen för att samverka och diskutera kring informationssäkerhet. Så, ja så har jag också lite sådär med i den. Vad ska man säga? Jag hjälper till lite i den gruppen där vi träffas alla "PUL-ombud". Eller inte "vi", för jag är ju inte "PUL-ombud", men vi träffar "PUL-ombuden" i kommunen så det är lite sådana frågor också.
N: Hm Okej. Så hur upplever du att ni arbetar med informationssäkerhet på just er kommun? Är det något som ni arbetar aktivt med? Förutom då dessa möten och sådär.
K7: Jaa. Jag kom hit för snart två år sedan och då var väl det arbetet relativt vilande kan vi väl säga. Det som gjordes var väl på IT-avdelningen där man jobbade med IT-säkerhet och det har man ju gjort hela tiden. Men då ville jag liksom ha lite bättre koll på det och då blir det ju att vi startade upp den här gruppen då, vår informationssäkerhetsgrupp. För att då samordna då kommunens arbete med informationssäkerhet och liksom komma igång litegrann då, men där är vi ju fortfarande litegrann i en uppstartsfas i ja, vi börjar ta tag i de där frågorna, men vi har ju inte kommit jättelångt så att säga. Och nu så jobbar vi ju ganska aktivt, men då mer med personuppgiftsfrågor och så i och med den nya dataskyddsförordningen som kommer då, så det är väldigt mycket fokus på det just nu. Men just det, det ska jag säga också. Nu förutom de som jobbar med IT-säkerhet så har vi ju ingen person som är utpekad för att jobba med informationssäkerhet, men vi har precis nu rekryterat en. En strateg för informationsförvaltning som kommer iallafall, ja typ 50 % arbeta med informationssäkerhet och han börjar efter sommaren.
N: Det är ju jättebra!
K7: Mmm!
N: Vet du förresten om ni var en del av MSB:s enkätundersökning: "En bild av kommuners informationssäkerhetsarbete, 2015"?
K7: Jaa, vi besvarade den enkäten.
N: Okej, har du även tagit del utav resultatet som kom efter?
K7: Ja, det har jag gjort.
N: Jättebra. Vi har ju valt att fokusera på tre olika områden från den enkäten nu i vår C-uppsats och den första delen handlar om policy och styrande dokument, så att jag undrar egentligen om ni har en informationssäkerhetspolicy och när den skapades.

K7: Vi har en policy från 2014, sedan har det väl egentligen inte hänt så mycket mer med den, så det är egentligen hög tid att uppdatera den, men ja, det är väl en sak som vi behöver göra. Den gäller väl t.o.m. detta året och sen måste vi ta om den.

N: Okej, vet du vem eller vilken del av organisationen som skapade den?

K7: Eh, den personen som tog fram den hade någon projektanställning men är inte kvar inom kommunen nu så jag är inte säker, men det är ju kommunkansliet som ansvarar för policyn. Så jag skulle tro att den var, eller kom härifrån kommunkansliet.

N: Så du vet inte vad den här projektarbetaren hade för bakgrund eller så?

K7: Nej, det har jag faktiskt dålig koll på.

N: Okej.. Vet du hur ni arbetar för att era anställda ska vara införstådda med policyn?

K7: Om jag ska vara ärlig så arbetar vi nog inte alls med det i dagsläget. Utan det är mer, ja att den finns.

N: Okej ja.. Det är ju bra iallafall att den finns..

K7: Ja, men man skulle ju önska att man gjorde någonting av den också!

N: Absolut. Och då till utbildning och kompetensutveckling, hur arbetar ni med utbildning och kompetensutveckling av era anställda på kommunen? För att de ska förstå informationssäkerhet då.

H: Mm, ja. Vi har just nu.. Vi håller på med en sådan här NanoLearning-kurs men jag vet inte om du har sett dem?

N: Jo, jag läste faktiskt att ni var en av de kommuner som hade det nämligen! Jag var inne på denna "MonkeyJungle", eller vad heter det nu? Junglemap!!

K7: Ehhh Jungle, någonting sådant…Så det kör vi ju just nu alltså. Så det kommer ut små kurser som kommer i mailen till alla anställda. Så det är vi mitt uppe i så det är någon slags grundnivå på den utbildningen då den är väldigt basic. Men det är det vi har och har gjort hittills. Som sagt ligger ju då vårat fokus rätt mycket nu på dataskyddsförordningen. Så vi håller ju på med det och har skickat alla då som kan vara berörda av det arbetet på kurser. Från alla förvaltningar och bolag. Detta är ju en informationssäkerhetsfråga man hanterar.

N: Okej, upplever du att det har tagit lite fokus då från resterande frågor inom informationssäkerhet?

K7: Jaa, det får jag ju säga. Det är ju det som är fokus just nu.

N: Okej, men hur ser framtiden ut gällande utbildningar inom informationssäkerhet, är det då NanoLearning som är görningen eller har ni några andra planer också?

K7: Vi har inga mer planer just nu. Men vi får väl se när vi har, är färdiga med NanoLearning-kurserna så får vi väl göra en utvärdering och se hur det har fallit ut och så får vi ju se sen hur vi går vidare men vi har inga färdiga planer redan nu.

N: Okej, vet du hur ni jobbade med utbildning innan det här med "NanoLearning"?

K7: Såvitt jag vet så har det inte varit någonting innan, inte på övergripande nivå iallafall. Det har varit mer riktat till IT-säkerhet isåfall.

N: Hmm okej.. Och då till kontroll och uppföljning: vet du hur ni arbetar med kontroll och uppföljning inom informationssäkerhet?

K7: Vi har ju liksom inget samlat grepp om informationssäkerheten på det sättet, utan det är snarare olika delar som följs upp på olika sätt, för att IT-avdelningen följer ju upp och kontrollerar IT-säkerheten, så de har ju ett team som jobbar med det. Sen när det gäller personuppgifter så har vi ju "personuppgifts-ombud" och sådär som kontrollerar och hanterar personuppgifter. Sedan har ju jag då som kommunarkivarie utför ju tillsyn över arkivering- och dokumenthantering. Men ja, som sagt ingenting riktat mot just informationssäkerhet som helhet, utan det är ju just dessa delar då.

N: Okej, så att.. Vi har frågat andra kommuner tidigare och då får vi mest svaret att man jobbar med kontroll och uppföljning mest efter incidenter. Men att många ligger efter i att jobba med det kontinuerligt. Är det ungefär samma för er då eller?

K7: Ja, det skulle jag väl säga, vi har ju ingen plan så för att följa upp informationssäkerheten, nä, det har vi inte.

N: Hmm okej, men då tänker jag att vi går in på lite avslutande frågor. Så de är lite breda, men det är för att vi vill ha olika spridda svar. Så jag undrar vad du upplever är den största utmaningen när det kommer till arbetet med informationssäkerhet på just er kommun? Alltså vad som kommer bli utmanande att handskas med?

K7: Mm, alltså det som jag ser och tänker är väl egentligen att det är svårt att få de olika verksamheterna att avsätta den tiden och resurserna som krävs för att jobba med de här frågorna. Vi är en ganska liten kommun och administrationerna på alla förvaltningarna är ju ganska "slimmad" och därför är det väldigt svårt att hitta någon som har det utrymmet för att jobba aktivt med de här frågorna och de som har den kompetensen är engagerade i massa andra frågor, så att det är egentligen det svåra. Jag tror att viljan finns, men inte riktigt möjligheterna. Det är mycket vi vill göra, men vi har inte riktigt folk till det, tyvärr. Men förhoppningsvis blir det ju lite bättre, för nu får vi ju åtminstone en tjänst som är dedikerad åt informationssäkerhetsarbete. Så kommer den strategen, så får vi ju se vad som händer. För det har ju också varit lite utav en brist innan; att vi inte har haft någon som har haft det här i sin tjänst, så det har ju varit en utmaning. Så nu får vi åtminstone det.

N: Det är ju jättebra! Men hur anser du då att attityden från de anställda är mot informationssäkerhet? Hur tacklar dom det generellt sätt?

K7: Generellt sätt så skulle jag nog säga att det är nog en ganska positiv inställning när man pratar om de här frågorna. Att man tycker att det är viktigt och att man vill göra rätt. Men sen är det ju kanske inte så prioriterat som jag kanske skulle önska, p.g.a. de skälen som jag pratade om innan. Men sen ser det ju ganska så olika ut i olika verksamhetsgrenar. De som jobbar mycket med sekretess och människor, t.ex. socialtjänsten. De har ju en större medvetenhet inom de här frågorna upplever jag, en större vilja att jobba med det. De är ganska duktiga på det skulle jag säga., på vår socialförvaltning. Medan man inom andra förvaltningar kanske inte tar det lika allvarligt. Till exempelvis våra utbildningsförvaltningar. Alltså skolan, där tycker jag att vi har brister. Där tror jag inte riktigt att man förstår utmaningen i det här. Så ja väldigt varierande.

N: Ja, vilket kanske egentligen är lite lustigt för det är ju inte så komplicerat som man vill tro att det är.

K7: Ja, men jag kan väl känna att det beror lite på sådär vilken grundinställning man har, till exempel när det kommer till socialtjänsten är ju deras första tanke att "ingen får komma till skada", liksom i allt jobb de gör och då blir det en naturlig fortsättning i deras arbete att tänka på det även med informationen. Medan man till exempel inom skolan så är väl första tanken när man jobbar att allting ska vara så smidigt som möjligt. Att allt ska gå så snabbt och lätt och när eleverna har idéer vill man ju ta vara på dem. Och då kommer kanske dessa frågor kanske mer i vägen och är jobbiga och ställer till det. Så att, så kan jag känna ibland. Beror liksom lite ibland vad man kommer ifrån för kultur i en verksamhet.

N: Verkligen. Då tror jag att jag har fått det jag vill ha av dig, jag tycker att du har gett mig bra svar. Om inte du vill tillägga något inom området?

K7: Inte vad jag kommer på men.. Nä, jag tror inte det! Men om det är någonting får du ju gärna höra av dig, ja om du upptäckt att du har missat något!

N: Ja, jättebra! Jag hör ju såklart också av mig sedan med det transkriberade materialet, sen också så att du kan godkänna vad du har sagt så att det känns okej med dig också, innan vi lägger in det i uppsatsen.

144 K7: Okej, ja men det är bra. Men dåså.
145 **N: Tack så mycket återigen för att du ville ställa upp på en intervju! Ha en bra dag!**
146 K7: Inga problem, lycka till med uppsatsen nu!

7.2.8 Transkribering av intervju: Kommun 8 (K8)

Datum: 2017-05-05, 10:00
Intervjuobjekt: K8
Intervjuare: S (Sofia Söderström)
Metod: Telefonintervju, inspelning av intervjun och transkribering efteråt.

S: Har du någon fråga eller är det bara för oss att köra igång?
K8: Det är bara att köra igång.
S: Vill du berätta lite kort om din roll inom kommunen?
K8: Ja, jag har kommunarkivarie.
S: Hur länge har du haft den positionen då?
K8: Till hösten blir det två år.
S: Hur involverad är du i informationssäkerhetsarbetet?
K8: Ehm, det var ju såhär, jag skickade väl över, vi har alltså tagit fram en informationssäkerhetspolicy som jag skrev tillsammans med kommunjuristen. Så nu så är det att än så länge så har vi inget arbete rent konkret. Vi har precis anställt en till jurist som ska jobba med informationssäkerhet och den nya dataskyddsförordningen. Och börjar i augusti, och då är det tänkt att då drar man igång ett stort projekt kring informationssäkerhet. Så just nu kan man säga att vi inte har något arbete.
S: MSB:s enkätundersökning, En bild av kommunernas informationssäkerhetsarbete 2015, var ni en del av den?
K8: Jag har svårt att tro det. Men jag har faktiskt ingen aning alls om det.
S: Du nämnde att ni har en informationssäkerhetspolicy, samt att det var du och en jurist som skapade den, när skapade ni den?
K8: Den skrevs förra sommaren och den togs nog i fullmäktige kanske i september 2016 eller någonting. Där på hösten iallafall, tidigt på hösten.
S: Är det du som är ansvarig för policyn i dagsläget eller vem är det?
K8: Nä, det borde vara juristen som är ansvarig. Men det är som sagt lite oklart då vi någon som konkret jobbar med det än.
S: Arbetar ni på något speciellt sätt för att era anställda ska vara införstådda med policyn?
K8: Nä inte än. Förhoppningsvis, vi får återkomma till hösten så kanske vi har bättre svar.
S: Vårt huvudfokus ligger på utbildning och kompetensutveckling av anställda, arbetar ni med detta i dagsläget?
K8: Nej.
S: Arbetar ni med kontroll och uppföljning?
K8: Nej, men sen finns det ju en tanke framåt för vad som ska göras sen.
S: Några avslutande frågor som är mer generella. Vad upplever du idag är den största utmaningen i arbetet med säkerheten?
K8: Ja alltså i vårt falls kommun är det ju såhär att vi har gått över till Google. Och det är bestämt att vi ska ha molnbaserade tjänster för allting. Även verksamhetssystemen och så. Och just, i och med, tanken är ju att vi ska hantera alla filer och mejl och allting sånt där i Google så är ju det den absolut största informationssäkerhetstwisten vi har. Att man vet inte hur man ska hantera det, det finns inga tydliga riktlinjer, där är det liksom som ett svart hål. Och det är väl ungefär som att de flesta anställda är ju medvetna om det. Men det finns inga direktiv hur man kan hantera det. Så det är den största, och det kommer även vara den största utmaningen när vi väl börjar jobba med det.

S: Har du någon uppfattning om den generella attityden mot informationssäkerhet hos de anställda idag?

K8: Jag tror nog att man tycker det är viktigt. Och man kan ju se, att i och med att vi har infört Google, och det är sen snart drygt ett år tillbaka, så är det ju någonting man diskuterar hela tiden. Och att det inte får vara såhär ungefär, och att man har liksom egna exempel, det här, vet ni vad som hände ungefär. Så jag skulle väl säga att det finns en medvetenhet om det, men inga redskap för att kunna hantera det.

S: Har ni någon mer framtid- och utbildningsplan inom kommunen?

K8: Nä inte mer än att vi ska göra ett stort projekt till hösten. Och där kommer det vara väldigt mycket utbildning, men jag tror också att det kommer vara väldigt mycket att försöka formulera krav på främst våran IT-verksamhet. Som inte är väl dom som är mest medvetna med problemet.

S: Innan vi avslutar, har du någon fråga eller någonting du vill lägga till?

K8: Nä. Om det är någonting ni har glömt får ni återkomma. Ni får jättegärna skicka ett exemplar på rapporten sen när den är klar.

S: Självklart, det gör vi jättegärna. Du kommer även få den transkriberade intervjun för godkännande.

K8: Ja.

S: Toppen, då hörs vi om ett tag. Tack hej!

K8: Ja lycka till! Hej

7.3 Initialt e-postmeddelande

Examensarbete: Informationssäkerhet, Lunds Universitet

Nelly Karlsson Ahlén <nellyahlen@gmail.com> 7 apr.
till kommun

Hej,

Vi heter Sofia Söderström och Nelly Karlsson Ahlén och vi läser sista terminen på det Systemvetenskapliga kandidatprogrammet på Lunds Universitet. Vi kontaktar Er gällande vår c-uppsats som handlar om informationssäkerhetsarbete i kommuner i Sverige. Vårt arbete grundas i en undersökning genomförd av Myndigheten för samhällsskydd och beredskap (*En bild av kommunernas informationssäkerhetsarbete*, MSB, 2015). I undersökningen framgår det bland annat att 136 av de 236 deltagande kommunerna inte erbjuder utbildning i informationssäkerhet för kommunens medarbetare. Därför kommer vårt fokus i uppsatsen ligga på vikten av utbildning och kompetensutveckling inom kommuner.

Vår fråga är därför om Ni vill medverka i en telefonintervju angående detta som är beräknad att ta mellan 15-30 minuter. Vi ser helst att detta e-postmeddelande vidarebefordras till berörda parter, förslagsvis informationssäkerhetschef/-samordnare, it-chef, jurist, arkivarie, verksamhetschef eller annan relevant person inom kommunen.

Om Ni vill medverka i en telefonintervju skickas en intervjuguide ut innan intervjun, för att Ni skall kunna förbereda innan intervjun äger rum, och således känna Er bekväma i situationen. Om möjligt ser vi gärna att telefonintervjun äger rum innan fredagen 5/5 2017.

Hoppas att Ni vill delta och därmed hjälpa oss i vårt uppsatsarbete.
Bifogar undersökningen som gjorts utav MSB.
Tack på förhand!

Vänligen,
Sofia Söderström 0768505671
Nelly Karlsson Ahlén 0707258484

MSB Undersökning
https://www.msb.se/RibData/Filer/pdf/27967.pdf

Referenser

Elektroniska källor:

Datainspektionen (2017a). *Dataskyddsreformen* [online] Datainspektionen.se
Avaliable: http://www.datainspektionen.se/dataskyddsreformen/
Accessed: 2017-05-08

Datainspektionen (2017b). *Dataskyddsförordningen* [online] Datainspektionen.se
Available:http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/
Accessed: 2017-05-08

Goede, C (2017). *Analysrapport informationssäkerhet i kommuner* [online] Informationssakerhet.se.
Available:https://www.informationssakerhet.se/nyheter/analysrapport-informationssakerhet-i-kommuner/
Accessed: 2017-04-25

Junglemap (2017a). *CISO* [online] Junglemap.com
Avaliable: http://www.junglemap.com/ciso
Accessed: 2017-05-08

Junglemap (2017b). *Customers* [online] Junglemap.com
Avaliable: http://www.junglemap.com/customers
Accessed: 2017-05-09

Kalmelid, K (2015). *Vad är informationssäkerhet?* [online] Informationssäkerhet.se
Available:https://www.informationssakerhet.se/Om-informationssakerhet-kon/vad_ar_informationssakerhet/
Accessed: 2017-04-25

Mitnick, K (2000). Reported in *The Economist* [online] Economist.com
Available: http://www.economist.com/node/1389553
Accessed: 2017-03-04

MSB (2011). *Datorstödd informationssäkerhetsutbildning för användare (DISA)* [online] msb.se
Available:https://www.msb.se/sv/Forebyggande/Informationssakerhet/Stod-inom-informationssakerhet/DISA--utbildning-informationssakerhet/
Accessed: 2017-04-23

MSB (2017). *Msb.se - About MSB* [online] msb.se
Available: https://www.msb.se/en/About-MSB/
Accessed: 2017-04-24

NE (2017). *Policy* [online] Nationalencyklopedin.se
Availabe: http://www.ne.se/uppslagsverk/ordbok/svensk/policy
Accessed: 2017-04-25

Regeringskansliet (2017). *Kommuner och landsting* [online] Regeringskansliet.se
Available: http://www.regeringen.se/regeringens-politik/kommuner-och-landsting/
Accessed: 2017-04-25

SKL (2017a). *Kommuner och landsting* [online] Skl.se.
Available: https://skl.se/tjanster/kommunerlandsting.431.html
Accessed: 2017-04-25

SKL (2017b). *Så styrs en kommun* [online] Skl.se.
Available:https://skl.se/demokratiledningstyrning/politiskstyrningfortroendevalda/kommunaltsjalvstyresastyrskommunenochlandstinget/sastyrskommunen.735.html
Accessed: 2017-04-25

SKL (2017c). *Kommunens ansvar* [online] Skl.se.
Available:https://skl.se/integrationsocialomsorg/socialomsorg/barnochunga/placeradebarnochunga/ensamkommandebarnochunga/kommunensansvar.3425.html
Accessed: 2017-04-24

SKL (2017d). *Informationssäkerhet*. [online] Skl.se.
Available:https://skl.se/naringslivarbetedigitalisering/digitalisering/informationssakerhet.1238.html
Accessed: 2017-04-25

Tryckta källor:

Agarwal, A. and Agarwal, A., (2011). The security risks associated with cloud computing. *International Journal of Computer Applications in Engineering Sciences*, *1* (pp.257-259).

Amankwa, E., Loock, M. and Kritzinger, E., (2014). A conceptual analysis of information security education, information security training and information security awareness definitions. *Internet Technology and Secured Transactions (ICITST), 2014 9th International Conference for* (pp.248-252). IEEE.

Amankwa, E., Loock, M. and Kritzinger, E., (2015). Enhancing information security education and awareness: Proposed characteristics for a model. *Information Security and Cyber Forensics (InfoSec), 2015 Second International Conference on* (pp.72-77). IEEE.

Andersson, B.-E. (1994). *Som man frågar får man svar*. Kristianstad: Rabén Prisma.

Andress, J. (2011). *The Basics of Information Security*. Waltham: Syngress Media.

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

Conner, D.R. and Patterson, R.W., (1982). Building commitment to organizational change. *Training & Development Journal*.

Dewey, C.M. and Shaffer, C., (2016). Advances in information Security Education. *Electro Information Technology (EIT), 2016 IEEE International Conference on* (pp.0133-0138). IEEE.

Dlamini, M.T., Eloff, J.H. and Eloff, M.M., (2009). Information security: The moving target. *Computers & Security*, *28*(3) (pp.189-198).

Gollmann, D. (2011). *Computer Security.* 3. uppl. West Sussex: John Wiley.

Gonzalez, J.J. and Sawicka, A., (2002). A framework for human factors in information security. *Wseas international conference on information security, Rio de Janeiro* (pp.448-187).

Höne, K. and Eloff, J.H.P., (2002). Information security policy—what do international information security standards say?. *Computers & Security*, *21*(5) (pp.402-409).

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

Kruger, H.A. and Kearney, W.D., (2006). A prototype for assessing information security awareness. *computers & security*, *25*(4) (pp.289-296).

Layton Sr T.P. (2005). *Information Security Awareness*. Authorhouse.

LeVeque, V. (2006). *Information Security – A Strategic Approach.* Hoboken, New Jersey: John Wiley & Sons, Inc.

Martins, A. and Elofe, J., (2002). Information security culture. *Security in the information society* (pp.203-214). Springer US.

MSB (2012). *Kommunens informationssäkerhet – en vägledning.* msb.se

MSB (2015). *En bild av kommunernas informationssäkerhetsarbete 2015.* msb.se

MSB (2016). *Informationssäkerheten i Sveriges kommuner. Analys och rekommendationer utifrån MSB:s kommunenkät 2015.* msb.se

Olofsson, M. (2016). *Höj säkerhetshetsmedvetandet hos de anställda med NanoLearning*. Junglemap.com

Pahnila, S., Siponen, M. and Mahmood, A., (2007). Employees' behavior towards IS security policy compliance. *System sciences, 2007. HICSS 2007. 40Th annual hawaii international conference on* (pp.156b-156b). IEEE.

Schlienger, T. and Teufel, S., (2002). Information security culture. *Security in the Information Society* (pp.191-201). Springer US.

Siponen, M.T., (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1) (pp.31-41).

Thomson, M.E. and von Solms, R., (1998). Information security awareness: educating your users effectively. *Information management & computer security*, *6*(4) (pp.167-173).

Thomson, K.L., von Solms, R. and Louw, L., (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, *2006*(10) (pp.7-11).

Whitman, M.E. och Mattord, H.J., (2008). *Management of information security*. 2 uppl. Canada: Course Technology, Cengage Learning

Whitman, M.E. och Mattord, H.J., (2011). *Principles of information security*. Cengage Learning.

Whitman, M.E., Townsend, A.M. and Aalberts, R.J., (2001). Information systems security and the need for policy. *Information security management: Global challenges in the new millennium* (pp. 9-18). IGI Global.

Wylder, J., (2003). *Strategic Information Security*. United States: CRC Press.