Uppsala universitet
Inst. för informationsvetenskap/Data- och systemvetenskap

# En kyrklig organisations informationssäkerhet

## – Policyimplementation och motivation till efterlevnad av policy

Kurs: Examensarbete, informationssystem
Nivå: C
Termin: HT-13
Datum: 2014-01-10

**Abstract**
The following study is dedicated to investigate what kind of problems an organisation might stumble upon in the process of implementing a policy related to information security. Alongside investigating the eventual problems occurring in the implementation process of an organisation, the study also sets out to analyse how an organisation can motivate staff in order to follow the guidelines of a policy. The collection of empirical data was done using interviews. In order to seek answers to our research questions a theoretical background is presented that illustrate the need for information security after which motivational theories are applied to our collected data.

To summarise the results of the study we find a gap of knowledge between the employees of the organisation. The organisational level of an employee together with the degree of participation in working with a policy seems connected to both the employee's knowledge of a policy as well as how well the employee are motivated to learn about and follow the guidelines provided from a policy.

**Nyckelord**:
Svenska kyrkan, informationssäkerhetspolicy, implementation, efterlevnad och motivation.

# Innehåll

# 1. Inledning

I detta kapitel presenteras motivet för undersökningen samt vilka problem vi ämnar lösa. Ämnets bakgrund presenteras samt organisationen undersökningen utförs hos. Därefter följer presentation av problembeskrivning och forskningsfrågor. Till sist presenteras syftet med uppsatsen med avgränsningar samt vilken målgrupp uppsatsen avser att inriktas mot.

## 1.1 Bakgrund

Idag använder allt fler organisationer IT-system för att underlätta arbetet för sina anställda. IT-systemen har blivit ett viktigt verktyg använt till många arbetsuppgifter. IT-systemet kan till exempel styra andra maskiner som konstruerar bilar, användas för att skriva dokument, skicka e-mail och liknande. Många organisationer är beroende av sitt IT-system och utan det skulle vissa arbetsuppgifter inte kunna utföras och andra skulle ta längre tid. Om IT-systemet skulle bli skadat och inte vara tillgängligt kan det skada organisationen ekonomiskt. Det är också vanligt att organisationerna lagrar känslig information på sina IT-system som inte får läsas av obehöriga. Det kan vara företagshemligheter, patent, personliga uppgifter eller liknande.

För att göra IT-systemet säkrare sätts tekniska lösningar i bruk. Brandväggar skyddar systemet från att obehöriga kan ansluta till systemet. Användare av systemet måste ha ett användarnamn och lösenord. Lösenordet måste ofta vara av en viss längd och bytas regelbundet. Information krypteras och lösenordsskyddas. Det finns även administrativa lösningar. Genom att skriva policydokument och rutiner användarna ska följa kan säkerheten förbättras. Förutsatt att användaren följer dem.

Användaren är ofta den svagaste länken i ett IT-system. Därför är det viktigt att användarna blir utbildade på rätt sätt när en ny policy ska implementeras (Aloul, 2012). Det är också viktigt att motivera användaren varför säkerhetsåtgärderna ska följas. Det spelar ingen roll hur säkert ett IT-system är om en användare ger ut information kan ge en obehörig tillgång till systemet. Det samma gäller policydokument. Det spelar ingen roll hur bra en policy är skriven om de anställda inte följer den.

Detta ämne valdes eftersom vi båda har ett intresse inom informationssäkerhet och organisationsstyrning. Vi valde att utföra undersökningen hos Uppsala kyrkliga samfällighet eftersom vi tidigare hade haft kontakt med dem och deras organisation var intressant för vår undersökning. Det är en del av Svenska Kyrkan och är en religiös organisation. Unikt med undersökningen är att organisationer av den här typen sällan undersökts inom området. Att genomföra en studie om informationssäkerhet och anställdas motivation till efterlevnad av policy blir således synnerligen intressant då undersökningen hjälper till att fylla detta, tämligen outforskade, område genom bidrag med ny kunskap efter avslutad studie.

## 1.2 Problemformulering

Att en organisation arbetar fram policydokument i avseende att styra personalen mot ett eftersträvat beteende är inget ovanligt och många gånger nödvändigt. Vem som helst kan fatta ett beslut gällande förändring av en annan individs handlingssätt men mänsklig fri vilja lämnar utrymme för individen i fråga att mottaga beslutet på valfritt sätt. Delade viljor förekommer överallt i vår vardag men även på arbetsplatser vilket organisationsledningen inte alltid lägger märke till och bör således uppmärksammas mer för att ena individers vilja (Dermer och Lucas, 1986).

Utmaningen hos beslutsfattare ligger således inte i beslutandeprocessen i första hand, utan snarare i var besluten tar vägen i avseende att få genomslag. Denna undersökning ägnas åt att utreda hur Uppsala kyrkliga samfällighet implementerat IT-relaterade policydokument och utröna huruvida policydokumenten genomsyrat organisationen. Om organisationen kan stoltsera med en lyckad implementation eller om glapp i kunskap eller utbildning lämnas till undersökningen.

Anledningarna till varför en individ följer eller inte följer beslut eller en gällande policy kan vara många och varierande. Vad anställda motiveras av blev därför en faktor värd att undersöka för att ta reda på om eventuella brister gällande efterlevnad av policy kunde härledas till motivationsbrist bland personalen. Ovanstående resonemang leder oss till nästkommande kapitel - vår frågeställning.

## 1.3 Frågeställning

Följande forskningsfrågor ämnar undersökningen besvara:

- *Hur mynnar IT-relaterade policydokument ut till organisationens olika delar?*
- *Hur kommer anställda i kontakt med policydokument och hur motiveras de att följa dem?*

## 1.4 Syfte

Syftet med studien är att undersöka hur en kyrklig organisation arbetar med att se till att IT-relaterade policydokument mynnar ut i alla delar av organisationen. I kapitlet om bakgrund nämns att liknande studier på den här organisationstypen sällsynta. Därav ämnar att undersökningen bidra till att fylla en del av det outforskade området i avseende att väcka ytterligare intresse att fortsätta utforska detta område i framtiden. Vår förförståelse är att det kan vara lättare att utforma ett policydokument än att få organisationen att agera enligt gällande policy på individnivå. På individnivå kan en mängd faktorer väga in vid mottagande och acceptans av styrningsbeslut. I undersökningen ämnar vi därför att söka svar på hur en organisation kan motivera personal till att mottaga och följa en policy.

## 1.5 Avgränsning

Under begränsning av given tidsram avgränsas studien till hur Uppsala kyrkliga samfällighet arbetar med att se till att IT-relaterade policydokument mynnar ut i alla delar av organisationen samt hur organisationens anställda motiveras att följa dess riktlinjer. Arbetet med utbildning om policydokument granskas genom studerande av hur policydokumenten är tänkta att färdas genom organisationens nivåer för att sedan se hur mellanhänder mottar och vidareförmedlar den. Tillsist undersöks hur anställda längre ned i organisationen får reda på information om relevanta policydokument samt deras kunskap om dem.

Hur de anställda motiveras att följa policydokument behandlar vi främst ur ett teoretiskt perspektiv. Först studeras dock hur anställda kommer i kontakt med relevanta policydokument. Sedan om det pratas om gällande IT-relaterade policydokument i arbetet eller om det på annat vis pratar om regler och riktlinjer gällande IT-området samt om de har en ansvarsroll i vidareförmedling av IT-relaterade policydokument. Detta för att skapa underlag för en diskussion om vad brister kan bero på varpå vi riktar in oss på motivation hos de anställda.

Undersökningen lägger ingen vikt vid att studera andra områden av personalens beteende och arbetsuppgifter på grund av tidsramen då vi eftersträvar ett djup i resultat. Om en anställd generellt är motiverad till andra delar av arbetet är inget vi ämnar undersöka. Tidsramen för undersökningen tillåter oss ej att ta hänsyn till detta. Teoretisk koppling till motivation och motivationsteorier berör alltså primärt anställdas motivation gällande just IT-relaterade policydokument. Utöver det syftar vi genomgående till policydokument relaterade till IT-säkerhet om inget annat anges.

## 1.6 Målgrupp

Forskningsbidraget i uppsatsen väntas få ett flertal intressenter. Potentiella läsare är kursens nuvarande medstudenter, handledare, eventuella forskare och framtida studenter med inriktning informationssystem. Studenter med närliggande eller liknande forskningsområden väntas även finna denna rapport läsvärd. Trots inriktning mot IT-relaterade policydokument väntas även studenter med inriktning mot organisationsstyrning och management delvis kunna dra nytta av våra slutsatser vid egen forskning.

Slutligen bör inte vårt praktiska kunskapsbidrag förkastas. Organisationen vi arbetat med är med största sannolikhet intresserade av vårt resultat. Särskilt om utredningen påvisar brister. Medvetna om att Uppsala kyrkliga samfällighet står inför en omstrukturering möjliggör det att situationen i framtida utformning ser annorlunda ut där uppmärksammade potentialer redan har förbättringsåtgärder inplanerade. Eventuella brister organisationen upptäckt på egen hand är dock nödvändigtvis inte de vår undersökning stött på. Uppsatsen avser att skapa mervärde i form av att undersökningen gjorts på organisationens verksamhet och därav kan möjliggöra förbättring där rutiner inte fungerar enligt avsikt. Även andra pastorat kan ta nytta av vår undersökning. Andra pastorat med en organisationsstruktur liknande den Uppsala kyrkliga samfällighet har, skulle kunna använda undersökningen för att uppmärksamma liknande problem i verksamheten.

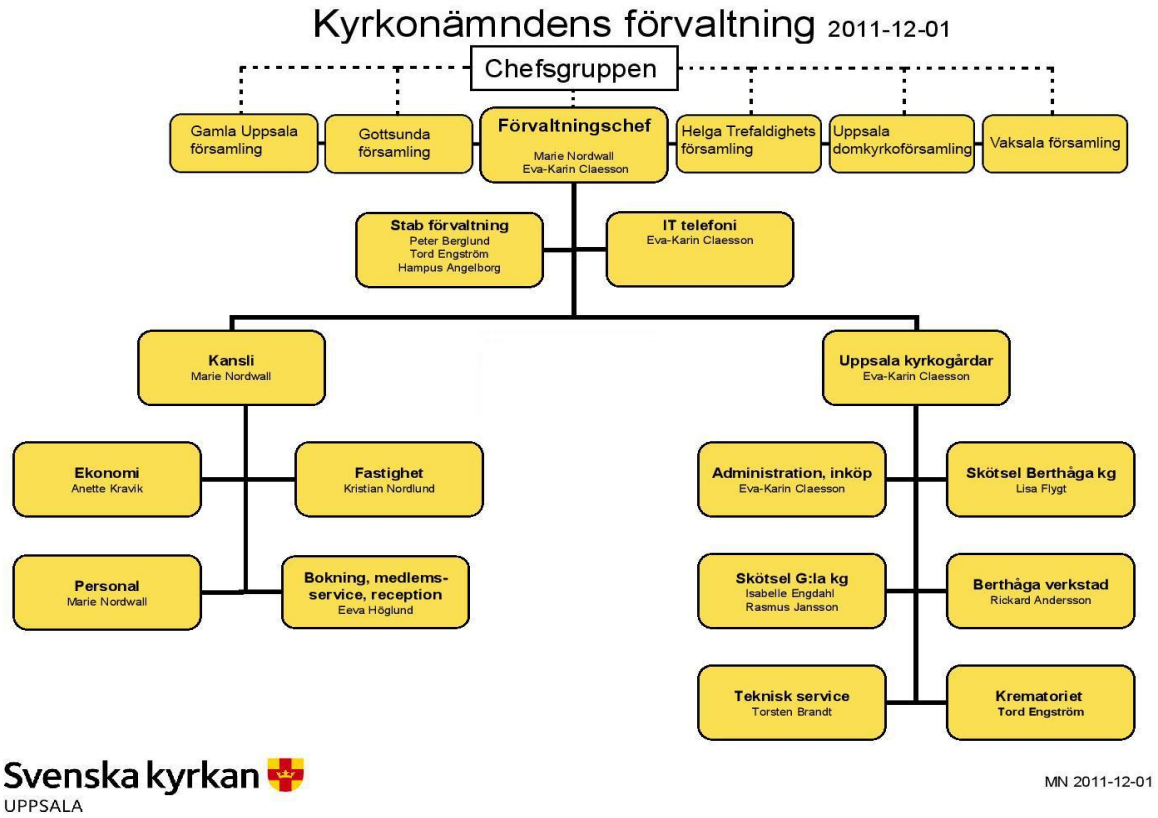
# 2 Metod

Följande kapitel är dedikerat till presentation av metodval och tillvägagångssätt för att samla in och behandla data. Undersökningen baseras på intervjuer och detta kapitel berör insamling av data, urvalsprocess vid val av informanter, beskrivning av intervjuerna samt hur vi ämnar behandla det empiriska underlaget från intervjusvaren. Detta för att precist och metodiskt genomföra undersökningen och därmed öka dess trovärdighet.

## 2.1 Val av empiri

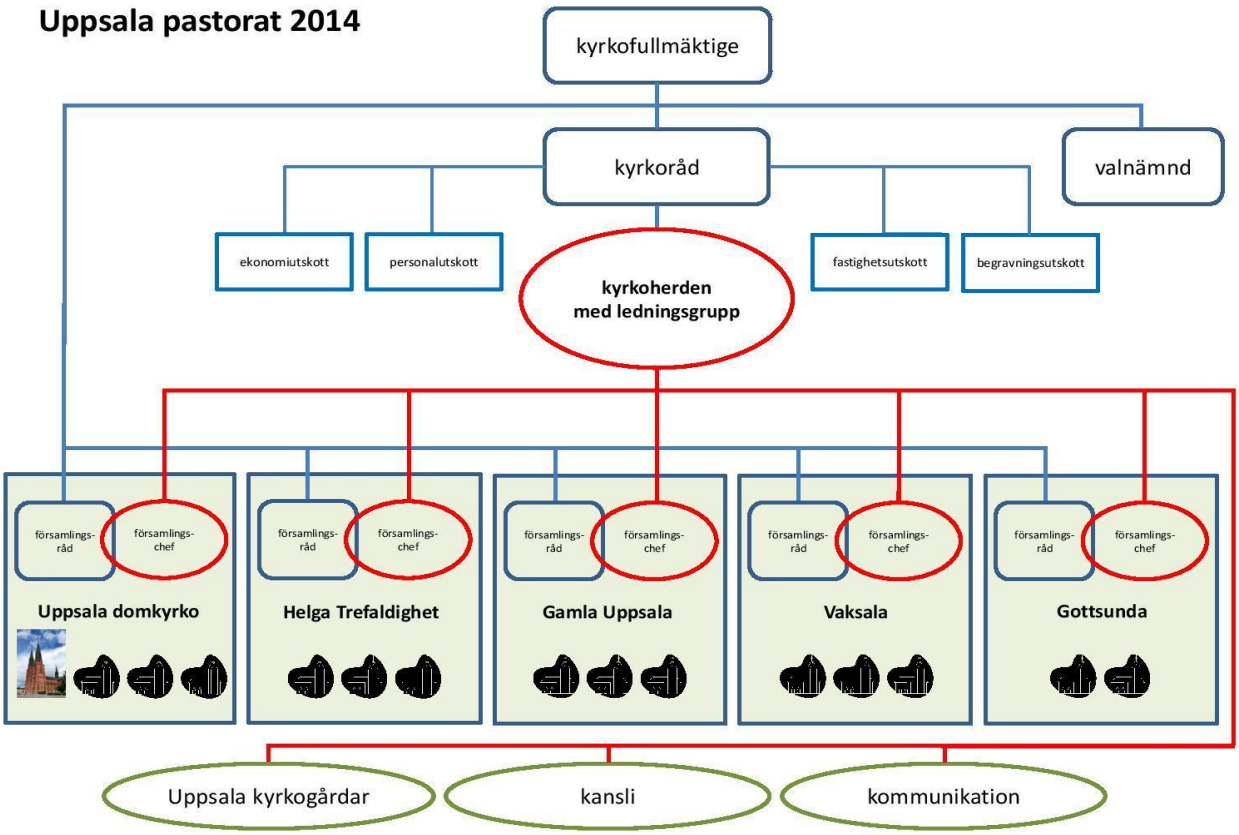
Uppsala kyrkliga samfällighet valdes som mål för undersökningen på grund av dess organisationstyp då den är intressant av många anledningar. Organisationen är en del av Svenska kyrkan och undersökningar av denna typ av organisation är sällsynt tidigare. Uppsala kyrkliga samfällighet består av Uppsala kyrkogårdsförvaltning samt fem församlingar (Gamla Uppsala församling, Gottsunda församling, Helga Trefaldighets församling, Uppsala domkyrkoförsamling och Vaksala församling) där varje församling har en kyrkoherde ansvarig för församlingen.

Uppsala kyrkogårdsförvaltning leds av två personer vilka även är ansvariga för Uppsala kyrkogårdar och kansliet. Uppsala kyrkogårdar består av sex delar: administration och inköp, skötsel av Berthåga kyrkogård, skötsel av Gamla kyrkogården, Berthåga verkstad, teknisk service och krematoriet. Kansliet består av fyra delar: ekonomi, fastighet, personal och bokning, medlemsservice och reception. Varje del har en ansvarig person för verksamheten. Kyrkoherdarna och förvaltningscheferna är tillsammans ansvariga för Uppsala kyrkliga samfällighet. Anställda på Uppsala kyrkliga samfällighet har mycket frihet när de arbetar. Existerande policydokument är generellt utformade och täcker de viktigaste delarna av ett avsett område. Anställda är fria att bestämma hur de ska sköta sitt arbete och planera sin arbetsdag så länge de sköter sina arbetsuppgifter och inte bryter mot någon lag, policy eller rutin.




*Figur 1: Översikt över Uppsala kyrkliga samfällighet. Församlingarna och förvaltningscheferna är på samma nivå i chefshierarkin.*

Uppsala kyrkliga samfälligheten står inför en omorganisation 2014 och kommer bli ett pastorat. Den stora skillnaden blir förekomst av en högsta chef samt att en ledningsgrupp bestående av kyrkoherdarna kommer skapas.




*Figur 2: Översikt över pastoratet Uppsala kyrkliga samfällighet ska omorganisera sig till. Till skillnad från tidigare finns en högsta chef och alla kyrkoherdar bildar en ledningsgrupp.*

## 2.2 Forskningsparadigm

*"A paradigm is a set of shared assumptions or ways of thinking about some aspect of the world"* (Oates 2006: 282).

Att ta sig an ett problem utifrån en slags verklighetsuppfattning blir likt att genomföra en undersökning utifrån ett slags ramverk. Med samlade antaganden om verkligheten möjliggör tillvägagångssätt att genomföra forskning och skapa ny kunskap. Denna undersökning är genomförd med enligt kritisk realism som utgångspunkt enligt dess vetenskapliga metod.

Kritisk realism har rötter i positivismen och har till grund för verklighetsuppfattningen antagandet att vår omvärld bestämd och företeelser inte är slumpmässiga (Trochim och Donneley, 2006). Enligt positivismen kan vem som helst exempelvis observera att om de släpper ett föremål, kommer det falla till marken. Vilket objekt som helst och samma resultat. Detta fenomen kan bekräftas som en sanning och vi kan även med matematikens hjälp beräkna åtgången tid från släpp-ögonblicket till objektet når marken. Att detta blir en sanning bygger på verklighetsuppfattningen att vår värld består av en uppsjö av samband påverkande varandra. (Oates, 2006)

Kritisk realism avviker från positivismen genom erkännandet att ingen observation är felfri och att all teori kan förändras. Positivismen söker mätbara sanningar medan kritisk realism, strävar efter sanningen men, tar hänsyn till att en undersökning eller mätning inte är perfekt och därmed går en sanning inte att uppnå till fullo (Trochim och Donneley, 2006). Utrymme till ständig förbättring finns således.

Därför genomförs vår undersökning enligt den kritisk-realistiska vetenskapsfilosofin på grund av ett varmare mottagande av kvalitativ datainsamling då denna undersökning genomförs med intervjuer. Vi själva blir mätinstrument till insamlat resultat där utrymme för hermeneutiska tolkningar blir svårundvikliga. Objektivitet är dock eftersträvat i högsta grad. Därför används vårt teoretiska underlag till analys av empirisk data och därigenom stärka dragna slutsatser genom förankring i etablerad teori.

## 2.3 Datainsamling

Empiriskt underlag har samlats in genom intervjuer i en *fallstudie* (Yin, 2009). Besvarande av frågeställning ställer krav på att få en detaljerad bild av hur anställda runt om i en organisation förhåller sig till informationssäkerhetspolicyn och därför valdes att genomföra undersökningen som en *kvalitativ fallstudie*. För att undersöka vilka problem en organisation kan stöta på vid implementation av en informationssäkerhetspolicy anser vi att intervjuer lämpar sig väl. Med dessa intervjuer ämnar vi att uppnå en djupare förståelse för hur policyn är tänkt att mynna ut till organisationens olika delar samt hur de anställda kommer i kontakt med policyn och se hur de motiveras att följa den. Målet var att intervjua personal från så många områden som möjligt förutsatt att de använder IT-systemen. Vi har intervjuat personer ansvariga för att ta fram nya policydokument, anställda med vidareförmedlingsansvar samt anställda med uppgift att följa policydokumenten.

För att genomföra vår undersökning tog vi kontakt med Uppsala kyrkliga samfällighet som valdes på grund av dess unika organisationstyp. Vår förstudie pekar på att liknande studier hos denna typ av organisation är ytterst sällsynt och denna undersökning bör därmed kunna tillföra forskningsområdet ny information. Därefter blev vi härledda till en person ansvarig för bland annat framtagande av, förändring av och vidareförmedling av IT-relaterade policydokument inom organisationen. Efter ett möte med denna person fick vi en lista med lämpliga personer att intervjua och vi valde godtyckligt ut personer från olika delar av organisationen. Vi tog kontakt med dessa personer och bestämde sedan datum för intervjuerna. Inför intervjuerna hade frågor förberetts som var anpassade efter vilken position inom organisationen personen hade och vad vi ville få ut av intervjun. Intervjuerna spelades in och dokumenterades.

## 2.4 Intervjuer

Tidigare benämndes att intervjuer skulle genomföras och detta kapitel ägnas åt att beskriva hur intervjuerna genomfördes. Ett besök gjordes hos Uppsala kyrkliga samfällighets IT-stöd där vi träffade vår kontaktperson tillsammans med en kollega till denne vilket resulterade i kontaktuppgifter till antal personer och ett urval bland dessa fick ske. Nästkommande kapitel beskriver och motiverar urvalet mer i detalj. Avsikten med undersökningen är inte att hänga ut någon individ. Deras roller och namn behandlas därför enligt överenskommelse vid intervjutillfällena.

Tre nivåer av Uppsala kyrkliga samfällighet undersöks med hjälp av intervjuer med utvalda informanter organisationens olika delar. Eftersom varje enskild nivå har olika arbetsuppgifter resulterade detta i olika intervjumallar, var och en anpassad för att leda oss att besvara vår frågeställning.

### 2.4.1 Intervjuguide

Intervjuerna inleddes med frågor om informantens arbetsuppgifter och position. Beroende på position ställdes olika kategorier av frågor. Frågor till ledningen berörde främst hur informationssäkerhetspolicyn skall implementeras samt vilka medel som används till att föra ned policyn i organisationens lägre nivåer. Informanten från ledningen fick även frågor om hur de arbetar med uppföljning samt hur personalen motiveras till att följa policyn.

Till mellancheferna ställdes intervjufrågor om hur de uppfattar styrningsdirektiv och förhållningssätt till informationssäkerhetspolicyn från ledningen samt deras roll mellanchefer vid tillämpning av policyn och utbildning av medarbetarna vid berörda områden. Slutligen fick informanterna på medarbetarnivå frågor om hur de skolats in att förhålla sig till informationssäkerhetspolicyn. Varje informant tillfrågas huruvida de agerar i enlighet med policyn eller ej via frågor om deras beteende i arbetsplatsens datormiljö. Det ställdes även frågor om deras datorvanor. För en mer detaljerad intervjuguide, se bilaga A.

## 2.5 Urval

Möjligheten att intervjua alla inom Uppsala kyrkliga samfällighet för att uppnå ett optimalt resultat var inte genomförbart vare sig från vår sida i from av tilldelad tidsram eller från organisationen i from av resurser. På grund av detta har ett urval skett i mån av ömsesidiga resurser från bådas sida i strävan efter bästa möjliga resultat med givna resurser. Styrning mellan nivåer och enheter kan uppfattas olika. Spridda åsikter existerar även alltid inom organisationer och dessa varierar beroende på position och personliga intressen. (Dermer och Lucas, 1986). Därmed vill vi komma åt störst möjliga antal nivåer inom organisationen och på så vis bilda en uppfattning om hur Uppsala kyrkliga samfällighet arbetar med att se till att IT-relaterade policydokument mynnar ut i alla delar av organisationen. Även om organisationen i nuvarande skick styrs enligt en plan struktur finns olika nivåer att undersöka och delen av organisationen undersökningen omfattar visade sig ha tre olika nivåer.

Informanter valdes slumpmässigt utifrån dessa nivåer och antalet valda informanter från respektive nivå varierar beroende på tidsramens begränsning (Sargeant, 2012). Från ledningens sida eftersträvas vetskap om hur budskap om policydokument och dess innebörd förs vidare nedåt inom organisationen. Få personer är direkt beslutsfattande och således valdes en person från ledningen att intervjuas och på så vis ta reda på hur informationssäkerhetspolicyn är tänkt att förmedlas. På mellannivå gavs möjligheten att hålla två intervjuer. Hos dessa var avsikten att se om och hur de kom i kontakt med informationssäkerhetspolicyn samt om de besitter roller med ansvar att vidareförmedla policyn. Slutligen valdes två personer på medarbetarnivå och dessa befann sig således på längre organisatoriskt avstånd. Fler från denna nivå hade gärna intervjuats för att säkerställa eventuella samband men på grund av tidsbegränsningen begränsades undersökningen till två informanter.

Att risken för missuppfattningar ökar i och med varje nivå i en organisation är inte särskilt konstigt. I detta fall undersöks informationssäkerhetspolicyns implementation. Individers fria vilja måste finnas med i form av en risk om det finns utrymme att bryta mot policyn. Med ovanstående i beaktande är alla nivåer givetvis otroligt viktiga att komma åt. Organisatoriskt avstånd från beslutsfattare bör kunna utgöra en risk för avvikelser och därav har vi valt dessa personer för att få bästa möjliga omfattning inom uppsatsens tidsram.

## 2.6 Granskning av intervjuer

Varefter intervjuerna är genomförda och dokumenterade skall de granskas metodiskt. Med avsikt av att informanternas svar skall analyseras likvärdigt kommer svaren att analyseras genom vald teori. Till undersökningens delar berörande personalens efterlevnad samt deras vanor i arbetsplatsens IT-miljö jämförs befintliga policydokument med informanternas intervjusvar med avsikt att kartlägga hur verkligheten ser ut. Uppsatsen belyser säkerhetsaspekten med syfte om att belysa en potentiell hotbild. Därefter används Dermer och Lucas resonemang om eventuellt styrningsglapp samt McGregors *Theory X and Theory Y* tillsammans med Herzbergs *Two-factor theory* för att förankra slutsatser i analysen till vald teoretisk bakgrund.

## 2.7 Källkritik

Då teori om informationssäkerhet och IT har förändras mycket under tidens gång är det viktigt att inte allt för gamla källor används. Internetkällor och Wikipedia har undvikits men förekommer i enstaka fall där ingen papperskälla har hittats. För att teorier inte ska motsäga varandra har källor jämförts med varandra.

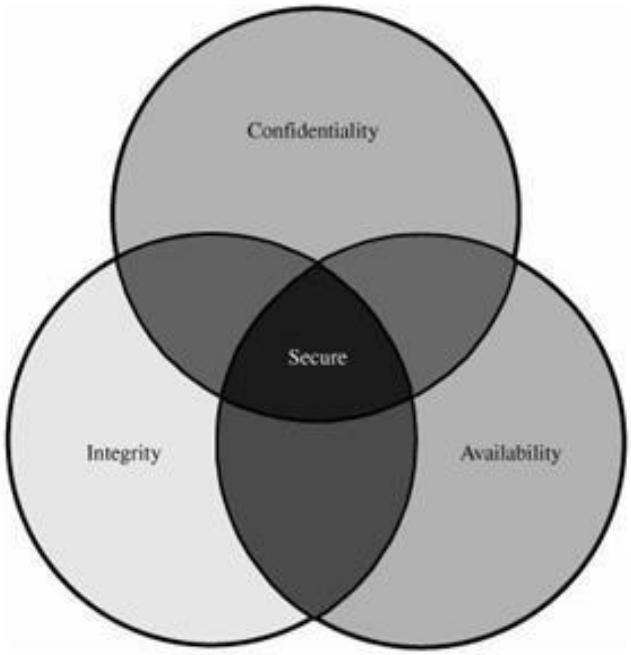
# 3 Teori

I detta kapitel kommer vi att gå igenom teorier relevanta för vår undersökning. Först kommer vi gå igenom vad säkerhet och informationssäkerhet innebär och varför det är viktigt med ett säkert IT-system. Därefter kommer vi gå igenom existerande hot mot IT-systemet för att få en bild över föreliggande risker. Till sist kommer vi gå igenom motivationsteorier för att förklara varför det är viktigt att motivera de anställda att följa en policy.

## 3.1 Säkerhet

Säkerhet innebär att någonting är skyddat. Det kan vara föremål i ett hus skyddade från stöld genom att huset har ett lås och ett larmsystem. Banker använder mycket säkerhet då de hanterar mycket värdesaker. De förvarar värdesaker i bankfack där endast banken och kunden som hyr facket kan komma åt. Bankfacken är skyddade av vakter, övervakningskameror, larmsystem och är inlåsta i ett bankvalv. Även våra pengar är skyddade. Vi kan placera dem på ett bankkonto och sedan koppla ett bankkort till kontot. För att använda bankkortet måste ett lösenord användas vilket skyddar pengarna på bankkontot från att vem som helst kan använda dem.

Pfleeger och Pfleeger (2006) skriver att det finns tre viktiga aspekter när det talas om datasäkerhet: *sekretess*, *integritet* och *tillgänglighet* (eng. *confidentiality*, *integrity* and *availability*), vilka behandlas nedan.




*Figur 3: När kriterierna för Confidentiality, Integrity och availability uppfylls resulterar det i säkerhet.*

*Sekretess (confidentiality)*
*Sekretess* innebär att datoriserade tillgångar endast är tillgängliga för behöriga personer. Det innebär att endast de som borde få tillgång till en viss information i systemet faktiskt får tillgång till informationen. Tillgång innebär att personen kan se, skriva ut och helt enkelt känna till att informationen existerar. Information får ej spridas till obehöriga personer.

*Integritet (Integrity)*
*Integritet* innebär att endast behöriga personer kan modifiera informationen. Det betyder att behöriga personer kan skriva, ändra, ta bort och skapa information. Detta innebär att informationen i systemet måste vara aktuell och presenteras på rätt sätt när den än används. Om en person ändrar i ett dokument måste dokumentet ändras på samma sätt för alla andra personer med rättighet att använda dokumentet. Förlorad integritet uppstår när information tas bort, ändras eller skapas utan att det sker för alla användare.

*Tillgänglighet (Availability)*
*Tillgänglighet* innebär att informationen ska vara tillgänglig när den behövs. Om en person eller ett system med behörighet att använda en viss information ska tillgången inte hindras. Tillgängligheten kan stoppas av en så kallad *denial-of-service-attack*. En *denial-of-service-attack* innebär att tusentals datorer skickar information till en hemsida, server eller dator vilket leder till att den överbelastas och stängs av (för djupare beskrivning se 3.3.1 Angriparens metoder).

## 3.2 Informationssäkerhet

Idag lagrar vi mycket information på datorer. Vi lagrar privata foton, dokument och andra filer vi kanske inte vill ska hamna i fel händer. För organisationer kan information vara extra värdefull. Organisationer lagrar företagshemligheter som patent och produkter de håller på att utveckla. Om dessa skulle hamna hos en konkurrent skulle det bli en katastrof. Därför är det viktigt att skydda sina IT-system från angrepp. Det är inte bara information som måste skyddas. Ofta är IT-systemet ett verktyg för de anställda. Om IT-systemet inte är skyddat kan det förstöras eller inte vara tillgängliga vilket leder till att de anställda inte kan använda dem och pengar och tid går förlorade.

Ett hot mot ett datorsystem är de händelser som leder till förlust eller att systemet skadas. Ett hot kan vara att IT-systemen inte fungerar en längre tid, information sprids till obehöriga eller att information är felaktig. Att information inte är tillgänglig när den behövs är också ett hot mot säkerheten i IT-systemet. Informationssäkerhet är resultatet av åtgärder använda för att förhindra hot mot IT-systemet (Pfleeger, 2006).

Ett IT-systems säkerhet är inte starkare än dess svagaste punkt likt talesättet att en kedja inte är starkare än dess svagaste länk. I många fall är det användaren som är den största svagheten i IT-systemet. Deras syn på säkerhet är ofta att ökad säkerhet leder till att deras arbetsuppgifter blir svårare och tar längre tid. Det tar tid att logga in och de måste komma ihåg långa lösenord som måste bytas regelbundet. Därför måste användarna motiveras varför de ska följa alla säkerhetsåtgärder (mer om motivering i kapitel 3.6 Motivation). Om de förstår riskerna med ett osäkert arbetssätt minskar risken att incident inträffar. Därför är det också viktigt att utbilda personalen. Om de inte har tillräckligt med kunskaper om säkerhet och inte vet hur de ska

hantera säkerhetsrelaterade situationer kan det leda till ett angrepp mot IT-systemet eller andra problem i IT-systemet. Om de anställda inte har tillräckligt med kunskaper hjälper väldigt få tekniska lösningar. Inga skydd hjälper om användaren själv ger ut användarnamn och lösenord till en obehörig person (Aloul, 2012).

Informationen som ska skyddas kan finnas i många former. Det kan vara dokument lagrade i pappersform, skisser av en prototyp lagrad i digital form, meddelanden som skickas via post eller via e-mail. Information lagrad i digital form kan skyddas genom att kryptera informationen eller genom att kräva lösenord för att använda informationen. Information lagrad i fysisk form kan skyddas genom att förvara den på ett säkert ställe som i ett kassaskåp, dokumentskåp med lås eller i ett bankfack (Pfleeger, 2006).

Informationssäkerhet kan delas upp i två kategorier: *administrativ säkerhet* och *teknisk säkerhet*.

*Administrativ säkerhet*
*Administrativ säkerhet* handlar om de administrativa delarna av organisationen som används för att skydda information och IT-systemet. För att se till att hela organisationen arbetar med säkerhet på samma sätt bör policydokument och rutiner skrivas. Policydokumenten och rutinerna avser att beskriva hur anställda skall hantera vissa säkerhetsrelaterade situationer. Om policydokument och rutiner inte följs kan det leda till att IT-systemet inte längre är säkert och kan bli utsatt för ett angrepp.

*Teknisk säkerhet*
*Teknisk säkerhet* handlar om de tekniska och fysiska lösningar som används för att skydda information och IT-systemet. Det är inte alltid enkelt att få anställda att följa de policydokument som finns. Det kan vara svårt att motivera varför ett lösenord måste vara en viss längd och varför datorn bör låsas när den lämnas obevakad. För att lösa dessa problem kan tekniska lösningar användas. Till exempel kan användaren vara tvungen att byta lösenord var 180:e dag och datorn låser sig eller loggas ut när den varit inaktiv i 30 minuter.

Även fysiska lösningar kan vara exempel på *teknisk säkerhet*. För att se till att endast behörig personal befinner sig i en byggnad kan passerkort användas. För att komma in i byggnaden måste passerkortet registreras och om det godkänns släpps den anställde in. Ett annat exempel är grindar som öppnas elektroniskt. När en person eller ett fordon ska ta sig in på området måste de först bli godkända av vakten. Personen eller fordonet kan bli godkända genom att ha någon som identifierar dem eller att vakten känner igen dem. På så vis kommer endast de som är behöriga in.

Vid analys av data används teorierna om säkerhet och informationssäkerhet för att motivera varför det är viktigt med säkerhet inom en organisation. Teorierna används även för att avgöra hur bra säkerhet organisationen i undersökningen har.

## 3.3 Informationssäkerhetspolicy

En informationssäkerhetspolicy är en policy som en organisation använder sig av för att beskriva hur organisationen arbetar för att skydda dess tillgångar. Genom att skriva en informationssäkerhetspolicy blir det enklare att se till att hela organisationen arbetar med säkerhet på samma sätt. En informationssäkerhetspolicy måste förklara det ansvar som alla individer som använder IT-systemet har. En informationssäkerhetspolicy bör innehålla följande (Al-Hamdani och Dixie, 2009):

- Hur vital information ska användas, delas och förstöras
- Hur tillgång till datorsystem ska ges ut och underhållas
- Hur datorsystemen skall användas
- Hur en säkerhetsincident skall hanteras
- Vilka rättsliga skyldigheter är involverade

Genom att skriva en informationssäkerhetspolicy blir det enklare att utbilda användare av IT-systemet. Om användarna blir utbildade och förstår varför vissa säkerhetsåtgärder finns blir det färre kostnader i IT-systemet. Det behövs inte lika många tekniska lösningar som ser till att policyn hålls utan användarna kan själva se till att de använder IT-systemet på ett säkert sätt.

## 3.4 Angripare

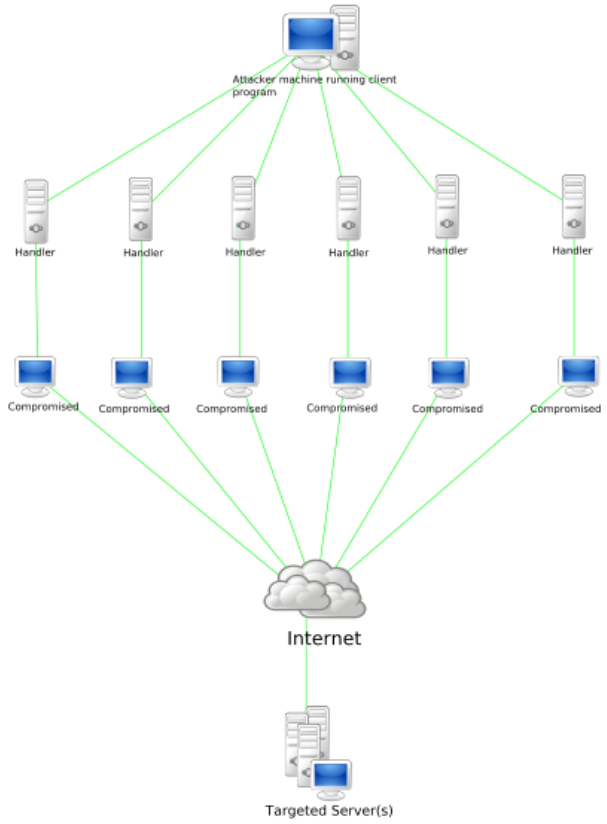
En attack mot ett IT-system innebär att en person eller ett program utnyttjar en svaghet i ett IT-system för att få kontroll över, stjäla känslig information i från eller förstöra IT-systemet. Det kan också vara för att upptäcka säkerhetshål i IT-systemet för att kunna åtgärda dem. Angripare i informationssäkerhetssammanhang brukar även kallas för crackare (eng. cracker). För att utföra en attack krävs det att angriparen har tre saker: *metod, möjlighet* och *motiv* . Om någon av dessa tre stoppas kan en attack ej genomföras. Detta är dock enklare sagt än gjort (Pfleeger, 2006).

### 3.4.1 Angriparens metoder

För att genomföra en attack kan angriparen använda en mängd metoder. Ett av de enklaste sätten att angripa ett IT-system är via en metod som kallas *bruteforce*. Det går helt enkelt ut på att angriparen försöker på egen hand gissa sig fram till lösenordet till ett IT-system. Detta kan göras manuellt eller med ett program som går igenom en lista med vanliga lösenord. Ett mer sofistikerat sätt att angripa ett IT-system är att lura användarna av systemet. Angriparen uppger sig för att vara en annan anställd på företaget och behöver hjälp. För att lösa problemet ber angriparen om till exempel lösenord eller annan vital information som behövs för attacken mot att angriparen återgäldar tjänsten senare. Den anställde tror att han har gjort något bra genom att hjälpa sin “kollega” fast i själva verket har denne gjort det möjligt för angriparen att ta sig in i IT-systemet. Angriparen kan fortsätta ta kontakt med fler anställda för att få ut mer information vilket underlättar attacken ytterligare. Denna typ av attack kan ta flera månader att genomföra och kräver stor försiktighet samt att ingen användare rapporterar incidenten (Flechais, 2005)(Pfleeger, 2006).

*DDOS-attack* är en annan metod en angripare kan använda. *DDOS-attack* är en förkortning för *distributed denial of service attack* och används för att få servrar och datorer att överbelastas och stängas av. Det kan till exempel användas för att slå ut en hemsida, e-tjänst eller viktiga IT-system för företag. För att genomföra en *DDOS-attack* krävs det att angriparen har tillgång till 100-, 1000- eller till och med 100 000-tals datorer beroende på hur kraftfull attacken behöver vara. För att få tillgång till en sådan mängd datorer har angriparen skapat ett virus som ger angriparen kontroll över en privatpersons dator. Viruset hamnar på datorn när privatpersonen laddar ner en fil med viruset på eller går in på en hemsida som innehåller viruset. Viruset ligger gömt i bakgrunden tills angriparen vill genomföra *DDOS-attacken*.

En dator infekterad med ett virus som har i uppgift att utföra en *DDOS-attack* brukar kallas för en *zombiedator* och ett nätverk med *zombiedatorer* kallas för ett *botnät*. När attacken ska genomföras skickas attackkommandot till en så kallade *hanterare* vilket är en annan dator som i sin tur skickar kommandot vidare till datorerna som är infekterade av viruset. Genom att skicka kommandot genom *hanterare* kan angriparen skydda sig mot att bli upptäckt. Angriparen kan ha flera *hanterare* för att göra det ännu svårare att upptäcka honom. När de infekterade datorerna fått kommandot börjar de skicka skräpdata till målet för attacken. Om tillräckligt många datorer skickar skräpdata till måldatorn eller servern överbelastas den och stängs av. Detta kan hjälpa vissa angripare att till exempel hindra att ett politiskt budskap sprids eller utpressa ett företag att mot pengar avbryta attacken (Mirkovic et al, 2004).




*Figur 4: DDOS-attack.*
*Angriparen skickar ett attackkommando till alla hanterare som skickar kommandot vidare till de infekterade datorerna som i sin tur utför attacken.*

### 3.4.2 Angriparens möjligheter

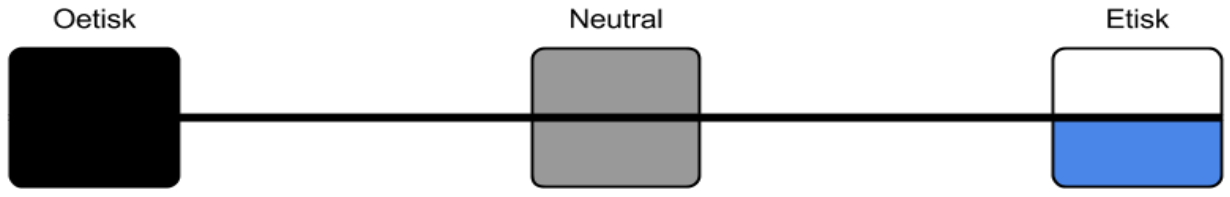
Möjlighet innebär att angriparen har tillräckligt med tid för att utföra attacken och att angriparen har tillgång till IT-systemet. Om angriparen ges tillräckligt med tid kommer denne tillslut komma in i IT-systemet. Den mänskliga faktorn bidrar till stor del till att angripare får tillgång till IT-systemet (Aloul, 2012).

### 3.4.3 Angriparens motiv

Det finns många anledningar att utföra en attack. Det kan vara för ekonomisk vinning, hitta fel åt ägarna av IT-systemet, sprida sina ideologiska idéer eller för att sprida förstörelse. Olika crackare brukar delas in i fyra stora kategorier: *white hat*, *black hat*, *grey hat* och *blue hat*. Sedan finns det flera mindre kategorier som kan placeras in någon av de tidigare nämnda kategorierna men har ett speciellt motiv som märker ut dem. Crackare delas in i kategorier efter hur etisk attacken var. *White hat* och *blue hat* är på den etiska sidan av skalan medan *grey hat* står i mitten och *black hat* på den oetiska sidan. De vi har fördjupat oss i är: *script kiddie* och *hacktivist.*

En *white hat* vill hitta säkerhetssvagheter i IT-systemet och meddelar sedan en administrator att han har hittat en svaghet och hur det kan åtgärdas. En *white hat* vill sprida kunskap om informationssäkerhet och göra IT-system säkrare. Till skillnad från en *white hat* som vill åtgärda säkerhetshål i IT-systemet vill en *black hat* utnyttja säkerhetshålen. En *black hat* vill hitta säkerhetssvagheter för att stjäla information, ta kontroll över eller förstöra IT-systemet. Informationen som samlas in kan säljas vidare och IT-systemen som back hat:en tagit kontroll över kan hamna i ett *botnät*. En *grey hat* är en blandning av *white hat* och *black hat*. De angriper IT-system för att hitta en säkerhetssvaghet och tar sedan kontakt med en administratör och berättar om svagheten. Därefter erbjuder de sig att åtgärda problemet mot betalning. En *blue hat* är väldigt lik en *white hat* fast är anställd av ett företag för att angripa deras IT-system. (Secpoint, 2013)(Wikipedia, 2014).

En *script kiddie* är en angripare som vill bli en crackare men har låg kunskap om IT-säkerhet. Eftersom en *script kiddie* inte har tillräckligt med kunskaper för att ta sig in i ett IT-system använder personen program och verktyg som någon annan har tagit fram för att utföra attacken. En hacktivist är en crackare som använder sina kunskaper om IT-säkerhet för att sprida ett politiskt, religöst eller ideologiskt budskap. Hacktivister använder ofta metoder som *DDOS* för att stänga ner hemsidor som uttrycker ett budskap som säger emot deras åsikt. Script kiddies och hacktivister kan sammanfattas som en *back hat*, *white hat* eller *grey hat* beroende på hur de utför sina attacker och mot vem eller vad som attacken utförs mot.




*Figur 5: Etikskala för crackare.*
*White hat och blue hat hamnar till höger på den etiska sidan av skalan. Grey hat hamnar i mitten och black hat till vänster på den oetiska sidan. Hacktivist och script kiddie kan hamna på båda sidor av skalan.*

Vid analys av data kommer teorierna om angripare användas för att få en bild om vilka hot en organisation står inför. Genom att förstå vilka hot mot organisationen som finns kan det bli enklare att skriva en policy för att motverka hoten.

## 3.5 Organisatoriska styrningsproblem

Att en organisations eller ett företags ledning har en avsikt de vill förmedla, betyder sällan att den till fullo genomsyrar alla nivåer av organisationen eller företaget i fråga. Detta hävdar Dermer och Lucas i artikeln *The Illusion of Managerial Control. Accounting, Organizations and Society,* (1986). Följande kapitel bygger genomgående på resonemang från nyss nämnd artikel. Kort sammanfattat belyses fenomenet att ledningens beslut många gånger uppfattas av dem själva att ha större genomslag än de faktiskt har. Traditionella kvantitativa resultatmått kanske inte alltid reflekterar hur ett styrningsbeslut mottages längre ned i organisationen.

Eftersom organisationer har delade viljor och verklighetsuppfattningar baserat på arbetsuppgifter och individuella intressen kan dessa hamna i konflikt. Avsikten bakom ledningens beslutande i form av informationssäkerhetspolicy kanske inte når alla medarbetare på samma sätt och utrymme för individuell tolkning och fritt handlingsrum måste tags i åtanke för att få genomslag. Orsakerna till eventuellt glapp i styrningen kan givetvis variera. Särskilt med hänsyn till arbetsuppgifter där varierande positioner medför olika ansvarsområden. Denna skillnad påkallar ett individuellt handlande i egen favör där arbetsuppgifter och position kan vara variabler. Organisationer bör ha detta i åtanke för att välja lämpliga informationskanaler och medel för varje beslut i avsikt att uppnå bättre enighet mellan organisationens alla delar.

Med hjälp av artikeln ämnar vi att belysa att organisatoriska beslut kan uppfattas och tolkas på olika sätt mellan olika positioner och nivåer i en organisation. Om undersökningen påvisar styrningsglapp i avseende att implementera IT-relaterade policydokument vill vi med hjälp av denna artikel föra en diskussion om eventuella anledningar till glappets uppkomst.

## 3.6 Motivation

Baserat på resonemang från föregående kapitel kan styrning av en organisation kalla på mer än enbart ett beslut. Att motivera anställda kan öka deras förmåga och vilja att prestera givet att förutsättningarna är de rätta. Teorierna om hur vi som människor fungerar och motiveras till arbete är många och därför har vi valt två teorier vi finner relevanta för att stå till grund för analys av insamlad data.

### 3.6.1 Douglas McGregors Theory X and Theory Y

*Theory X och Theory Y* är en tvådelad teori byggande på två distinkta antaganden om organisationsledningars syn på anställdas beteende. Traditionell byråkratisk organisationsstyrning bygger på antagandet att människor är lata, icke-arbetsvilliga, behöver övervakas och undviker arbete i högsta möjliga mån. Detta är *Theory X*. Övervakning krävs av de anställda för att de ska sköta sina arbetsuppgifter. Straff är nödvändiga om arbete inte sköts enligt lednings krav och ansvar är något som undviks vid möjlighet. Individen arbetar för att ställa mat på bordet och har ingen till låg ambition gällande sitt arbete. (McGregor, 1966)

Alla organisationsledningar följer dock inte antagandet om anställdas beteendemönster från *Theory X* utan faller i stället in under *Theory Y*, något av en motpol gentemot *Theory X*. Organisationsledningar utgår enligt *Theory Y* från antagandet att anställda söker både mental och fysisk stimulans samt att de flesta även finner ett tillfredställande av behov tack vare prestation i arbetsuppgifter. Egen drivkraft motiverar individen då denne strävar efter att uppnå såväl egna som organisatoriska mål samt för personlig utvecklings skull. Handlingsfrihet, ansvar och självständighet leder enligt *Theory Y* till ökad produktivitet. Mycket finns att ge och företag nyttjar sällan potentialen hos alla anställda till fullo. (McGregor, 1966)

Vid analys av empirisk data skall vi med hjälp av *McGregors Theory X och Theory Y* undersöka om mönster i informanternas beteende kan identifieras med ovanstående. Detta i avseende att hitta förklaringar till beteenden hos organisationens anställda. Med bättre förståelse för individers handlande kan vi även komma att dra slutsatser om hur organisationen kan dra nytta av kännedomen och därmed anpassa sig om utrymme för optimering upptäcks i säkerhetsarbetet.

### 3.6.2 Herzbergs Two-factor theory

I boken *The Motivation to Work* (Herzberg et al, 1959) diskuteras motivation och Herzbergs *Two-factor theory*. Denna var tilltalande gällande analys av anställdas motivation till kommande delar av uppsatsen. Hela kapitlet, bortsett från kapitlets sista stycke, bygger på ovan nämnda verk. Sista stycket omfattar ett eget resonemang om organisationen samt en koppling till hur teorin ämnas bringa nytta till uppsatsen.

En anställd blir inte motiverad bara för att en hög lön erbjuds. Inte heller av förmåner, arbetets status, goda arbetsförhållanden eller bra relationer med chef eller övrig personal. Faktorer som dessa är enbart bekvämlighetsfaktorer (*hygienfaktorer*) för att minimera den anställdas missnöje och dessa är inte tillräckliga för att uppnå motivation till prestation. I stället nämns självförverkligande faktorer vara det som påkallar drivkraften i individer. Känslan att åstadkomma något betydande, identifiera sig med sina arbetsuppgifter, känna att ansvarstagande ger utdelning och att ansträngning ger utdelning är i stället vad som uppkallar motivation hos individer. Möjligheten att utvecklas.

Teorin bygger på en incremental modell och kretsar runt att ständigt utvecklas. Att prestera under dessa förhållanden främjar ytterligare prestation och motivationen byggs således upp mer och mer. För att exemplifiera ovanstående skulle en person som tagit på sig ansvar för en arbetsuppgift de finner intressant identifiera sig i arbetet och se ett egenintresse för att klara av uppgiften väl. Med dessa grunder att motiveras beskrivs det även fördelaktigt att individen känner att arbetsuppgiften leder till något positivt och personlig vidareutveckling. Känslan av att prestera väl driver viljan att ytterligare fortsätta prestera i framtiden för att tillfredställa sina egna behov att utvecklas.

En, av oss, bildad uppfattning är att organisationen lyckats skapa en miljö där många *hygienfaktorer* uppfylls och att de anställda upplever arbetsplatsen som trivsam. Många anställda har dock arbetsuppgifter där datorn enbart är ett av många arbetsverktyg och vardagligt arbete kretsar runt annat än datorn, trots att den till någon slags grad kan användas. Herzbergs teori ämnar vi använda till vår analys och leda oss till slutsatser om att skapa förutsättningar där personalen blir gradvis mer motiverad till att ta reda på samt anamma organisationens riktlinjer rörande datoranvändning.

# 4 Resultat

I det här kapitlet presenteras resultatet av vår undersökning. Först presenteras varje intervju för sig och sedan en sammanfattning av alla intervjuer.

## 4.1 Intervjuerna

I vår undersökning har fem personer arbetandes på Uppsala kyrkliga samfällighet intervjuats. Dessa fem intervjuer bildar tillsammans insamlad data till undersökningen. Underlaget från varje intervju är således en viktig del till att i senare kapitel analysera utfallet och dra slutsatser om undersökningsresultatet.

### 4.1.1 Intervju 1

Första intervjun vi presenterar är med en av förvaltningscheferna för Uppsala kyrkogårdsförvaltning. Informanten delar tjänsten med en annan person. Informanten har arbetat inom Svenska kyrkan sedan 1992. Informanten började arbeta på ekonomiavdelningen och har även arbetat som bland annat sekreterare och personalutvecklare. Mellan 2005 och 2009 har informanten varit ansvarig för kyrkogårdarna i Uppsala och har sedan 2010 arbetat som förvaltningschef för Uppsala kyrkogårdsförvaltning.

*Datoranvändning*
I arbetet använder informanten datorn för att skicka e-mail, använda outlook för att schemalägga möten och andra aktiviteter inom sitt arbete. Kalendern i outlook är väldigt viktigt informanten har många möten och samtal. Program för att sköta ekonomin och godkänna attester används. Även Excel och Word används mycket. Till sist används datorn för att se de anställdas instämplingar. Mycket lite känslig information lagras på datorn och eventuellt lagrad information gäller personalärenden. Information skyddas från obehöriga genom att lösenordsskyddas eller skrivas ut och placeras i en personakt. Det mesta av informationen som hanterar är offentlig.

*Implementation och utbildning av policy*
När informanten började arbeta inom Svenska kyrkan blev informanten utbildad av ledningsgruppen till arbetet. Ofta får de anställda leta efter relevanta policydokument själva men att i alla fall informantens tidigare chefer har gått ut med var de viktiga policydokumenten finns att ta del av. Informanten känner inte till alla policydokument som Svenska Kyrkan har men vet grovt vad de innebär och var de kan läsas vid behov. När en ny policy ska implementeras har informanten en stor roll i processen. När en ny policy ska tas fram har informanten och i vissa fall personen som delar chefsrollen i uppdrag att se till att en handläggare förbereder, skriver underlaget och kanske själva synpunkten till policydokumentet. Sedan tas ärendet upp i kyrkonämnden som är styrelsen som beslutar när en ny policy ska implementeras.

Policydokument är väldigt generella vilket ibland medför behov av att rutiner eller anvisningar kopplas till själva dokumentet. Därför behöver informanten skriva anvisningar och rutiner till policydokument så de blir lättare att följa för de anställda. Informanten har ingen roll i utbildningen när en ny policy har implementeras. Dock har informanten en introduktion för nyanställda. Då går informanten igenom vissa policydokument men utbildningen handlar mest

om manualer och organisationsscheman och liknande. Det är respektive arbetsledare eller chef som är ansvarig för utbildning när en ny policy har implementerats. Nyligen har de gjort ett försök och haft utbildning av personal tillsammans med Previa, ett företag som hanterar företagshälsovård. Där har de tagit upp frågor som personalhälsovård, lönesamtal och i framtiden IT då det har upptäckts ett behov av att utbilda arbetsledare inom dessa ämnen. Det finns även en personalhandbok som beskriver rutiner när ny personal anställs och även hur ny personal ska utbildas om viktiga dokument.

Informanten försöker motivera anställda att följa de policydokument som finns på de möten som hålls. Dock sker detta endast när behovet finns. Det inte räcker att gå igenom en policy en gång utan att det är ett levande arbetssätt som pågår hela år. När missförstånd gällande policydokument eller rutiner upptäckts försöker informanten ta upp det på möten eller utvecklingssamtal för att åtgärda problemet. Informanten tror att IT-enheten ofta pratar om gällande policydokument då det ingår i deras arbetsuppgifter och de arbetar just med datorer och mobiltelefoner. I informantens arbete pratas det om policydokument när det påträffas i ett ärende. Det viktigaste är inte att alla medarbetare kan alla policydokument utan att de anställda ska veta att den finns och var den kan hittas när den behövs.

När det upptäcks att någonting inte fungerar lyfts det upp till ledningsgruppen för att fatta ett beslut om problemet måste ses över. Det är viktigt att personer med rätt kompetens tar fram underlaget till policyn. IT-relaterade policydokument kommer därför ofta ifrån IT-enheten. En utredningssekreterare kan finslipa policyn att fungerar bra uttrycksmässigt och stämma som en policy samt att nya rutiner kan arbetas fram.

*Efterlevnad av IT-policy*
Informanten använder sällan arbetsplatsens internet för att göra icke arbetsrelaterade, det händer ungefär fem gånger per år. Det beror på att informanten sällan har någon dödtid under arbetsdagen i och med sin position och informanten vill vara en förebild för sina anställda. Om en kollegas dator skulle sluta fungera och kollegan behövde skicka ett dokument skulle informanten inte låna ut sina inloggningsuppgifter. Däremot kan kollegan logga in på vilken dator som helst på arbetsplatsen så informanten skulle kunna låna ut sin dator tillfälligt eller hjälpa kollegan skicka dokumentet via sitt användarkonto. Dock skulle informanten övervaka situationen.

När informanten är på semester eller sjukskriven ser informanten oftast till att det genereras ett automatiskt meddelande som berättar att informanten ej kan svara och hänvisar till en person som kan hantera ärendet. I och med att informanten har en smartphone via arbetet kan e-mail besvaras även när informanten är sjukskriven eller på semester. Informanten har ej installerat programvara som inte har med informantens arbetsuppgifter att göra. Informanten anser att risken mot IT-systemet är låg. IT-systemet är säkert för sitt ändamål och det finns en kompetent IT-enhet. Information som lagras är i stor del tillgänglig för allmänheten men en del personlig information lagras. Om informationen skulle läcka ut skulle organisationens rykte ta skada men inte väldigt allvarligt. Däremot kan enstaka personer ta skada i fall informationen rör dem. För att se till att information inte försvinner ifall IT-systemet skulle gå sönder finns det säkerhetskopieringsprogram.

*Sammanfattning*

| | |
|---|---|
| Position och arbetsuppgifter | Ansvarig för Uppsala kyrkogårdsförvaltning. Sköter inköp, anställning, beslutsfattande, delegering av arbetsuppgifter med mera. |
| Datoranvändning | Informanten använder datorn för att göra kontorsarbete som att skriva dokument, använda Excel, skicka e-mail etc. Viss känslig information lagras på datorn men det gäller mest personlig information. |
| Kännedom om policy | Har god kännedom om policydokument. Vet var dokumenten finns och vad många av dem innebär. |
| Ansvar för vidareförmedling av policy | Har litet ansvar i vidareförmedling av policydokument. Utbildar om policydokument på personalmöten när behovet finns. |
| Ansvar för framtagande av ny policy | Har ansvar för framtagning av ny policy. Tar till sammans med assisterande chef och handläggare fram underlag för policydokument. Tar även hjälp av andra enheter när en policy angående enhetens arbetsuppgifter ska tas fram (till exempel IT-enheten hjälper till att ta fram IT-policydokument). |
| Risker och efterlevnad | Informanten följer de rutiner och policydokument som finns i vardagen. Risken är liten att ett angrepp mot IT-systemet skulle inträffa på grund av informanten. |
| Upplevd hotbild | Informanten anser att säkerheten i IT-systemet är god och att IT-personalen är kompetent. Eftersom det mesta av informationen som lagras i IT-systemet är tillgänglig för allmänheten är det inte intressant att utföra en attack mot IT-systemet. |

*Figur 6: Sammanfattning av intervju 1*

### 4.1.2 Intervju 2

Andra informanten arbetar som kyrkoherde på en av församlingarna i samfälligheten. Informanten har arbetat som kyrkoherde i samfälligheten sedan 2011 och sedan 1985 i Svenska kyrkan. Informanten är ansvarig för församlingen och chef för ungefär 25 personer.

*Datoranvändning*

I arbetet använder informanten datorn för att skriva dokument, använda Excel och skicka e-mail. Informanten använder även datorn för att redigera bilder. Det händer att det lagras känslig information om klienter för att underlätta att komma ihåg vad som sagts. För att komma åt informationen måste ett användarnamn och lösenord skrivas in.

*Implementation och utbildning av policy*

När en ny policy ska implementeras har informanten i uppgift att utbilda personal och se till att de kan den. Däremot har informanten ingen roll när en ny policy ska tas fram och det beror på att samfälligheten har en IT-avdelning som är ansvarig för att ta fram nya policydokument när de behövs. När ny personal har anställts har informanten också i ansvar att utbilda dem i de relevanta policydokumenten till deras arbetsuppgifter. När en ny anställd börjar får de gå igenom en introduktionspärm som innehåller policydokument, rutiner och andra dokument som beskriver hur den nyanställde ska bete sig och hantera vissa situationer.

Den nyanställde förväntas känna till policydokument och rutiner när utbildningen är klar. All personal blir informerad under personalsamlingar som sker med jämna mellanrum. När personal blir utbildad eller informerad om olika policydokument brukar det inte talas om varför viken gällande varför policydokument skall följas eller medförande risker om de inte följs. Informanten anser att det är självklart varför de ska följas. Genom att ha personalsamlingar ser informanten till att personalen blir påmind om policydokument och rutiner. Det sker en personalsamling en gång i veckan men policydokument och rutiner brukar det talas om ungefär en gång per år.

*Efterlevnad*
Det händer att informanten gör icke arbetsrelaterade saker med datorn som att gå in på Facebook eller liknande. Däremot anser informanten att det är tillåtet att göra detta för att få en kort paus från arbetet så länge det jobbet sköts ordentligt. Eftersom det är tillåtet att ta en rökpaus borde det vara tillåtet att ta en Facebook-paus tycker informanten. Informanten lånar ej ut sitt användarkonto ifall en kollega har problem. Däremot skulle informanten hjälpa kollegan. I kyrkans IT-system går det att logga in från vilken dator som helst. Därför kan informanten låna ut sin dator ifall det behövs.

När informanten är sjuk eller är på semester skapar informanten oftast ett automatiskt meddelande som berättar att informanten inte kan svara och ger kontaktuppgifter till någon som kan. Eftersom informanten har en smartphone via jobbet kan informanten svara på e-mail även när informanten är sjuk eller på semester. Det är viktigt att det alltid går att nå någon som är ansvarig.

*Yttre hot mot IT-miljön på arbetsplatsen*
Det finns hot mot IT-miljön anser informanten. Informanten anser att samfällighetens IT-system inte är säkrare än andra IT-system. Informanten tar för givet att e-mail och annan kommunikation över internet kan läsas av myndigheter som FRA (Försvarets Radioanstalt). Däremot tror han att informationen inte är intressanta för utomstående. Det mesta av informationen som lagras är antingen tillgänglig för allmänheten eller gäller privatpersoner.

*Sammanfattning*

| | |
|---|---|
| Position och arbetsuppgifter | Informanten arbetar som kyrkoherde. Som kyrkoherde utför informanten kontorsarbete, har samtal med personer som behöver stöd och är ansvarig för församlingen i Gamla Uppsala. Informanten är även chef för ungefär 25 personer. |
| Datoranvändning | Informanten använder datorn för att utföra kontorsarbete som att skriva dokument, skicka e-mail, redigera bilder med mera. Datorn används även för att föra vissa anteckningar till samtal med olika privatpersoner. |
| Kännedom om policy | I och med sin ledarroll har informanten bra koll på många av de policydokument och rutiner som finns. Har koll på vart de finns att läsas vid behov. |
| Ansvar för vidareförmedling av policy | Har litet ansvar för vidareförmedling av policydokument. Vid nyanställning medverkar informanten till en viss del i utbildningen av den nyanställde inom policydokument och rutiner. Dock utförs större delen av utbildningen av den nyanställdes närmaste kollegor. Även vid personalmöten samtalas det om policydokument om behovet finns. |
| Ansvar för framtagande av ny policy | Inget men det kan hända att informanten medverkar i framtagningen av en ny policy om det skulle behövas. |
| Risker och efterlevnad | Informanten är bra på att följa de policydokument som finns gällande IT-säkerhet. Dock har program som ej har med informantens arbetsuppgifter installerat. Risken för en attack mot IT-systemet på grund av informanten är mycket låg. |
| Upplevd hotbild | Informanten anser att hotet mot IT-systemet är mycket låg då väldigt lite känslig information lagras och den känsliga information som lagras är av personlig karaktär. Dock tar informanten för givet att all kommunikation över internet kan läsas av obehöriga. |

*Figur 7: Sammanfattning av intervju 2*

### 4.1.3 Intervju 3

Tredje informanten arbetar som på samfällighetens IT-avdelning som IT-tekniker sedan ungefär fem år tillbaka. Huvudsakliga arbetsuppgifter uppgår till att sköta samfällighetens datanät, nätverk, datorer, programvaror och mycket därtill med viss betoning på variation inom områdets bredd.

*Datoranvändning*

Datorn inte bara ett redskap utan likställs med exempelvis en arm. Självklarhet att använda dator till i princip allt. Vanligen sköts också mycket mailkontakter, surf, användande av intranät och användande av olika system. Ärendehantering nämns som ett exempel på detta. Känslig information hanteras i och med positionen på IT-avdelningen. Informanten kan logga in med administratörsbefogenheter vid behov och kan sköta tilldelning av behörigheter samt styra åtkomst. Åtkomstbehörighet arbetas noga med på ett förebyggande sätt för att skydda känslig information. Att skydda informationstillgångar aktivt mer än av IT-systemens skydd är inget som sker på daglig basis men långsiktiga insatser pågår ständigt. Behörighet sätts till olika grupper enligt principen åtkomst vid behov i största möjliga mån. Vissa luckor nämns dock förekomma.

*Informationssäkerhetspolicy*
I arbetsintroduktionen fick informanten direktiv gällande organisationens IT-system av kollegor. Rådande policys och förhållningssätten till dem beskrevs både just på arbetsplatsen och på nationell nivå. Detta skedde muntligt hänvisades till olika länkar för områdesrelevant information. Någon policy som ska läsas och skrivas under av varje användare innan denne får tillgång till IT-system men samtidigt nämns också att den sekretess ett företag kan ha inte kan jämställas med informantens arbetsplats i och med samfällighetens öppenhet. Präster har exempelvis tystnadsplikt om viss känslig information och sådan information hanterar de i enlighet med den. Sedan nämns att en tydlig informationssäkerhetspolicy inom organisationen om hur de anställda de facto ska tänka och bete sig inte finns samlad.

Däremot finns information om hur lösenord måste se ut tillsammans med andra policydokument med riktlinjer, anpassade till verksamheten. Olika lösenord till olika system används och krav för lösenordssäkerhet samt lösenordsbyten varierar beroende på system i fråga. System är inte ihopkopplade och domäninloggningen nämns vara en av de känsligare inloggningarna samt behandlas därefter. Alla användare tvingas därför byta lösenord var sjätte månad och har också krav på lösenordets innehåll av säkerhetsskäl. Dessa krav skall även gälla mail. Utöver detta har IT-avdelningen i och med kunskapsområde ansvar i att vara med vid utformning eller förändring av policydokument inom IT-området.

*Vidareförmedlingsroll av policy*
Positionen medför ansvar att föra policy- och styrningsdokument vidare vill anställda inom organisationen. Vanligtvis sker detta med interna utskick av information vid behov. Vanligtvis rör det sig om dokument som är ämnesspecifika. Till exempel telefonipolicy, länkar till policy för internetanvändning eller mailhantering och dessa gäller från nationell nivå. När någon börjar på arbetsplatsen delges den av information relevant för just dem och deras arbetsuppgifter. Några kontinuerliga utskick till alla inom organisationen som påminnelser görs inte. Utskickad information finns i stället att tillgå via intranät och alla har möjlighet att ta del av denna om och när de vill. Huruvida var och en väljer att göra det är svårt att avgöra då det också är svårt att kontrollera. I stora drag anser organisationen att de har en god säkerhetsnivå och pratar ibland om förbättring av policy men främst vid behov eller när något uppmärksammas kunna förbättras.

*Efterlevnad*
Informanten använder ibland sociala medier på arbetsplatsen. Många har sociala medier och flera just Facebook som del av arbetet. Att sätta sig på Facebook på fikarasten är således inget som förbjuds eller finns tekniska hinder för. På nationell nivå, rörande hela kyrknätet, finns dock filter mot webbplatser med olämpligt innehåll. Då menas sådant ingen har nytta av i sitt arbete. Mycket frihet under ansvar finns oavsett position råder inom organisationen och de har inte samma "superhemligheter" som företag kan ha att försvara från obehöriga. Skydd från virus finns givetvis och dessutom begränsningar i datormiljön för ytterligare skydd. Lokalt, på datorer, är det väldigt öppet men däri finns även ett terminalskrivbord där de flesta arbetar i. I denna miljö finns en hel del spärrar för användaren i syfte att skärma av arbete från personligt bruk.

Om en situation uppstår där en kollega behöver ett dokument skulle inte användarkonto och lösenord lånas ut. Hos denna informant skulle detta vara extra känsligt i och med sin position. Berättigad att tilldela åtkomst samt styra behörigheter måste det visas hänsyn till detta. Övriga användare uppmanas till att inte dela med sig av lösenord med uppgifter för användarkonton och det är även fördelaktigt att stå som gott exempel. Informanten nämner dock egen försiktighet mot närmaste kollegor som mindre och agerar med större aktsamhet ju mer främmande en person är. Sedan berättas dock att situationer där lösenord lånas ut faktiskt uppstår inom organisationen.

*Yttre hot mot IT-miljön på arbetsplatsen*
Låg hotbild om att obehöriga kommer åt känslig information i och med öppenheten hos organisationen men det säkert finns personer kapabla att utnyttja viss information inom organisationens nät, nämns av informanten. Känsligheterna är snarare av personlig karaktär och därmed mer känsliga på individnivå än skadliga för organisationen på annat sätt. Andra potentiella intrång som nämns är de av experimentell typ. Möjligheten att försöka bryta sig in, enbart med avsikt att se om det går, utan att nödvändigtvis förstöra. Att hot finns måste alltid vara i medvetandet och att potentiella angripare aldrig kan uteslutas.

*Sammanfattning*

| | |
|---|---|
| Position och arbetsuppgifter | IT-tekniker på IT-avdelningen. Sköter samfällighetens datanät, nätverk, datorer, programvaror och annat inom områdets bredd. |
| Datoranvändning | Datorn används till i princip allt. Mail, surf, intranät, systemhantering, ärendehantering, tilldelning av behörigheter, åtkomst. Förebyggande arbete för informationssäkerheten inom organisationen. |
| Kännedom om policy | God kännedom om vilka dokument organisationen har att förhålla sig till samt var de finns och när de bör tillämpas. |
| Ansvar för vidareförmedling av policy | Ja. Vanligtvis i form av interna utskick med information efter behov. Oftast ämnesspecifik information eller dokument. Länkar med relevant information till nyanställda eller länkar till exempelvis telefoni- eller mailpolicy. Påminnelser skickas ej ut då all information finns på intranätet för anställda att läsa vid behov. Uppföljning om alla lär sig om policydokumenten sker ej. Ansvar lämnas åt var och en. |
| Ansvar för framtagande av ny policy | Ja. I och med kunskapsområde har IT-avdelningen ansvar i att vara med vid utformning eller förändring av policydokument inom området. |
| Risker och efterlevnad | Informanten kan använda arbetsdatorn för ickerelaterade uppgifter ibland. Att till exempel logga in på Facebook, på fikarasten, känns inte konstigt. Berättar att kyrknätet har nationella filter där vissa sidor blockeras på grund av dess innehåll. Anställda har frihet under ansvar och datorer på lokal nivå är väldigt öppna, men betydligt mer begränsade i de terminalskrivbord de flesta sköter sitt arbete i. Skulle ej låna ut sina inloggningsuppgifter men känner till att det förekommit inom organisationen. |
| Upplevd hotbild | Öppenheten och typ av lagrad information leder till låg sannolikhet för intrång. Organisationen har inte några hemliga företagshemligheter vilket bör minska intresset att göra intrång. Däremot hanteras en del personligt känsliga uppgifter vissa skulle kunna utnyttja mot enstaka individer. |

*Figur 8: Sammanfattning av intervju 3*

### 4.1.4 Intervju 4

Fjärde informanten arbetar som präst och har arbetat inom Svenska Kyrkan sedan 2002. Personen har även verksamhetsansvar och arbetsuppgifterna består bland annat av själavårdande samtal, hantering av mail, skrivande av texter samt internetanvändning utefter behov.

*Datoranvändning*
Personens datoranvändande i arbetet går ut på att skriva mycket mail, texter samt internetanvändande efter verksamhetens behov. Positionen präst medför vardaglig kontakt med personlig information vilken vissa gånger kan vara känslig. Dessa känsliga uppgifter sparas ibland på arbetsdatorn och för att förhindra obehörig åtkomst till dessa används inloggning till användarkonto. Utöver inloggningen skyddas de inte aktivt via ytterligare försiktighetsåtgärder.

Arbetsdatorn kan användas privat och tillåts att medtaga hem. Således finns också vissa privata vanor förknippade med datorn. Mail av privat karaktär nämns som exempel på det och till detta används arbetsmailen. Datorn delas inte med någon annan utan är personligt tilldelad informanten.

*Policy – introduktion och efterlevnad*
Informanten berättade att vetskap om att policy och riktlinjer finns men några egentliga detaljer runt dessa. Eventuellt kom information om informationssäkerhetspolicy i samband med utbildning i början av tjänsten och berättade att organisationen inte följer upp eller kontrollerar om de anställda följer policyn eller ej. Ibland används jobbmailen även till privata ändamål och vid frånvaro skickas ej automatiska utskick men informanten får mail även till telefonen som ständigt är uppkopplad. Då finns möjligheten att själv besvara ärendet eller slussa personens fråga vidare till annan som kan behandla uppdraget.

Arbetsplatsens internet är inte strikt spärrat till ett fåtal sidor och informanten berättade att denne har använt arbetsplatsens dator och internetuppkoppling till icke arbetsrelaterade ting, exempelvis sociala medier. Personliga användarkonton respekteras och utlånande av lösenord till användarkonto har ej förekommit. Möjligheten att installera programvara på datorn finns och informanten har också installerat programvara på sin arbetsdator. Dock ej något som antas vara förbjudet.

Osäkerhet råder om egentliga direktiv angående installation av ny programvara men berättade att viss mjukvara är också nödvändig till arbetet och det krävs exempelvis ingen kontakt med IT-avdelning för att lägga in ny mjukvara i datorn. Vid fråga om egna enheter är tillåtna på arbetsplatsen antar informanten att det är möjligt men är samtidigt osäker på grund av att arbetsdatorn även används hemma samt att informanten använder separata mobiltelefoner för arbete samt privat bruk. Om hotbilden mot organisationens IT-miljö känner sig vår informant sig säker i arbetsplatsens IT-miljö och uppskattar sannolikheten för ett intrång som låg.

*Sammanfattning*

| | |
|---|---|
| Position och arbetsuppgifter | Präst. Verksamhetsansvar, själavårdande samtal, mail, skrivande av texter samt internetanvändning |
| Datoranvändning | Mycket mail, textskrivande, internetanvändande |
| Kännedom om policy | Vet om att riktlinjer ska finnas men inga detaljer om dessa. Eventuellt kan policydokument ha nämnts vid utbildning men inget sedan dess |
| Ansvar för vidareförmedling av policy | Nej |
| Ansvar för framtagande av ny policy | Nej |
| Risker och efterlevnad | Vissa uppgifter sparas på datorn. Skyddas med inloggning. Privata mail från jobbmailen kan skickas och visst användande av arbetsdator till icke-arbetsrelaterade ändamål förekommer. Automatiska utskick vid frånvaro görs ej, men har mail till telefon och svarar själv eller slussar vidare även vid frånvaro. Lösenord har ej lånats ut till andra. Hinder att installera programvaror har informanten inte stött på när denne gjort det någon gång vilket även tjänsten ibland kräver. Angående användande av egna enheter i arbetsplatsens nät antogs att det gick, men har ej prövat. Osäker på riktlinjer om riktlinjer för programvaror och egna enheter finns. |
| Upplevd hotbild | Informanten känner sig säker i arbetsplatsens IT-miljö och uppskattar sannolikheten för intrång som låg. |

*Figur 9: Sammanfattning av intervju 4*

### 4.1.5 Intervju 5

Sist ut bland presenterade informanter är informant nummer fem. Personen är diakon till yrket och har på nuvarande position arbetat i ungefär ett års tid. Vardagliga arbetsuppgifter uppgår till själavårdande aktiviteter, andakt, sorgarbete, aktiviteter med äldre samt att hålla språkkurs avsedd för nyanlända till Sverige.

*Datoranvändning*

Informantens datorvanor i arbetet kretsar runt mailhantering, tidsrapportering, bokning av lokaler samt att nå ut med reklam med information om aktiviteter i arbetet. Medveten om att information kan vara av känslig grad sparas inte sådant på arbetsdatorn i onödan. Sådan information hålls främst i huvudet. Sparad information relaterad till känslig data består vanligen av kontaktuppgifter tillsammans med eventuell kommentar om återkoppling eller möte samt dag och tid. Många gånger hanteras information mun till mun på grund av dess känslighetsgrad och samtalen skrivs sällan ned vare sig med papper och penna eller på elektroniskt vis.

*Policy – introduktion och efterlevnad*

Vetskapen om någon informationssäkerhetspolicy är vag, bortsett från ett antagande om policyns existens. Informanten är därför osäker på dess innebörd. Vid sin arbetsintroduktion beskrevs hur datorsystem fungerade gällande mail och andra nödvändigheter relaterade till kommande arbetsuppgifter. Någon policy talades det dock inte om. Föga förvånande talades det således inte om någon informationssäkerhetspolicy i arbetet.

Angående mail händer ibland att privata mail skickas från arbetsplatsens mailadress. Vid frånvaro eller om informanten av annan anledning inte kan svara på mail anordnas inte automatiskt svar till avsändaren om frånvaron men är medveten om att det bör göras om det inte är något som sköts automatiskt. Informanten har inte använt arbetsplatsens internetuppkoppling till icke arbetsrelaterade uppgifter, exempelvis sociala medier eller nätforum. Att användarkonton är personliga respekteras. Lösenord skulle ej och har ej lånats ut till kollega. Någon situation för behov av detta har heller inte uppstått ännu. Om egna enheter tillåts gissar informanten att det borde gå men är osäker på grund av att denne inte provat någon egen enhet i arbetsplatsens IT-miljö. Huruvida regler och riktlinjer om medtagande av egna enheter råder vet personen inte.

Även denna intervju avslutades med att informanten läts beskriva om denne kände sig säker i arbetsplatsens IT-miljö och hur hotbilden upplevdes. Trygghetskänslan upplevdes bra men kände ändå att sannolikheten för intrång ändå fanns och att det mycket väl kan hända att obehöriga tar sig in i organisationens IT-system. Avslutningsvis berättade informanten att denne, en tid tillbaka, mottagit ett mail från en kollega med hänvisningar om att vissa uppgifter behövde ändras eller uppdateras. Kollegan vars mail uppgavs vara avsändare hade nämligen inte skickat ut ett sådant mail. IT-avdelningen kontaktades för att utreda problemet och därav informantens uppfattning om sannolikhet för intrång.

*Sammanfattning*

| | |
|---|---|
| Position och arbetsuppgifter | Diakon. Själavårdande aktiviteter, andakt, sorgarbete, aktiviteter med äldre samt språkkurser för nyanlända till Sverige. |
| Datoranvändning | Mail, tidsrapportering, bokning av lokaler, nå ut med reklam för aktiviteter. |
| Kännedom om policy | Antagande om att sådan finns, osäker på dess innebörd. Fick vid utbildning reda på information relevant för informantens arbetsuppgifter men pratade ej om policy. |
| Ansvar för vidareförmedling av policy | Nej |
| Ansvar för framtagande av ny policy | Nej |
| Risker och efterlevnad | Privata mail kan skickas via jobb-mail. Autosvar vid frånvaro skickas ej, men vet att det bör ordnas. Använder ej arbetsplatsens internet till icke-arbetsrelaterade uppgifter. Har ej installerat programvaror men antar att det skulle gå och personen skulle ej låna ut lösenord om en kollega frågade. Tror egna enheter borde fungera på arbetsplatsen men har ej provat och vet ej om det finns särskilda riktlinjer om detta. |
| Upplevd hotbild | Känner sig trygg i arbetsplatsens IT-miljö men är medveten om att intrång kan ske. Ganska låg sannolikhet för intrång men trots det möjligt. |

*Figur 10: Sammanfattning av intervju 5*

## 4.2 Summering av intervjuer

Helheten intervjuerna utgör summeras nedan i relation till de områdena närmast berörande våra forskningsfrågor. Först hur organisationens policydokument skapas och sedan hur Implementationen av dem går till. Därefter följer en summering av informanternas beteende i efterlevnadssyfte i avseende gällande säkerhetsrisker. Slutligen avslutas vårt kapitel om empiri med identifierade problem med beskrivning av påträffade brister.

### 4.2.1 Policydokument - uppkomst och utbildning

Vid framtagande av en ny IT-policy eller förändring av en gammal fördelas ansvar till IT-avdelningen att tillsammans med handläggare förbereda och skriva underlag för policyn. Därefter presenteras policydokumentet inför chefen för kyrkogårdsförvaltningen vilket medför att ett ärende hos kyrkonämnden bildas angående det nya policydokumentet. Först efter policydokumentet godkänts blir det redo att implementeras i organisationen.

Det finns rutiner för hur ny personal ska skolas in i sin tjänst. Vanligtvis håller kollegor eller en chef i utbildningen vid nyanställningar enligt informanterna. Information om vardagliga rutiner skall läras ut och relevant information avses att förmedla om relevanta policydokument samt var den nyanställde hittar en relevant policy vid behov. Ledningens roll vid utbildning är att tillsätta lämplig personal att vidareförmedla policydokument till övriga anställda. Genom organisationen letar sig policydokument nedåt via arbetsledare och chefer. Dessa ansvarar därefter för att informationen till deras medarbetare når fram.

Enligt ledningens vilja att delegera arbetsuppgifter till de mest lämpade hamnar således en del av vidareförmedlingsansvaret hos IT-avdelningen varav en av våra informanter arbetade inom. I egenskap av att besitta stor kunskap inom IT-området samt att arbeta med organisationens datanät, nätverk och datorer har denna informant tillgång till andra medel vid policyimplementation än arbetsledare och chefer. På grund av ämneskunskapen är IT-avdelningen även med vid skapande samt ändringa av policydokument.

Delar av direktiv och riktlinjer från policydokument kan justeras med hjälp av tekniska lösningar. Skydd i nätverk och datorer är IT-avdelningens ansvar vilket medför att de ibland kan styra användare att följa delar av en policy tack vare införande av tekniska begränsningar. Exempel på detta nämns vara tekniska krav på lösenordsbyte efter avsedd tid samt krav på lösenordets innehåll av tecken. Utöver ovanstående har IT-avdelningen mer ansvar vid implementation av organisationens policydokument. Interna utskick görs vid behov med länkar till relevanta policydokument. Vanligtvis utefter verksamhetens behov. Till exempel nämns att nyanställda förses med information om policydokument nödvändiga för deras position och arbetsuppgifter. Någon uppföljning med efterlevnadskontroller är dock inte något som utförs. Informationen de skickar ut finns att läsa på intranätet och skickas heller inte ut flera gånger i påminnelsesyfte.

### 4.2.2 Efterlevnad av policy

Från ledningens sida är kännedomen om policydokumenten god. Vetskap om vilka policydokument organisationen arbetar med samt dess ungefärliga innebörd finns men framför allt betonas vikten av att veta var de olika policydokumenten finns att tillgå och i vilka situationer de bör tillämpas. Informanten i ledningen nämner att egen detaljkunskap om dokumenten saknas men likt föregående mening beskriver krävs inte detaljkunskap om organisationens policydokument. Viktigt däremot, är kännedom om när en policy skall tillämpas samt var den finns att tillgå vid det tillfället.

Informanterna med högre organisatorisk position har mer kunskaper om de policydokument och rutiner som finns än de med en lägre position. Informanterna med en högre position känner till att det finns IT-relaterade policydokument och vet var nödvändig information om en policy eller rutin kan hittas vid behov. De är också bättre på att följa gällande policydokument. En av informanterna hävdade att denne ville vara en förebild för anställda och poängterade vikten att själv följa policydokument och rutiner. Att anställda kan alla policydokument utantill, utan de förväntas generellt veta hur de ska arbeta och vilka rutiner som finns. Anställda skall veta var ett policydokument kan läsas vid behov.

Informanterna med lägre position har mindre koll på organisationens policydokument och rutiner. Ett av organisationens policydokument hänvisar till aktsamhet vid användande av arbetsplatsens internet vid icke arbetsrelaterade ändamål. Icke arbetsrelaterad användning får inte gå ut över personens arbetsuppgifter. Att använda arbetsdator till något icke arbetsrelaterat var något flera informanter ibland gjorde. Dock hävdade en av de högre uppsatta informanterna, i enighet med policyn, att detta är tillåtet under förutsättning att arbetet sköts. En av informanterna liknade detta med en kortare paus för att orka med arbetsdagen. Samtliga i undersökningen svarade att de inte skulle ge ut sina inloggningsuppgifter till en kollega. Detta gör det svårare för angripare att utnyttja de anställda för att ta sig in i IT-systemet. Däremot svarade informanterna vi klassificerat som anställda på lägre organisatorisk nivå att de inte känner sig trygga i vilka gällande policydokument de bör känna till om informationssäkerhet och hur de ska använda IT-systemet.

Utbildningsprocessen finner vi i praktiken beskrivas på ett liknande sätt oavsett vilken plats eller nivå i organisationen en anställd befinner sig på. Närmaste kollegor och chefer eller arbetsledare ser till att skola in nyanställda. De visar och berättar om vad nyanställda behöver veta samt var nödvändig information finns. Vår undersökning antyder dock på ett kunskapsglapp gällande riktlinjer för IT-området.

## 4.3 Identifierade problem

Genomförandet av våra intervjuer visade en antydan om att kunskapen gällande organisationens IT-relaterade policydokument varierar. De främsta punkterna gällande förbättringsmöjligheter anser vi vara följande:

- Policydokument genomsyrar inte organisationen enligt avsikt. Största problemet är saknad vetskap om dokumentens existens
- Eventuell bristande kunskap om rådande IT-relaterade policydokument tycks främst härledas till medarbetare med längre organisatoriskt avstånd till ledningen
- Uppföljning gällande kännedom om policydokument behöver förbättras
- Trots låg kännedom om policydokument i organisationens lägre nivåer agerar anställda över lag i enighet med gällande policy
- Bristande kunskap kan utgöra risker

Förbättring i organisationsstyrningen ses som en ständigt pågående process. Sedan en kortare tid tillbaka har därför ett samarbete med företaget Previa pågått med syfte att bland annat höja kompetensen inom IT-området hos arbetsledare. Som vi tidigare nämnt antyder svaren från våra informanter att kunskap och kännedom om organisationens policydokument är låg hos anställda längre ned i organisationen. Att anställda, trots låg kännedom, generellt arbetar enligt gällande policy kan vara en anledning till att inte problem gällande kunskapsbristen inte upplevs från ledningens sida.

# 5 Analys och Diskussion

Följande kapitel presenterar vår analys av forskningsresultatet. Resultatet diskuteras och ställs i relation till vald teori med avsikt att lägga grund till avslutande kapitel där vi bland annat presenterar slutsatser. Att IT-relaterade policydokument existerar inom organisationen gav våra informanter svar på. Undersökningen visade även att policydokument var något organisationen arbetade med men kännedom om gällande policydokument var dock splittrad. Det organisatoriska avståndet från ledning uppenbarade sig vara en avgörande faktor gällande vetskapen om vilka policydokument som gäller, var de finns att tillgå samt dokumentens innebörd.

## 5.1 Policyimplementation

I resultatdelen benämns att ny personal vanligtvis utbildas av kollegor, chefer eller arbetsledare. Bland genomgångar av vardagliga rutiner, arbetssätt och beskrivningar av hur arbetsplatsens IT-system används för just dem framgår av intervjuerna att nyanställda under utbildningen ska komma i kontakt med relevanta policydokument. Likt vi i föregående kapitel avslutades med, finns dock ett kunskapsglapp gällande policydokument på IT-området.

Vår informant från ledningen fäster vikt vid att ha rätt person till rätt uppgift för att lyckas väl. Till viss del anser vi att organisationen lyckas väl med detta enligt vår undersökning. Arbetsledare och chefer har kännedom om organisationens policydokument och vet när de bör tillämpa dem. Att sedan nå ut med dessa kunskaper till organisationens anställda på lägre nivå är svårare, döma av vår undersökning. Likt vi nämnde i resultatkapitlet verkar organisationen vara medvetna om att förbättringsutrymme finns gällande detta område och samarbetet med Previa tyder på vilja till att bli bättre.

Informanterna med vidareförmedlingsansvar uppger att nyanställda får den information de behöver under sin utbildning och att de under utbildningen kommer i kontakt med de policydokument relevanta för den nyanställdes arbetsuppgift. Detta väcker funderingar om hur informationen om policydokument mottags av den nyanställde samt hur den nyanställde senare i arbetet tappat kännedom om organisationens policydokument. Intervjusvaren tyder på att anställda med vidareförmedlingsansvar då och då kommer i kontakt med organisationens policydokument men att anställda bortom arbetsledare och chefer inte kommer i kontakt med gällande policydokument. Vi misstänker att detta kan vara en bidragande anledning till kunskapsbristen.

## 5.2 Diskussion om efterlevnad

Utan avsikt att upprepa tidigare nämnd information allt för mycket påvisade undersökningen vissa brister. Sammanfattat pekar vår undersökning åt en koppling mellan position i organisationen och anställdas kunskapsnivå om policydokument. Kunskap om policydokument kan härledas till position inom organisationen samt ansvarsrollen att vidareförmedla policydokument till andra anställda. Anledningarna till osäkerhet angående policydokument kan givetvis vara ett flertal samverkande faktorer och i vår undersökning har vi ej haft möjligheten att ta alla omständigheter. Dock anser vi kunna se vissa mönster från intervjuerna och för således våra resonemang enligt informanternas svar.

Eftersom vår undersökning fokuserar på implementation av policy samt motivation att följa gällande policydokument är det dessa områden vi analyserar även om fler faktorer kan påverka efterlevnaden. Vårt resultat bygger enbart på data från intervjuerna och känslan vid genomförande av intervjuer har genomgående varit att samtliga informanter varit ärliga när de besvarat våra frågor. Från flera informanter framgår att anställda har stor handlingsfrihet och själva får ta ansvar för sitt arbete samt sina arbetsuppgifter. Vissa svar väcker dock tankar om förbättringsområden samt potentiella förklaringar till hur glapp kan ha uppstått.

Beslut och policydokument genomsyrar inte organisationen enligt ledning avsikt. Delar av undersökningens resultat stämmer överens med hur Dermer och Lucas resonerar om regler och ledningens uppfattning av besluts genomslag. Trots minimal kännedom om policydokument i organisationens lägre nivåer verkar de anställda över lag agera i enlighet med gällande policy. Sett från ledningens sida anser vi således att policydokumentens innebörd över lag kan antagas nå fram godtyckligt. Dermer och Lucas menar att förändring efter beslut kan vara svåra att mäta den egentliga effekten av. Tendenser av detta påträffas i vår undersökning när vardagligt arbete, utifrån ledningens perspektiv, kanske tycks pågå enligt policy trots att anställda på lägre nivåer knappt känner till dokumentens existens.

Baserat på intervjuerna av anställda med vidareförmedlingsansvar får de anställda den information de behöver vid anställning. När informanternas arbetsuppgifter skiljer sig mycket åt är det naturligt att olika information blir relevant beroende på omständigheterna. Om IT-relaterade policydokument inte har en märkbar närvaro i arbetet hos en anställd finner vi det inte konstigt att kunskapen för det området är litet. Alla drags dock med arbetsuppgifter där vetskap om organisationens policydokument är nödvändig till en eller annan grad.

Med utgångspunkt i att en anställd får tillräcklig information vid anställning kan vi också diskutera vad det kan bero på. Herzberg beskriver att *hygienfaktorer* måste uppfyllas innan en individ påbörjar en successivt ökande motivationsprocess. Magkänslan vid de möten vi haft säger oss att organisationen verkar fylla många av dessa grundläggande behov. Personalen känns generellt välmotiverad samt uppskattar sina arbetsuppgifter samt kan identifiera sig med dem. Genom egen erfarenhet kan vi erkänna att det är svårt att ta till sig all information i situationer där mängder av ny information hastigt skall inläras. Informanter med ansvar i vidareförmedling av policydokument tycks ha en annan inställning till organisationens policydokument. Policydokument är av kännedom och ett intresse att medarbetare också ska känna till policydokument, relevanta för dem, visas.

Pfleeger och Pfleeger benämner tre viktiga aspekter om datasäkerhet varav en av dem är *tillgänglighet*. När informationen om relevanta policydokument endast visar sig hastigt under en anställds utbildning skulle det kunna vara en bidragande faktor till att kännedom om policydokumenten hamnar i skymundan. Att en anställd saknar tillräcklig vetskap om dessa dokument skulle kunna vara en bristande *hygienfaktor* för den anställde att lära sig om organisationens gällande policydokument. Anställdas motivation tycks, på lägre nivåer, påträffas vid andra områden närmare primära arbetsuppgifter.

Med stor handlingsfrihet inom organisationen och låg kontroll av anställda passar organisationsledningens syn på anställda till stor del stämma överens med McGregors *Theory Y*, (1966). Ansvar lämnas till individen och krav ställs således på anställda att söka information om policydokument på egen hand. På lägre organisatorisk nivå kan inställningen mot IT-relaterade policydokument vara mer passiv. Att likställa detta mot antaganden från McGregors *Theory X* är dock inte rättvist trots att strävandet efter kunskap om organisationens relevanta policydokument glider undan.

Ovan nämner vi variationer i arbetsuppgifter och tänker att någon *hygienfaktor* just i detta område bidrar till saknaden av policykunskap och därmed en passiv inställning. Undersökningen lade ingen vikt vid att studera andra områden av personalens beteende och arbetsuppgifter men när informanterna beskrev sina arbetsuppgifter påträffades inga tecken på motvilja till arbete likt antagandena om anställda i *Theory X*. I stället möttes vi av tecken på driv och vilja när de beskrev sina arbetsuppgifter påminnande om antagandena i *Theory Y*. En av informanterna hävdade att denne ville vara en god förebild och poängterade vikten att själv följa policydokument och rutiner.

## 5.3 Risker och hot

Vår informant på IT-avdelningen anser organisationen har god informationssäkerhet. Organisationens öppenhet banar ej väg för begär att komma åt företagshemligheter då i princip allt är offentligt. Dock är informanten medveten om att alla nätverk kan utsättas för intrång samt att informationssäkerhet inte får glömmas bort eller ignoreras. Informanten som arbetar som kyrkoherde anser att organisationen inte är bättre skyddad en någon annan men att organisationen inte är en intressant måltavla. Informanten anser att all kommunikation över Internet kan övervakas och läsas. Dock lagras känslig information om privatpersoner. Om denna information skulle läckas ut skulle det få vissa konsekvenser men organisationen skulle inte skadas allvarligt. Däremot kan deras ryckte skadas om ett sådant angrepp skulle inträffa.

Angripare har litet intresse i att utföra en attack mot samfälligheten. Lite information är intressant för dem och det skulle vara svårt att få någon slags ekonomisk vinning. *White hats* och *grey hats* kan ha ett intresse att hitta säkerhetshål i IT-systemet. *Black hats* och *script kiddies* kan också ha ett visst intresse angripa IT-systemet men samfälligheten är inte i mer risk än någon annan organisation. Däremot kan *hacktivister* ha i intresse att angripa samfälligheten. Samfälligheten är en kristen organisation och en del av Svenska kyrkan. *Hacktivister* med en annan religion kan ha i intresse att utföra en *DDOS-attack* för att stoppa tillgängligheten av samfällighetens IT-system för att försvåra deras arbete.

De anställda med lägre position utgör en större del av organisationen och okunskap om säkerhet kan leda till att en incident inträffar. Risken att en obehörig skulle få tillgång till inloggningsuppgifter via en anställd är låg då samtliga informanter svarade att de inte skulle ge ut uppgifterna ens till en kollega. Det finns en viss risk att virus kommer in i IT-systemet då några av informanterna svarade att de har installerat programvara som inte har med deras arbetsuppgifter att göra men samtidigt har IT-systemet virusskydd för att förhindra detta. Ett problem är att de anställda inte vet vilka rutiner som finns och är osäkra på var de kan ta del av dem.

## 5.4 Metodreflektion

Över lag tycker vi att vi har valt metod för vår undersökning väl. Däremot finns det alltid någonting som går att förbättras. I vårt fall är det största problemet med vår undersökning urvalet. För att få bättre stöd för vår slutsats skulle vi behöva intervjua fler personer. I vår undersökning har vi intervjuat fem personer där alla kommer från olika delar av organisationen. Det är stor sannolikhet att dessa personer inte representerar resultatet vi skulle fått fram om fler personer från varje del hade intervjuats. Urvalets storlek berodde på tidsbrist. Ett annat problem med urvalet var att personerna inte blev helt slumpmässigt utvalda. När vi tagit kontakt med organisationen och uttryckt vårt intresse av att utföra intervjuer fick vi en lista med personer som vår kontaktperson valt ut. Det var ungefär två personer per position inom organisationen men alla positioner fanns inte med. Dock valdes personer ut slumpmässigt utifrån listan med undantag av förvaltningschefen som kändes viktig att få med i undersökningen.

För att ytterligare stärk underlag för slutsatser kunde även en kvantitativ studie genomförts utöver den kvalitativa. Att undersöka hur bra anställda var på att följa de policydokument som fanns var fem personer är alldeles för lite för att få ett bra underlag även om vi kan påpeka eventuella samband. En kvantitativ studie med enkäter hade kunnat skickas ut till större delen av, om inte hela, organisationen vilket skulle höja resultatets validitet. Då skulle eventuellt ett annat resultat fås fram.

Genom att göra en kvalitativ studie och fokusera på utvalda delar av organisationen kunde vi fördjupa oss bättre samt få ett mer detaljerat resultat. Mer tid kunde läggas på varje intervju i stället för att ha många korta. Inför intervjuerna hade vi förberett frågor anpassade efter vilken position personen vi intervjuade hade. Det gjorde att vi lättare kunde ta reda på relevant information. Till exempel är det inte relevant att fråga om en persons roll i att ta fram nya policydokument om vi sedan tidigare visste att personen inte hade någon roll i detta.

För att undersöka efterlevnaden användes främst organisationens egna policydokument. Utifrån dessa dokument kunde vi avgöra hur väl personer som intervjuades följde dem. Eftersom organisationens egna dokument användes blev det enkelt att få ett mått på hur väl policydokumenten följdes. Vi analyserar empirisk data med hjälp av vår teori enligt beskrivning i kap 2.5.

# 6 Avslut

Avslutande kapitel reflekterar vi över uppsatsens resultat samt analys av resultat. Slutsatser presenteras utifrån nämnda kapitel varefter vi avslutar med förslag till fortsatt forskning. I kapitlet lämnar vi även förslag och rekommendationer för lösningar av brister eller tänkbara åtgärder i avsikt att minska dem. Vi lyfter även fram frågeställningen i avsikt att framhäva hur vi anser ha lyckats besvara våra forskningsfrågor:

- *Hur mynnar IT-relaterade policydokument ut till organisationens olika delar?*
- *Hur kommer anställda i kontakt med policydokument och hur motiveras de att följa dem?*

## 6.1 Slutsatser

Baserat på de svar våra informanter försett oss med till undersökningen har vi kunnat dra vissa slutsatser.

- Glapp är funnet i kunskapsnivån om IT-relaterade policydokument mellan de personer vi intervjuat
- Samband funnet mellan anställdas kunskapsnivå om IT-relaterade policydokument samt den anställdes organisatoriska nivåtillhörighet
- Eventuell förklaring av sambandet kan härledas till ansvarsroller gällande vidareförmedling av policy
- Ansvar om vidareförmedling kan kopplas till högre motivation om att ha kännedom beträffande vilka policydokument som är relevanta, var de finns att tillgå samt när de bör tillämpas
- Individers handlingsfrihet och egna ansvar inom organisationen tillsammans med avsaknad av uppföljning gällande kunskap om IT-relaterade policydokument kan vara eventuell orsak till kunskapsbrist om relevanta policydokument

Att glapp visade sig vid policyimplementation var något vi misstänkte skulle påträffas när intervjuerna genomfördes. På vilket sätt var dock bortom vår uppskattningsförmåga. Ett spännande påträffat samband var, vilket punkterna ovan nämnde, att kunskapsnivån om organisationens policydokument tycktes kunna höra samman med den anställdes organisatoriska tillhörighet. Vidare diskussion om detta ledde oss till en antydan om ännu ett samband. Personer högre upp i organisationen tycktes mer motiverade att ta lärdom av relevanta policydokument, hålla reda på var de finns samt var de fanns att tillgå.

Ett samband tycktes synas mellan mängden ansvar för vidareförmedling av organisationens policydokument samt individens kunskap och engagemang inom området. Organisationsledningen tycks dela synen på anställda med McGregors *Theory Y* om att frihet och ansvar leder till prestation vilket på de flesta håll säkerligen stämmer. Dock skulle viss kontroll eller uppföljning, likt antagandena i *Theory X* kräver, gällande kännedom om organisationens policydokument kunna vara ett hjälpmedel till att säkerställa att kunskapen stannar hos anställda.

Vi misstänker att när organisationens IT-relaterade policydokument inte berörs i en anställds vardagliga arbete kan de komma att glömmas bort. Hos anställda med ansvar rörande vidareförmedling av policydokument visade undersökningen att de tycks besitta bättre kunskap gällande området. Fler drag i beteendet pekade åt likheter med antaganden i McGregors *Theory Y* när ansvarsrollen växte vilket även påvisar likheter med Herzberg som menar att motivation att prestera är en ökande process. Viktigt att ha i åtanke är att vi inte fann kunskapsbristen inom området att vara en motvilja eller lathet från individerna utan snarare vara orsakat av en medvetenhetsbrist gällande policydokumentens existens och innebörd.

Individer med vidareförmedlingsansvar tycktes vara mer motiverade att besitta nödvändig kunskap om de policydokument som berörde dem eller skulle föras vidare till andra anställda. Ännu ett samband träder här fram. Ökat ansvar visar även, i vår undersökning, medföra ökad motivation och kunskap om organisationens policydokument. Organisationen har här lyckats skapa en arbetsmiljö där vidareförmedlingsansvar motiverar anställda till nödvändigt intag av relevant information om relevanta policydokument. Om sambandet sträcker sig till fler områden var inget undersökningen berört och kan därför varken förnekas eller bekräftas.

I undersökningen gavs inte möjligheten att följa en process enligt ovanstående stycke på grund av given tidsram och vi kan därför inte bekräfta sambandet mellan ansvarsroll och motivation. I undersökningen lyckades vi dock observera att, precis som ovanstående stycke beskriver, fann vi att individer med större ansvar i implementationsprocessen tycks vara mer motiverade att besitta nödvändig kunskap om IT-relaterade policydokument.

Kunskapsglappet undersökningen påvisade pekade åt att organisatoriskt avstånd från ledningen var en bidragande faktor till en anställds kunskapsnivå inom området. Detta må väl stämma, men avståndet i sig verkar inte vara den starkaste faktorn till kunskapsnivå och motivation utan snarare ansvarsrollen positioner på högre organisatorisk nivå medför. När våra informanter inte längre hade ansvar vid att föra vidare kännedom om organisationens policydokument, tycktes deras motivation riktas åt anda delar av arbetet.

Att denna kunskap minskar skulle kunna bero på handlingsfriheten och brist på uppföljning inom området . Andra arbetsuppgifter tar större plats då de är mer centrala och vardagligt arbete kallar inte på samma behov av kännedom om policydokument som hos de anställda med vidareförmedlingsansvar. Medvetenhet om brister medför lyckligtvis utrymme för förbättring och nedan diskuterar vi eventuella förbättringsmöjligheter och förslag på vidtagande av åtgärder.

## 6.2 Förbättringsförslag

Efter genomförd studie, analys av resultat och våra dragna slutsatser presenteras nedan förslag på åtgärder för att minimera problem vid implementation av policydokument. När anställda har stor frihet i hur de utför sitt arbete kan det, likt tidigare påpekat, medföra komplikationer. När minimal uppföljning sker gällande kunskap om policydokument hos anställda hamnar organisationen i en situation där organisationens policydokument tappar genomslag. Angående att nå ut med policydokument mer effektivt till anställda utan vidareförmedlingsansvar, på lägre organisatorisk nivå, anser vi att policydokument skulle kunna bli del i deras vardag trots att nuvarande arbetsuppgifter givetvis skall fortsätta vara centrala.

När en anställd saknar kunskap om policydokument förlitar de sig till sunt förnuft men samtidigt utgörs en risk när vetskap om en policy saknas, blir det svårt att vara motiverad till att följa den. Kunskapsbrist leder ökad risk för angrepp mot organisationen. För att förbättra kunskapen om säkerhet bör organisationen förtydliga att policydokument finns att tillgå samt underlätta tillgängligheten för alla anställda. Detta skulle kunna ske redan vid utbildning av nyanställda men även nuvarande anställda.

Organisationen bör regelbundet utföra uppföljning för att se till att policydokument följs. Uppföljning bör ske oftare vid ny policyimplementation samt vid nyanställning. För att få de anställda mer motiverade att följa de policydokument som finns bör policydokumenten få en större del av vardagen. Om de anställda skulle ha möjlighet att påverka de policydokument som finns skulle de dels ha större kunskap om dem eftersom de har varit med och tagit fram policydokumenten och dels känner sig mer motiverade att följa den. Anställda skulle kunna känna sig mer motiverade att följa policyn eftersom i och med de varit med och tagit fram den. Då skulle också en ansvarskänsla för policyn kunna träda fram, en slags stolthet över sitt bidrag till den.

Genom att ge de anställda mer ansvar över policydokumentens utformning blir de en större del av vardagen. Det leder till att de anställda blir bättre på att följa policydokumenten då de anställdas kunskaper om vilka rutiner som finns ökar. Det kommer i sin tur leda till att hela organisationen kommer få ett säkrare arbetssätt eftersom policydokumenten blir mer integrerad i de anställdas vardag och det får bättre kunskaper om säkerhet.

## 6.3 Besvarande av forskningsfrågor

Genomförda intervjuer gav oss möjligheten att se hur policydokument mynnar ut i organisationens olika delar. Möjliga brister vid implementation av policydokument kan vara många och likaså anledningar till eventuella problem. De huvudsakliga implementationsproblem vår undersökning lett oss till är följande:

Vid implementation av policydokument kan individers handlingsfrihet inom organisationen vara en bakomliggande orsak till påträffad kunskapsbrist om relevanta policydokument. Låg grad av uppföljning gällande kännedom om IT-relaterade policydokument orsakar att kunskapen hos anställda inte säkerställs. Utan delaktighet i policyarbetet påvisar undersökningen att anställdas relation till policydokument försvinner när de inte blir en del i arbetet.

Förutsatt att anställda under utbildning kommer i kontakt med relevanta policydokument, likt intervjusvaren visar, skulle mer vikt kunna fästas vid att se till att informationen framgår tydligare. När kunskap om policydokument inte når fram enligt avsikt kan det leda till minskad medvetenhet vilket kan innebära säkerhetsrisker. Förutom ökade säkerhetsrisker kan bristande medvetenhet hos anställda leda till saknad motivation att förskaffa sig kännedom om policydokument.

Anställda delaktiga i policyimplementation blir mer motiverade att inhämta nödvändig kunskap om var gällande information finns att tillgå vid behov. Motivation att följa en policy förutsätter kännedom om att den finns och när den bör tillämpas. Vår undersökning visar att anställda med kännedom om policydokument även var mer motiverade att följa dem. Delaktighet i policyarbetet anser vi därför vara den viktigaste faktorn för att motivera anställda att följa en policy då de lättare kan identifiera sig i den. I vår undersökning ser vi därför ett samband där högre delaktighet i form av ansvar lett till personal mer motiverad att följa en policy.

## 6.4 Framtida forskning

Om mer tid funnits till att utföra undersökningen skulle det vara intressant att intervjua fler personer inom organisationen. För att få det bästa resultatet bör alla i organisationen intervjuas. Det skulle även vara intressant att utföra undersökningen på andra organisationer för att få ett bättre underlag för våra påståenden. Om glappet mellan anställda och ledningen angående kunskap om policydokument upptäckas hos fler liknande organisationer kan vårt resultat styrkas ytterligare. I vår undersökning undersökte vi en väldigt öppen organisation som inte lagrade mycket känslig information så resultatet från en väldigt sluten organisation med mycket känslig information skulle vara väldigt intressant att ställa i relation till resultatet.

Avsaknaden av liknande studier på denna typ av organisation gör vårt resultat intressant. Trots begränsad omfattning av vår studie skulle resultatet kunna väcka andra forskares intresse att bygga vidare på studien, göra liknande undersökningar på andra pastorat eller liknande organisationer. Detta skulle kunna ge bredare underlag gällande vårt resultat där våra slutsatser både skulle kunna stärkas med bättre belägg eller eventuellt motbevisa samband vi funnit. Även andra delar av Svenska kyrkan kan tänkas ha en liknande organisationsstruktur och denna undersökning kan tänkas vara intressanta för jämförelsestudier.

Att generalisera resultat samt slutsatser från undersökningen ställer vi oss försiktiga till på grund av låg grad av statistiska belägg i form av större omfattning av informanter och därav högre säkerhet. Dock kan undersökningsresultatet ses som en språngbräda för området vilket kan skapa förutsättningar till vidare forskning att bygga vidare på våra upptäckter vilket vi anser vara det unika med undersökningen.

# 7. Referenser


Al-Hamdani, W.A. & Dixie, W.D. (2009) *Information Security Policy in Small Education Organization*. Information Security Curriculum Development Conference (S. 72-78).

Aloul, F (2012, Augusti 3) *The Need for Effective Information Security Awareness*. Journal of Advances in Information Technology. Hämtat december 14 2013 från http://ojs.academypublisher.com/index.php/jait/article/view/jait0303176183/5224

Angela Sasse, M och Flechais, I (2005) Usable Security: Why Do We Need It? How Do We Get It? Hämtat december 14 2013 från http://discovery.ucl.ac.uk/20345/2/cransimpsonbook.pdf

Dermer J.D, Lucas, R. G, (1986) *The Illusion of Managerial Control. Accounting, Organizations and Society*, 11 (6), s. 471-482

Hacker (computer security). (2014, January 2). I: *Wikipedia, The Free Encyclopedia*. Hämtat 18:09, Januari 2, 2014, från http://en.wikipedia.org/w/index.php?title=Hacker_(computer_security)&oldid=588817415

Herzberg, F. Mausner, B. Snyderman, Barbara B B, (1959). *The Motivation to Work*. New York. John Wiley & Sons Inc. ISBN 0471373893

McGregor, D. (1966). *The Human Side of Enterprise.* Leadership and motivation. Cambridge, MIT.

Mirkovic, J., Dietrich, S., Dittrich, D. & Reiher, P. (2004) *Internet Denial of Service Attack and Defense Mechanisms*. Upper Saddle River, N.J: Prentice Hall Professional Technical Reference.

Oates, B. (2006). *Researching information systems and computing*. London Thousand Oaks, Calif: SAGE Publications.

Pfleeger, C. & Pfleeger, S. (2007). *Security in computing*. Upper Saddle River, NJ: Prentice Hall.

Sargeant, J (2012) *Qualitative Research Part II: Participants, Analysis, and Quality Assurance*. Hämtat december 29 2013 från http://www.jgme.org/doi/pdf/10.4300/JGME-D-11-00307.1

Trochim, W., Donneley, J. P., (2006) *The Research Methods Knowledge Base, 3e.* Cincinnati. Atomic Dog Publishing. ISBN 1592602916

*Types of Hacker* (läst 2013). Hämtat december 14 2013 från http://www.secpoint.com/types-of-hacker.html

Yin, R. K. (2009), *Case Study Research: Design and Methods, 4e.* Thousand Oaks. Sage inc. ISBN 978-1-4129-6099-1

# Bilaga A - Intervjuguide

## Gemensamma frågor för alla intervjuer

### Inledning

- Beskriv kort vad du har för position inom svenska kyrkan och vad du har för arbetsuppgift.
- Hur länge har du arbetat inom svenska kyrkan?
- Beskriv vad du använder dator till i arbetet?

### Policydokument

- Beskriv hur fick du lära dig om informationssäkerhetspolicyn?
- Pratas det om policyn i det vardagliga arbetet?

### Efterlevnad

- Sparar du känslig information på din dator?
- Om Ja: Vad gör du för att se till att informationen inte hamnar hos fel person?
- Har du använt arbetsplatsens internet för att göra icke-arbetsrelaterade saker?
  Exempelvis att gå in på facebook eller ett nätforum?
- Om en kollegas dator slutar fungera och hon behöver skicka ett dokument, lånar du ut ditt användarkonto?
- Kan du använda egna enheter som privat mobiltelefon eller laptop på arbetsplatsen och har du i så fall gjort det
- När du går på semester eller är sjuk, gör du så att det automatiskt skickas ett email som berättar att du inte kan svara?
- Har du installerat någon programvara som organisationen inte tillåter eller inte skulle tillåta?
- Ser du några yttre hot mot Svenska kyrkans informationssäkerhet?

## Intervju 1

### Implementation av policy

- Beskriv hur det går till när en policy implementeras.
- Har du någon roll i att vidareförmedla informationssäkerhetspolicyn till andra?
- Om Ja: Beskriv kortfattat på vilket sätt du arbetar med det.
- Hur utbildas personalen när en policy ska implementeras?
- Försöker ni på något sätt motivera de anställda att följa policyn?
- Arbetar ni med någon slags uppföljning för att säkerställa att policydokumenten följs?
- Arbetar du med att förbättra de informationssäkerhetspolicyer som finns?
- Om Ja: Hur arbetar du med att förbättra era informationssäkerhetspolicyer?

## Intervju 2

### Implementation av policy

- Har du någon roll i att vidareförmedla informationssäkerhetspolicyer till andra?
- Om Ja: Beskriv kortfattat på vilket sätt du arbetar med det. Gärna något exempel
- Om någon är nyanställd. Blir denne informerad om informationssäkerhetspolicyn i samband med introduktionen till arbetet?
- (Om ansvarsroll finns:) Försöker ni på något sätt motivera anställda att följa policyn?
- Finns någon slags uppföljning för att säkerställa att policydokumenten följs?
- Arbetar du med att förbättra de informationssäkerhetspolicyer som finns?

## Intervju 3

### Implementation av policy

- Har du någon roll i att vidareförmedla informationssäkerhetspolicyn till andra?
- Om Ja: Beskriv kortfattat på vilket sätt du arbetar med det.
- Beskriv hur du blev utbildad i de policydokument som finns.
- Arbetar du med att förbättra de informationssäkerhetspolicys som finns?
- Om Ja: Hur arbetar du med att förbättra era informationssäkerhetspolicies?

## Intervju 4

**Kännedom om policydokument**

- Känner du till att det finns en informationssäkerhetspolicy?
- Om Ja: Beskriv hur fick du lära dig om policyn? Hur var informationen om att policyn skulle följas?
- Om Nej: Blev du på annat sätt informerad om vad som är eller inte är tillåtet gällande datoranvändning i arbetet?

## Intervju 5

**Kännedom om policydokument**

- Känner du till om det finns en informationssäkerhetspolicy?
- Om Ja: Beskriv hur fick du lära dig om policyn? Hur var informationen om att policyn skulle följas?
- Om Nej: Blev du på annat sätt informerad om vad som är eller inte är tillåtet gällande datoranvändning i arbetet?