EXAMENSARBETE

Informationssäkerhet i kommuner

Mattias Niemi

Filosofie magisterexamen
Informationssäkerhet

Luleå tekniska universitet
Institutionen för system- och rymdteknik

LULEÅ TEKNISKA UNIVERSITET

Förord

Denna D- uppsats omfattar 15 högskolepoäng och ingår i en filosofie magisterexamen inom området informationssäkerhet. Ämnet informationssäkerhet tillhör avdelningen för datavetenskap som är en del av Institutionen för System- och Rymdteknik vid Luleå Tekniska Universitet.

Jag som skrivit vill passa på att tacka några personer som haft betydelse för mig och hjälpt mig under min utbildning och med mitt examensarbete. Först ett stort tack till Harriet Nilsson och Lars Furberg för allt stöd och engagemang under min utbildning.

Ett stort tack till alla respondenter som ställt upp och svarat på mina frågor. Tack vare er har denna uppsats varit möjlig att genomföra. Tack för ert bemötande, öppenhet och tid. För att examensarbetet blev verklighet vill jag tacka till Sören Samuelsson för hans handledning.

Piteå, juni 2011

Mattias Niemi

Sammanfattning

Denna uppsats behandlar hur informationssäkerhet behandlas i kommuner och den prioritering kommunledningen gör utifrån deras uppfattning av risk och den strategiska vikten som läggs på deras informationssystem. Utgångspunkten är en rapport från Myndigheten för samhällsskydd och beredskap som visar på att det finns stora brister i planeringen för att kunna driva deras verksamhet vidare efter avbrott. Kommuner måste fungera även om det uppstår en störning i form av ett avbrott i deras informationssystem . Därför är det viktigt att identifiera vilka verksamheter i kommunen som är helt nödvändiga för att kunna undvika oacceptabla konsekvenser för medborgarna. Utöver detta har kommunerna svårigheter att hålla en kontinuitet i sin planering. Studien fann att informationssäkerhet inte prioriteras högt av kommunledningen mycket på grund av de kontextuella faktorerna inom och utanför kommunen . Detta påverkade de strategiska och operativa insatser som kommunen vidtar .

Abstract

This thesis deals with how information is treated in the municipalities and the priority local management makes based on their perception of risk and the strategic importance placed on their information systems. The starting point is a report from the Agency for Civil Contingencies, which shows that there are major gaps in planning to run their operations further from failure. Municipalities must function even if there is a disturbance in the form of an interruption in their information systems. It is therefore important to identify which activities in the municipality that is completely necessary to avoid unacceptable consequences for the citizens. In addition, the municipalities have difficulty in maintaining continuity in their planning. The study found that information security is not high priorities for the council leadership much because of the contextual factors within and outside the municipality. This affected the strategic and operational action by the municipality to take.

Innehållsförteckning

1 Inledning

I detta kapitel vill jag teckna en bakgrund för den aktualitet som mitt uppsatsämne har samt beskriva den utgångspunkt som jag har för mitt arbete.

1.1 Bakgrund och problemområde

Rapporten ”*Samhällets informationssäkerhet, lägesbedömning 2009*” från *Myndigheten för Samhällsskydd och Beredskap (MSB)* visar att samhällets olika funktioner idag är beroende av fungerande IT och hantering av information. Därför är en tillräcklig nivå av informationssäkerhet nödvändigt och viktigt, vidare så utgör människors beteende utgör ofta den svaga länken i arbetet med säkerhet. Detta både försvårar och direkt hotar informationshanteringen. Rapporten pekar också på att hoten blir alltmer avancerade och den IT- relaterade brottsligheten bedrivs på närmast en rent affärsmässig nivå. Hotbilden är redan idag ett betydande problem där exempelvis bedrägerier blir allt mer sofistikerade och utnyttjar mänskliga svagheter i allt större utsträckning.

En allt komplexare IT-miljö och fler integrerade nätverk medför att fokus ofta läggs på mer begränsade och hanterbara IT-relaterade problem inom den egna organisationen. Rapporten tar upp att kopplingar och analyser också måste ske från ett samhällsperspektiv. För att kunna utnyttja informationsteknikens stora potential och skapa ett tillräckligt förtroende hos användarna är det avgörande att bygga upp grundläggande informationssäkerhet och kompetens inom informationssäkerhetsområdet.

Avgörande faktorer för at nå framgång är förtroende och användarvänlighet men brister i tekniska lösningar, integritetsskydd och ett otillräckligt säkerhetsmedvetande skapar hinder för att kunna utnyttja IT effektivt. Av den anledningen är ett ändamålsenligt arbete med informationssäkerhet som hanterar dessa brister är mycket viktigt och bidrar till en god samhällsutveckling både nationellt och internationellt.

Att effektiv IT-användning förutsätter både administrativ som teknisk säkerhet är något som MSB rapporten betonar. Rapporten lyfter fram olika områden som behöver särskild uppmärksamhet, däribland outsourcing (extern tjänstehantering), nya användarmönster och kontinuitetsplanering.

Kontinuitetsplanering är en grundläggande del av det interna arbetet med säkerhet för att kunna säkerställa organisationens verksamhet. Brister har identifierats i flera sammanhang, bland annat brister hos kommuner i deras arbete med att motverka och dokumentera avbrott i sin verksamhet samt att skydda kritiska rutiner från effekter av oförutsedda avbrott eller katastrofer. Bristerna pekar på ett behov av åtgärder för att främja ett systematiskt arbete med informationssäkerhet.

De flesta kommuner har policydokument och definierade ansvarsroller och inriktning för hur arbetet med informationssäkerhet skall genomföras. Trots det finns där stora brister när det gäller kontinuitetsplanering och dess omfattning. De största brister rör planering relaterat till hur verksamheterna arbetar för att motverka och agera vid oplanerade avbrott.
Rapporten pekar på att det i många fall saknas katastrofplaner och brister i hur kontinuitetsplanering ska samordnas mellan ledning, verksamhet och IT-stödet. Inom verksamheterna saknas också insikten om hur beroende de är av IT-stödet. Kommunerna har också svårt att hålla sin planering aktuell och få en kontinuitet i hela planeringsprocessen. Ett flertal av de undersökta kommunerna har startat upp processen men den har sedan tappat fart och när de tar nya tag i planeringen tas inte de tidigare erfarenheter och kunskaper tillvara.

De hot och risker som finns i vår omgivning skapar ett behov av säkerhet. Begreppet säkerhet kan appliceras på i princip all mänsklig verksamhet och i alla delar av samhället, därför är det nödvändigt att vara medveten om vilka hot som existerar och hur man kan skydda sig mot dessa hot (Oscarsson, 2001). Säkerhetsproblem som kan kopplas ihop med datorer har existerat så länge datorer har funnits. De säkerhetsaspekter som kommer i fråga handlar om säkerhet kopplad till datorer och informationsteknik (IT). Det vill säga IT-säkerhet och informationssäkerhet (ibid.).

Inledning

Informationsteknologin har inneburit stora fördelar för utvecklingen av vårt samhälle och det har skapat nya möjligheter att kommunicera och interagera med varandra samt underlättat vår tillvaro. IT har blivit en integrerad del av vårt moderna liv och genomsyrar alla aspekter av affärsliv och privatliv (Van Niekerk & Von Solms, 2009). Samtidigt behöver de flesta organisationerna informationssystem för att kunna växa och överleva. De behöver därför vara målmedvetna med att skydda sina informationstillgångar. Många av de processer som är nödvändiga för att uppnå detta bygger på ett strukturerat beteende från människor inom organisationen eftersom medarbetare utgör, avsiktligt eller oavsiktligt, på grund av slarv eller okunskap, det största hotet mot informationssäkerhet (ibid.).

Med informationssäkerhet menas organisationens förmåga att bevara konfidentialitet, riktighet och tillgänglighet hos information. Utöver detta infattas begreppen autencitet, spårbarhet, oavvislighet och tillförlitlighet. Informationssäkerhet utgår ifrån att information är viktig och oftast en vital resurs som kan vara utsatt för hot, oavsiktliga såväl som avsiktliga, och måste därför skyddas på ett sätt som garanterar att informationen inte kommer till obehörigs kännedom, modifieras, förstörs eller på annat sätt görs otillgänglig (SIS HB 550, 2007). IT-området är mycket föränderligt och den tekniska utvecklingen går mycket snabbt och blir allt mer komplex. Informationssäkerhet är inget undantag utan tillhör istället de områden som förändras snabbast (Oscarsson, 2001).

Konsekvensen av framstegen som skett inom informationstekniken och förändringen av organisationens gränser har satt information och data i förgrunden. Detta då information hjälper företag att realisera sina mål och underlättar för chefer att fatta adekvata beslut. I företagens gamla affärsmodeller fanns ofta data och information lokaliserat på ett enda ställe. De var därför lättare att skydda och förhindra att de kom i orätta händer . Det var möjligt att med ganska stor säkerhet garantera dess konfidentialitet, riktighet och tillgänglighet Dhillon, (2001). I dag, på grund av organisationens karaktär och vidden av den informationsbearbetning som krävs av organisationen, handlar ledning av informationssäkerhet inte längre enbart om konfidentialitet, riktighet och tillgänglighet. Organisationer måste fokusera på att etablera ansvar, integritet hos personer, trovärdighet och etik menar Dhillon och Backhouse (2000) samt Dhillon (2007).

Förändring i organisationers strukturer, framstegen inom informations- och kommunikationstekniken, och den ökade tilliten på information hos organisationer innebär en hel del utmaningar i att utöva en bra ledning av organisationen. De senaste åren har visat att organisationer inte lyckats att utveckla policys som kan hantera de problem som informationssäkerhet innebär Dhillon, (2001).

Med utgångspunkt från organisationers beroende av datorsystem i sin verksamhet är det möjligt att anta att de har väletablerade kontinuitetsplaner och katastrofplaner. Tyvärr visar forskning visar att så inte är fallet. Det läggs inte tillräckligt vikt på katastrof och kontinuitetsplanering från ledningens sida utan det anses som oviktigt och fokus läggs istället på projekt som generar intäkter(ibid.).

En studie av Elspeth McFadzean, Jean-Noel Ezingeard and David Birchall, (2007) visar att ledningens engagemang för informationssäkerhet är starkt kopplat till ledningens uppfattning av risk och det strategiska värdet av IT. Detta återspeglas i budgeten för informationssäkerhet och de förändringar som organisationen genomför för att skapa och upprätthålla god informationssäkerhet.

Det finns enligt Dhillon (2007) också problem med att överföra beslut som rör informationssäkerhet mellan de olika nivåerna i organisationer. Detta innebär att när beslut landar på den operativa nivån av organisationen uppstår oavsiktligt en brist på ägarskap av frågan. I många fall intar högsta ledningen en hands-off attityd, vilket förvisso kan fungera om organisationen inte är beroende av sina IT-system. Detta är ju sällan fallet i dagens verksamhetsmiljöer. Därför är det viktigt att skilja på vilken nivå beslut skall tas på, strategisk, administrativ eller operativ nivå och koppla dem mot de olika mål som finns på respektive nivå. Balansen mellan strategiska och operativa beslut bestäms till stor del av organisationens omgivning och miljö. Det är därför nödvändigt att identifiera ett brett utbud av strategiska och operationella mål. Det är svårt rangordna dessa eftersom de är så kontextberoende(ibid.).

När människor fattar beslut som medlemmar av en organisation måste de ta hänsyn till en rad olika förhållanden som hänger ihop med den organisatoriska kontexten för handlande. Behöver de även ta hänsyn till bland annat sin plats i den formella organisationsstrukturen, vilka mål organisationen strävar att realisera, vilka slags regler och procedurer som gäller för arbetet samt vilka kulturella principer som gäller för organisationen March, (1994).

Inledning

Informationssäkerhet har som område lidit brist på helhetssyn och styrning, det vill säga behoven av konfidentialitet, riktighet och tillgänglighet i all information och informationshantering. Att studera enbart tekniska lösningar är inte tillräckligt, även andra faktorer som användarmönster, ekonomiska förhållande och rättslig reglering har betydelse. Olika aktörer påverkar utformningen och nivån av informationssäkerhet, alltifrån myndigheter, teleoperatörer, lagstiftare, antagonister, standardiseringsorgan, teknikutvecklare och organisationsledning. Utöver dessa aktörer så tillkommer den enskilda individens påverkan av utformning och nivå av informationssäkerhet. Förutom olika aktörer innefattar helhetssyn även allt från en vardagssäkerhet till säkerhet vid krishantering (MSB,2009).

Organisationer och dess informationssystem utsätts i allt större utsträckning för risker som är IT-relaterade. Det vill säga potentiella hot och sårbarheter. Informationssäkerhet har blivit viktigare eftersom organisationer hotas både från interna och externa miljöer McFadzean et al., (2007).

Samtidigt som IT blir mer och mer kritisk för företag och andraorganisationer så ökar hoten och sårbarheten. Därmed också riskerna till följd av mer komplex teknik, e-handel och outsourcing Haverblad, (2006).
Många teoretiker förespråkar att effektiva policys skall skapas på högre ledningsnivå. Detta för att högre chefer är kapabla att kunna utvärdera organisationen med en helhetssyn samt har befogenhet att se till att nya system och rutiner genomförs i tid. Det finns dock en fortsatt brist på förståelse om den strategiska vikten av att hantera informationssäkerhet McFadzean et al., (2007).

Dhillon(2007) pekar på fyra typer av utmaningar för ledningen av informationssäkerhet. Den första utmaningen är att etablera bra ledningsrutiner i en geografisk utspridd miljö och samtidigt kunna kontrollera organisationens verksamhet. Den andra utmaningen är att etablera säkerhetspolicys och rutiner som korrekt avspeglar den organisatoriska kontexten och nya affärsprocesser. Den tredje utmaningen är att fastställa relevanta tekniska kontroller och tillhörande ansvarsfördelning. Den fjärde utmaningen är att etablera adekvata IT- katastrof återställningsplaner (disaster recovery plans).

Informationssäkerhet är en nyckelfaktor för verksamheter. Kontinuitet på information är livsnerven i detta millennium. Skyddet av information från källor utom eller inom organisationen är avgörande för att framgångrikt kunna driva verksamheten(ibid.).

Haverblad, (2006) pekar på några vanliga problem som drabba IT-verksamheten i en organisation. Allt större krav ställs på att IT-verksamheten ska kunna tillgodose hög tillgänglighet och tillförlitlighet. Samtidigt som krav på riskhantering och förmåga att kunna återskapa IT-tjänster vid allvarlig störning eller katastrof, inom för organisationen rimlig tid, inte ägnas samma uppmärksamhet. Riskanalyser och värdering av riskerna genomförs inte riskmedvetandet är lågt inom organisationen. Riktlinjer och policy för informationssäkerhet saknas eller så har de inte förankrats, därför de följs inte. Bristerna i säkerhet gör att organisationer inte skyddar sina tillgångar och information i den utsträckning som är nödvändig, vilket gör att de utsätter sig för onödiga risker. Ingen säkerhetsställer att kritiska IT-tjänster och information kan återskapas och återställas i händelse av en allvarlig störning, genom att upprätta en kontinuitetsplan för IT. Detta för att minimera påverkan på kärnverksamheten och detta skulle inträffa. Avsaknaden av vision, mål och strategi för IT-verksamheten eller om den inte är sammanlänkad med kärnverksamhetens strategier och mål resulterar i att IT-verksamheten inte vet vad som förväntas av dem och måste gissa sig till vilka behov som finns. De får basera deras beslut och prioriteringar efter vad de tror är prioriterat och ofta innebär det att IT-verksamheten inte stödjer verksamhetsprocesserna(ibid.).

Eftersom en kommun måste fungera även om störningar och avbrott sker är det ju därför viktigt att identifiera de verksamheter som är absolut nödvändiga för att undvika oacceptabla konsekvenser för verksamheten, och i slutändan medborgarna. Rapporten från MSB beskriver en bild av läget som råder idag och var brister finns, men som jag ser det, svarar den inte på frågan varför det ser ut som det gör. Varför saknas katastrofplaner och kontinuitetsplaner? Att prioriteringen av informationssäkerhet inte är speciellt hög går att utläsa av de brister som presenteras i rapporten. Prioritering är i ordets rätta bemärkelse att ge företräde åt något. För mig innebär prioritera att välja, i detta sammanhang utgör att inte välja också ett val. Oavsett beslut eller icke beslut blir frågan vad grundar sig detta val på? Enligt Brunsson i Czarniawska, (1998) fattas beslut ofta av irrationalitet och inte av rationalitet.

McFadzean et al., (2007) menar att de två faktorerna, uppfattningen av risk hos ledningen och det strategiska värdet IT har för organisationen, påverkas av följande orsaker: organisationens mål och strategier, den roll säkerhet och informationssäkerhet har, olika variabler i organisationens omgivning och till sist olika lagar och förordningar. Det vill säga den organisatoriska kontexten, informationssäkerhets kontexten, omgivnings kontexten och politiska/legala kontexten.

Eftersom uppfattning av risk och det strategiska värdet av IT kan kopplas till användningen och anpassningen av informationssäkerhetsstrategier och andra verktyg ser jag det som intressant att undersöka, om dessa två faktorer kan svara på frågan, varför prioritering av informationssäkerhet ser ut som den gör enligt MSB:s beskrivning.

Utifrån ovanstående ser jag tre frågor som sammanfattar problemområdet

- Hur spelar ledningens riskmedvetenhet och det strategiska värdet som de lägger på IT in på deras engagemang för informationssäkerhet?
- Utifrån MSB rapporten, handlar problemet om att kommunens ledning inte kan se de IT-relaterade riskerna eller handlar det rent av om att de inte vill se?
- Varför prioriteras informationssäkerhet som den gör?

1.2 Forskningsfråga

- Hur och varför prioriteras informationssäkerhet som den gör i verksamheter?

1.3 Syfte

Jag vill skapa förståelse för faktorer som påverkar beslut och resurstilldelning för utvecklandet av informationssäkerhet inom en organisation. Därför är mitt syfte att undersöka hur och varför informationssäkerhet prioriteras som den gör i verksamheter genom att undersöka hur ledningen uppfattar risk och det strategiska värdet av deras informationssystem.

1.4 Avgränsningar

Jag har valt att begränsa studien till att endast studera kommunala verksamheter eftersom dessa så hårt kritiserades av MSB. Ytterligare begränsning är att endast titta på administrativa beslut som kan tas av organisationen och avgränsa mig från att studera politiska beslut vilket innebär att jag endast studera kommunledningen i form av kommunchef, förvaltningschef och andra högre tjänstemän som samverkar med kommunledningen i säkerhetsfrågor.

1.5 Disposition

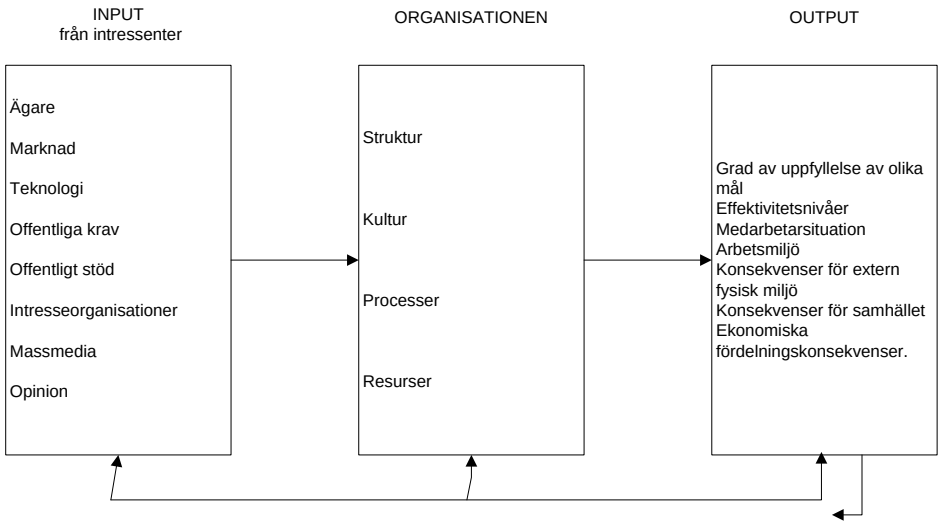
I kapitel 1 ger jag en inledande beskrivning av mitt problemområde där jag motiverar mitt ämnesval. Kapitel 2 består av en genomgång av de teorier som jag anser är mest relevant för mitt uppsatsämne och som avser att beskriva och förklara organisationer som öppna system, organisationen och dess informationssystem, kraven på informationen och riskerna med informationshantering samt faktorer som påverkar ledningens uppfattning av risk och hur detta hur detta påverkar strategiska val. Kapitlet avslutas med att ta upp om ledning och beslutsfattande i en organisation. Kapitel 3 beskriver mitt val av metod för undersökningen och vilka undersökningsobjekt jag har. Kapitel 4 redovisar min empiri och reslutat av undersökningen. Kapitel 5 redovisar min analys och Kapitel 6 omfattar slutsatser och egna kommentarer.

2 Teori

I detta kapitel redogör jag för min teoretiska referensram som innefattar hur organisationer beskrivs, dess informationssystem, informationssäkerhet, risk och riskhantering, kontinuitetsplanering, ledningen och informationssäkerhet och hur kontextuella faktorer påverkar strategiska och operativa insatser. Kapitlet avslutas med teorier om beslutsfattande och en teoretisk syntes.

2.1 Organisationen och omvärlden

En organisation kan definieras på olika sätt Luthans & Stewart, (1976) säger att en organisation är ett socialt system. Churchman, (1968) menar att organisationer är ett system med ett antal delar som har samordnats för att uppnå ett mål och samverkar med sin omgivning för att bilda en helhet Organisationer tar hänsyn till sina intressenter och anpassar sitt beteende efter deras preferenser. Organisationen försöker att finna jämvikt med sin omgivning Schoderbek et al., (1990).



Figur 2.1 Modell för organisationen och omvärlden Bakka et al., (2006).

Enligt ovanstående modell är organisationer öppna system som präglar och präglas av sin omvärld, situationsteorin har sin utgångspunkt eller förutsätter i tre typer av variabler Bakka , Fivesdal och Lindkvist, (2006).

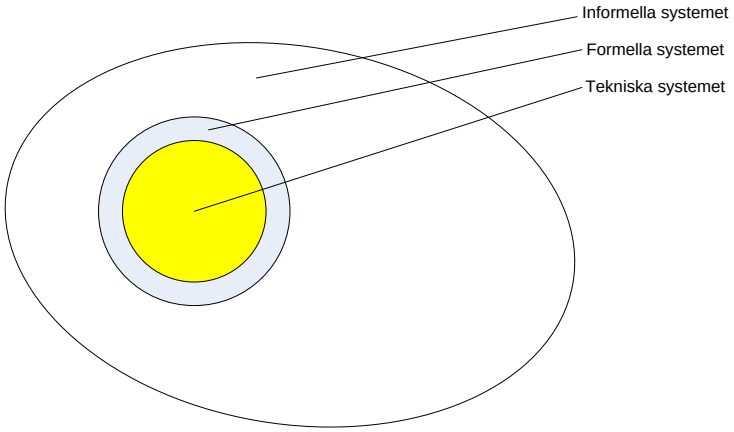
Omvärlden
Mintzberg, (1983) beskriver fyra huvudvariabler som kan användas för analyser av omvärlden. Han är i den betydelsen en situationsteoretiker eftersom han lägger avgörande vikt på hur olika omvärldsfaktorer kommer att påverka organisationsformer och organisationsproblem. Han bortser inte från det komplexa samspelet mellan yttre och inre förhållanden. Organisationer har olika handlingsalternativ som är kopplade till organisationens ålder och storlek, dess teknologiska och strategiska kompetens Bakka et al., (2006).

1. Stabilitet. Omvärlden beskrivs efter dimensionen av stabil-dynamisk, det vill säga hur organisationens omvärld präglas av osäkerhet, oväntade och oberäknade händelser.
2. Komplexitet. Enkel eller komplexa krav som ställs på organisationens expertis och teknologi, klassar organisationens omvärld.
3. Heterogenitet. Denna variabel graderas från homogen till heterogen omvärld och kan användas för att beskriva kunder, produkter och geografiska områden.

4. Fientlighet. En bestämd omvärld kan enligt Mintzberg, (1983) beskrivas efter dimensionen vänlig eller fientlig. Alltså hur omvärlden präglas av konkurrens och konflikter där hög fientlighet genererar osäkerhet för organisationen, denna variabel blir särskilt viktig för organisationens reaktionsförmåga att agera på utmaningar och hot.

2.2 Organisationen och dess informationssystem

Dhillon (2007) menar att en organisation att bestå av tre delar det informella systemet, det formella systemet och det tekniska systemet som ständigt interagerar med varandra. Han liknar dem i med ett stekt ägg(figur 2.2).



Figur 2.2 Det stekta ägget analogin, omarbetad efter Dhillon (2007)

Dhillon (2007) menar att dessa tre system måste koordineras annars resulterar detta till en undermålig skötsel eller öppnar upp organisationen för en rad sårbarheter.

Genom att använda det stekta ägget analogin figur 2.2 så kan koordinationen beskrivas så här, äggulan representeras av det tekniska systemet som hålls på plats av det formella systemet av regler och föreskrifter här representerat som äggulans membran. Det informella systemet representeras här av äggvitan.

Denna analogi visar den underordnande roll det tekniska systemet har i en organisation. Det varnar också för konsekvenserna med att överbyråkratisera det formella systemet och relationen med det informella systemet.

2.2.1 Det informella systemet

Det formella systemet med dess regler och procedurer fungerar inte om människor inte antar och accepterar dem. Att göra så är en social process där människor interagerar med tekniska system och gängse regler samt anpassar sin egen uppfattning för att säkerhetsställa att syftet uppnås. Denna institutionalisering sker genom informell kommunikation där individer och grupper delar och utbyter erfarenheter och skapar mening associerat med deras handlingar. Vanligtvis talar vi att sådana beteende mönster som kultur. Kulturen binder på många sätt samman organisationen. Ur ett säkerhetsperspektiv handlar det om att upprätthålla beteende mönster, värderingar och integritet hos människorna. Åtgärder för att upprätthålla dessa exempelvis genom ökad medvetenhet säger Dhillon är mest kostnadseffektivt(ibid.).

2.2.2 Det formella systemet

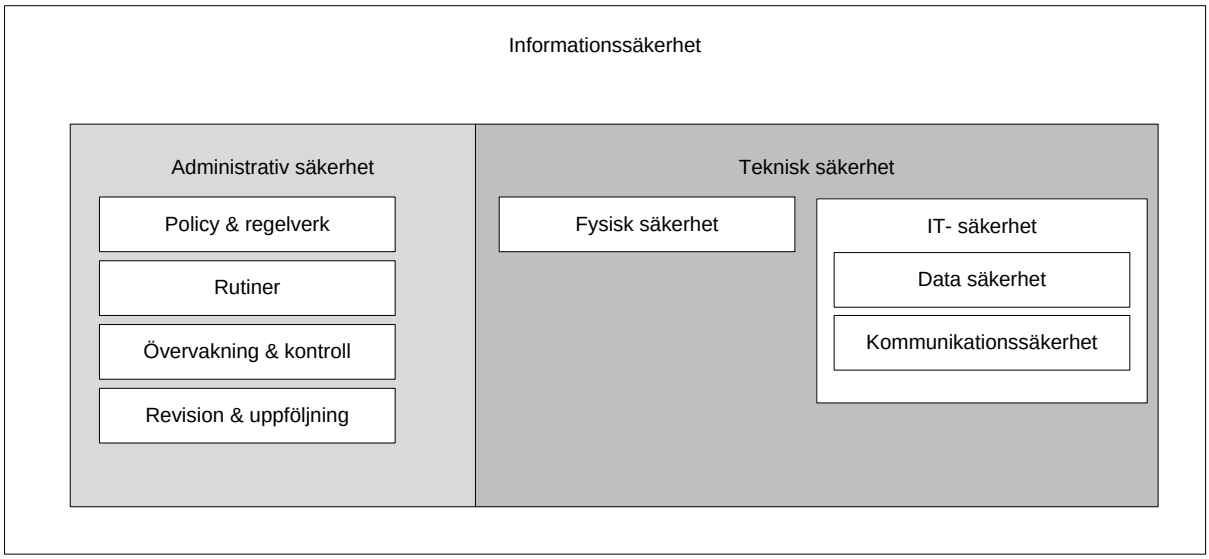
I det formella systemet återfinns organisationens byråkratiska strukturer med regler och procedurer. Ur ett säkerhetsperspektiv handlar det om att skapa organisatoriska strukturer och processer för att kunna garantera en god säkerhet. Det innebär att skapa tydliga strukturer för ansvar och att dessa vidmakthålls, att integriteten för rollerna bibehålls samt att adekvata affärsprocesser skapas och att deras integritet etableras. Utöver detta behövs en övergripande strategi och policy etableras för att se till så att organisationen och dess aktiviteter håller rätt kurs Dhillon (2007).

2.2.3 Det tekniska systemet

Det tekniska systemet automatiserar delar av det formella systemet genom att datorisera rutin aktiviteter.
Ur ett säkerhetsperspektiv handlar det om att säkra hårdvara, mjukvara och data på ett sådant sätt att dessa inte modifieras, förstörs, röjs, avlyssnas, avbryts eller fabriceras genom att använda sig av olika tekniska skyddsåtgärder som exempelvis kryptering.

2.3 Informationssäkerhet och dess beståndsdelar

Informationssäkerhet avser förmågan hos en organisation att kunna upprätthålla en önskad nivå av konfidentialitet, riktighet och tillgänglighet när det gäller hantering av sin information. Begreppet omfattar egentligen hanteringen i alla former, elektronisk, pappers- eller talad form. För min uppsats har hanteringen elektroniskt och pappersform störst vikt med tanke på den kritik som MSB har. Min syn på informationssäkerhet är att den omfattar mer än den tekniska aspekten, som att säkra själva informationssystemet, som exempelvis andra resurser som medlemmarna av organisationen och deras förmåga beskrivs av MSB (2009).
Att beskriva informationssäkerhet som begrepp kan göras på olika sätt det beror på vilket ändamålet är. Jag har valt att använda mig av samma synsätt som beskrivs av *SIS Handbok 550, Terminologi för informationssäkerhet, Utgåva 3*. Där utgångspunkten är den miljö som skyddsåtgärderna återfinns i uppdelade på administrativa skyddsåtgärder och tekniska skyddsåtgärder enligt figur 2.3.



Figur 2.3 Informationssäkerhet utifrån skyddsåtgärderna omarbetad efter SIS HB 550,utgåva 3 (2007)

Att beskriva informationssäkerhet på detta sätt ökar förståelsen för att informationssäkerhet inte kan bedrivas ur endast ett tekniskt perspektiv utan måste kompletteras av administrativa åtgärder i form av policy, regelverk och rutiner för att kunna fungera effektivt . Även om denna uppdelning kan anses allmänt vedertagen så saknar modellen perspektivet på den informella delen av informationssäkerhet som Dhillon (2007) tar upp.

2.3.1 Krav på informationen

Kraven som en organisation har på sin information är kontextspecifikt, det vill säga att det beroende på vilket sätt systemet skall användas så kommer förväntningar på krav som konfidentialitet, riktighet och tillgänglighet att variera. Kravet riktighet är exempelvis högre när gäller elektroniska transaktioner, till exempel banksystem, medan kravet konfidentialitet kan förväntas vara högre i ett militärt system. Däremot kan system som levererar samhällsnyttiginformation som nyheter istället kräva hög tillgänglighet. Autentisering och oavvislighet blir särskilt viktigt för organisationens nätverksmiljö Dhillon, (2007).

Dhillon räknar upp följande olika typer av krav som finns på informationen.

- **Konfidentialitet** – detta krav innebär att information endast är åtkomlig till den som skall ha tillgång till den och att den inte får göras tillgänglig eller avslöjas för obehöriga.
- **Riktighet** – kravet på riktighet syftar på att informationen skall vara tillförlitlig och att samtliga som tar del av den skall kunna lita på den. Det vill säga att informationen inte förändrats vare sig obehörigen, av misstag eller på grund av störningar i systemet.
- **Tillgänglighet** – detta krav innebär att informationen skall vara tillgänglig när helst den behövs och där den behövs. Tillgänglighetskonceptet har ofta jämställts med kontinuitetsplanering och återställning efter katastrof men syftar mer på pålitligheten av data och relaterar till att avsiktligt förhindra tillgång till data eller tjänst.
- **Autenticitet** – kravet på autenticitet blir särskilt viktigt för organisationer som har nätverksbaserade informationssystem. Att veta att ett meddelande verkligen kommer från den avsändare som säger sig vara källa till meddelandet.
- **Oavvislighet** – kravet att informationen går att lita på, att den inte kan förkastas, vilket innebär att användare använder sig av digitala signaturer för att garantera dokuments äkthet och ursprung (ibid.).

2.4 Ledning av informationssäkerhet

För att kunna hantera informationssäkerhetsprocesser är det nödvändigt att förstå några grundprinciper kring management eller ledning av en organisation. I sin enklaste form är management eller ledning, en process att uppnå ett mål med en given uppsättning av resurser. Chefen som är medlem i organisationen är utsedd att vakta och administrera resurser, koordinera fullgörandet av uppgifter och hantera de många roller som är nödvändiga för att uppnå de uppsatta målen. En chef spelar en rad olika roller i en organisation Whitman & Mattord, (2008) och Mintzberg, (1973) identifierar i sin bok ” The nature of managerial work” tio olika roller som en chef utför. Han gör följande indelning av rollerna:

- Informationella roller: Insamling, bearbetning, och användandet av information som rör slutförandet av målet
- Interpersonella roller: Interagerande med överordnade, underordnade, utomstående intressenter och andra parter som påverkar eller påverkas av slutförandet av uppgifterna
- Beslutande roller: Val av alternativa vägar, och lösandet av konflikter, dilemman eller utmaningar.

Mest intressant för mitt arbete är rollerna som beslutsfattare som innefattar rollen som entreprenör, krislösare, resursfördelare och förhandlare. För min uppsats är rollerna krislösare och resursfördelare av störst betydelse och förklaras enligt nedan:

- Krislösare - I denna roll försöker ledaren hantera kriser som inte kan ignoreras indelat på tre typer
    a) Konflikt mellan de anställda.
    b) Konflikt i förhållandet till andra organisationer
    c) Faktisk eller hotande förlust av organisationens resurser
- Resursfördelare – Att fördela resurser är en central ledarskapsfunktion. Kontroll över resurser i form av personal, pengar, tid, material och utrustning ger ledningen kontroll över utveckling av strategi och prioriteringar av vad som ska satsas på. Resursfördelning är en integrerad del av beslut om vad som skall göras, när och hur uppgifterna ska lösas(ibid.).

I sitt dagliga arbete ställs chefer inför att lösa de problem som uppstår kopplat till verksamheten och oavsett om problemet är litet eller stort, följer samma grundläggande process för att kunna lösa problemet Whitman &

Mattord, (2008). Genom att definiera och klargöra problemet, samla in fakta och göra bedömningar, ta fram alternativa lösningar och jämföra dessa för att sedan välja och implementera det bästa alternativet samt sedan utvärdera lösningen så kan problemet avhjälpas(ibid.).

Teorier om beslutsprocesser kommer ursprungligen från normativa teorier om rationellt beteende. Centralt blir då tanken om att individer handlar rationellt eller förnuftigt när individen skall fatta beslut om vad som skall göras när denne ställs inför ett problem March, (1994).

Herbert Simon, (1997) utvecklade en teori om rationellt beslutsfattande kallat ”den ekonomiska människan ” (the economic man). Han använde analyser av marknadsbeteende som grund. Den ekonomiska människan träder in på marknaden fast besluten att få ut det mesta av sina pengar utan att ta någon sentimental hänsyn. Hon vet vad hon vill, hon jämför priser och kvaliteter, hon fattar inte sitt beslut innan hon har full överblick över sina olika alternativ till handling. Men hon blir också nöjd, vilket är en förutsättning för modellen om objektiv rationalitet. Simon, (1997) menar att beslutsfattande enligt ”the economic man” är ett ideal och inte empiriskt möjlig eftersom den förutsätter tre viktiga steg (1) att kunna lista alla alternativ som är möjliga, (2) uppskatta alla konsekvenser som följer med varje tänkbart alternativ,(3) en jämförande utvärdering av dessa konsekvenser. Detta är inte möjligt eftersom människan saknar den kognitiva förmågan att genomföra detta och det skulle ta väldigt lång tid.

Tidsfaktorn påverkar rationaliteten genom att tidspress kan innebära att det inte är möjligt att utvärdera tillräckligt många alternativ och konsekvenserna av dessa. Men det är framförallt förmågan eller kunskapen om att värdera olika alternativ och se konsekvenserna av ett visst agerande som har störst inverkan på hur ett val görs(ibid.).

Eftersom teorin om den ekonomiska människan hade sina begränsningar empiriskt utvecklade Simon en ny modell som byggde på både normativa element och empiriska element som ingår i förutsättningarna för beslutsfattande. Han räknar med två typer av beslutspremisser; empiriska premisser och värderingspremisser. De empiriska premisserna bygger på olika slags kunskap och information om organisationen och dess omvärld och värderingspremisserna innehåller organisationens mål och de olika begränsningar som moral och lagstiftning lägger på olika handlingar.

Denna modell fokuserar på empiriska beteendemönster och Simon kallar den ”the administrative man” vilket är den ofullkomliga empiriska versionen av ”the economic man” Bakka et al., (2006).
Egenskaperna i administrative man till skillnad mot economic man är:

- Den administrativa människan har mål, men de är ofta rätt oklara och skiftande
- Den administrativa människan bedömer vissa möjliga alternativ och vissa konsekvenser av dessa.
- Den administrativa människan bedömer alternativ efterhand som beslutsfattaren har förmåga att behandla dem.
- Den administrativa människan väljer det första tillfredställande alternativet som dyker upp.

Den administrativa människan söker således satisfierande lösningar istället för optimala lösningar Jacobsen & Thorsvik, (1995) och Simon (1997). Den administrativa människan ser till sin omgivning och är inte känslolös i sitt beteende. Teorin om den administrativa människan kan användas för att förstå den begränsade rationalitet som finns i det administrativa beteendet och beslutsfattande som görs av organisationer(ibid.).

För att förstå hur beslut fattas i organisationer är det möjligt att utgå från ovan nämnda administrativa människa där rationalitet är en process där individen värderar olika alternativ och väljer det alternativ som tros vara det bästa för att nå målet.

När människor fattar beslut som medlemmar i en organisation behöver de ta hänsyn till den organisatoriska kontexten för handlandet. March, (1994) beskriver något som han kallar konsekvenslogik och bygger på fyra frågor som en beslutsfattare behöver ställa sig:

1. Frågan om alternativ, vilka handlingar är möjliga?
2. Frågan om förväntningar, vilka konsekvenser i framtiden kan följa med varje alternativ? Hur sannolik är varje enskild konsekvens om ett alternativ väljs?
3. Frågan om preferenser, hur värdefulla är de konsekvenser som kan kopplas till varje alternativ som beslutsfattaren har?
4. Frågan om beslutsregel, hur ska ett val göras mellan alternativen i förhållande till hur värdefulla konsekvenser är för respektive alternativ?

Den organisatoriska kontexten innebär, den position beslutsfattaren har i den formella strukturen, vilka mål organisationen strävar efter att uppnå, vilka regler och procedurer som gäller för arbetet samt de kulturella principer som gäller för organisationen.

Utöver detta behöver beslutsfattaren och beakta något som March, (1994) kallar lämplighetslogik vilket innebär vad som passar sig att göra inom de strukturella och kulturella ramar som organisationen ger. Detta genom att ställa sig tre ytterligare frågor:

1. Frågan om igenkännande, vad för slags situation är det frågan om?
2. Frågan om identitet, vad är jag för slags person? Vilket slags organisation är det här?
3. Frågan om regler, vad gör en person som jag eller organisation som denna i den här situationen?

Dessa två former av logik förekommer sida vid sida i de flesta organisationer och utgör en del av den organisatoriska kontext som medlemmarna i organisationen omfattas av. Detta kommer att påverka deras beslutsbeteende Jacobsen & Thorsvik, (1995).

Dhillon, (2007) pekar på att vid administrativa beslut är viktigt att kunna förstå vidden på strategiska aspekter av informationssäkerhet. Lika viktigt är förståelse för strukturer och processer som krävs för adekvat informationshantering.

Oförmåga att kunna ta fram dessa strukturer och processer kan förklara de flesta säkerhetsöverträdelser som sker. Viktiga beslut som rör strukturer och processer är handlar om att etablera ansvar och auktoritet. Alltså är det viktigt att beslutsfattare har en nödvändig nivå av medvetenhet och kunskap inom informationssäkerhet för att kunna fatta adekvata beslut(ibid.).

Förutom att fatta beslut för att kunna uppnå organisationens mål kräver ledningen av organisationen en del grundläggande färdigheter. Dessa färdigheter åsyftar de karaktärsdrag, funktioner, principer och ansvar som ledningen av en organisation innefattar Whitman & Mattord, (2008)

Dessa kan beskrivas av administrationsteorin som bygger på bland annat på de tankar som Henri Fayols hade om ett företags administration redan i början av 1900-talet Fayol, (1916) . Han identifierade sex funktioner som kan beskriva ett företags verksamhet. Dessa är *teknisk verksamhet* (industriell och hantverksmässig produktion, förädling**),** *kommersiell verksamhet* (inköp, försäljning, handel), *finansiell verksamhet* (anskaffning och förvaltning av kapital), *säkerhetsfrågor* **(**skydd av egendom och anställda), *redovisning* (inventering, bokslut, kostnadsberäkningar, statistik m.m.) och *administration* (planering, organisation, chefskap, samordning och kontroll). Han menar att dessa väsentliga funktioner återfinns i alla företag stora som små oberoende om verksamheten är komplicerad eller enkel. Funktionerna har ett nära samband med varandra. Den tekniska funktionen är beroende av råmaterial, avsättning för sina produkter, kapital, vissa säkerhetsåtgärder och planering (ibid.).

Fayol representerar för mig ursprunget till det som idag benämns som management och omfattar alla typer av organisationer privat som offentlig, produkt- eller tjänsteproducerande, därför är han viktigt i min teoretiska referensram. Av hans sex olika funktioner så är funktionerna *säkerhet* och *administration* de som jag ser som mest viktiga för att gå över till det som idag karaktäriserar ledning av informationssäkerhet. Säkerhetsfunktionen skall skydda organisationens materiella tillgångar och de anställda mot stöld, eldsvåda och översvämning. Den ska förhindra attentat, strejker och allt annat som stör ordningen och hotar organisationens utveckling eller rentav dess överlevnad. Här ingår också allt som bidrar att göra organisation säker och ger dess anställda nödvändig känsla av trygghet (ibid.).

Fayol beskriver administration så det innebär att *planera***,** *organisera*, *utöva chefskap*, *samordna* och *kontrollera.* Där *planera* innebär att utforska framtiden och utforma en verksamhetsplan. *Organisera* innebär att bygga upp

företaget materiellt och socialt. *Utöva chefskap* innebär att motivera de anställda så att arbetet blir utfört och samarbetet fungerar. S*amordna* innebär att länka samman och harmonisera skilda ambitioner och åtgärder. K*ontrollera* innebär att se till att allt som händer överensstämmer med fastställda regler och utfärdade direktiv. Administrationen är den enda funktionen som ansvarar för att, planera för verksamheten, skapa en organisation, samordna inriktning och vidta åtgärder(ibid.).

Den moderna synen på administration eller management innebär att de fem funktionerna är sammansatt till fyra *planera, organisera, leda och kontrollera* Whitman & Mattord, (2008).

Principerna för ledning av informationssäkerhet påminner mycket om de generella principerna för management, när det gäller ledarskap, men de övergripande målen och de kortsiktiga målen skiljer sig åt mellan dem inom IT och övrig företagsledning. Detta framförallt då fokus läggs på att säkra upp verksamheten, ledning av informationssäkerhet får då ett annorlunda utseende och baseras på följande funktioner (ibid.).

Planering . Som en förlängning av den grundläggande planering av affärsstrategi som sedan överförs till en IT-strategi består denna del av att omarbeta IT-strategin till planer för incident och kontinuitetsplanering, planer för riskhantering, policyplanering samt planering för säkerhetsprogram i form av utbildning, träning och ökad medvetenhet. Varje plan har sina unika målsättningar och alla tjänar på samma organiserade och metodiska ansats.
Policy. Denna funktion innebär att utveckla policys och riktlinjer utifrån IT – strategin på olika nivåer alltifrån övergripande nivå till en mer detaljerad systemnivå.
Program. Denna funktion handlar om olika fristående program som bedrivs inom informationssäkerhet och vara utbildningsprogram eller program som rör fysisk säkerhet.
Skydd . Skyddsfunktionen innefattar aktiviteter som riskhantering men också skyddsåtgärder, tekniker och verktyg som återspeglas in den övergipande säkerhetsplanen.
Personal . Personal är den vikigaste länken och denna funktion behandlar rollen som människor spelar inom säkerhetsprogrammet såväl säkerhetspersonal som övrig personal.
Projektledning. Denna funktion handlar om att informationssäkerhetsarbetet ofta bedrivs i projektform oavsett om det handlar om att introducera ett nytt utbildningspaket för hela organisationen eller en teknisk skyddsåtgärd eller policy (ibid.).

Haverblad, (2006) säger att det krävs en medvetenhet av IT-relaterade risker hos alla inom organisationen. På alla nivåer inom organisationen är det nödvändigt att ha en förståelse för riskerna. Speciellt på ledningsnivå eftersom det är ledningsgruppen som skall fatta beslut om verksamhetens tolerans av risk.

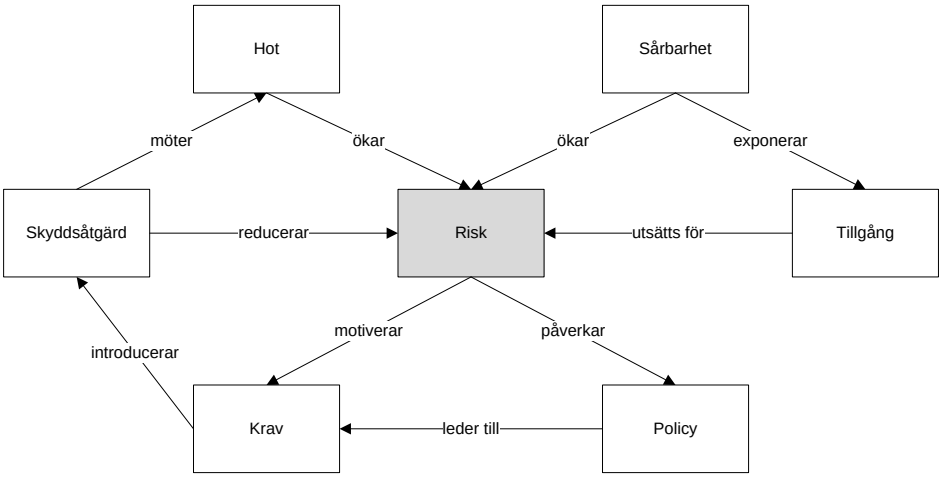
2.5 Problem relaterade till ledningen av informationssäkerhet

När det kommer problem med ledningen av informationssäkerhet pekar von Solms & von Solms, (2004) listar tio dödssynder ledningen kan begå när det gäller att implementera informationssäkerhet i organisationen och bygger på de olika dimensionerna av informationssäkerhet men det kan delas in i fyra olika klasser Dhillon, (2007):
Säkerhetsstrategi och policy- utvecklingen av strategi och policy som fastställer det sätt som administrativa aspekter av informationssäkerhet sköts.
Ansvars- och auktoritetsstrukturer - definition av organisatoriska strukturer och hur medarbetare skall anmäla till sina överordnade. Sådana definitioner hjälper till att etablera åtkomstregler för system.
Affärsprocesser- att definiera det formella informationsflödet i organisationen, detta måste matcha affärsprocesserna för att kunna tillgodose verksamhetens integritet.
Roller och färdigheter - identifiering av nyckelpersoner och att kunna behålla dessa i organisationen är lika viktigt som att definiera säkerhetspolicyn, strukturer och processer (ibid.).

2.6 Risk och informationssystem

” If you know the enemy and know yourself, you need not fear the result of a hundred battles. If know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”
Sun Tzu, The art of war referrers i Withman & Mattord, (2005)

Denna insikt av den kinesiske generalen för över 2400 år sedan fångar enligt min mening essensen av vad riskhantering handlar om. Gerber & Von Solms, (2004) menar att risk existerar på grund av kombinationen hot, sårbarheter och tillgångars värde. En sårbarhet som utgör en svaghet i säkerhetssystemet kan utnyttjas för att skapa förlust av eller skada på tillgången/tillgångarna och hotet är källan eller omständigheten som har potential att orsaka förlusten eller skadan. Det komplexa samband som omfattar risk kan illustreras av figur 2.4



Figur 2.4 komplexa sambandet mellan de olika modulerna i en riskhanteringsprocess. Omarbetad efter SIS HB 550 Utgåva 3 (2007).

I min litteraturstudie har jag funnit ett flertal olika indelningar av och benämningar på processen att hantera risk men de gemensamma dragen är att riskhantering handlar om att först identifiera hot mot och sårbarheter i sina informationstillgångar och sedan bedöma sannolikheten och effekten av att hotet skulle realiseras. Resultatet blir ett ställningstagande och ett val av strategi för att antingen acceptera, minimera eller helt undanröja risken med hjälp av olika skyddsåtgärder såväl tekniska som administrativa. En reflektion jag gör är att initiativet för att genomföra en riskhanteringsprocess kan komma från två håll. Uppifrån i organisationen genom ett helhetsperspektiv, som vid förändringar av krav i affärsprocesser, eller underifrån när nya hot och risker upptäcks.

Gerber & Von Solms, (2004) använder en definition av riskanalys som summan av riskidentifiering, bedömning och utvärdering. Haverblad, (2006) säger att vid riskanalys identifieras hot och sårbarheter som därmed utgör potentiella risker. Riskanalys handlar om att förstå risker, hur de kan uppstå, hur de påverkar och de konsekvenser som dessa har för kärnverksamheten.

2.6.1 Riskhantering

Jag har valt att utgå från den indelning som Dhillon (2007) gör avseende riskhantering. Riskhantering avseende säkerhet hos IT-system, är enligt honom en process som hjälper organisationer att balansera funktionsbehov och ekonomiska kostnader förenade med IT-baserade system. Syftet med riskhantering är att möjliggöra att organisationen kan fortsätta hantera sin information på ett adekvat sätt. Själva processen med riskhantering omfattar tre delar; *riskbedömning*, *riskreducering* och *riskutvärdering*.

2.6.2 Riskbedömning

Riskbedömningsprocessen innebär att identifiera och bedöma risker samt deras påverkan på organisationens informationstillgångar. Processen omfattar prioritering, implementering och upprätthållandet av en acceptabel risknivå. Vid riskbedömning genomlyses hela systemutvecklingsprocessen för att finna potentiella hot, resultatet är att lämpliga kontroller för att minimera risk kan identifieras Dhillon, (2007). Vid riskbedömning utgår bedömaren ifrån att risk, är en funktion av sannolikheten av ett givet hot resulterar i en sårbarhet. En sådan sårbarhet kan få negativa konsekvenser för organisationen.

För att kunna bestämma sannolikheten av framtida negativa händelser bedöms, hoten, sårbarheterna, och kontrollerna i kombination med varandra. Samspelet mellan hot, sårbarhet och kontroll är den påverkan en negativ händelse kan ha(ibid.).

Detta hjälper till att rekommendera strategier för riskreducering. Riskutvärdering hanterar den kontinuerliga utvecklingen av riskhanteringsprocessen så att en framgångsrik riskhantering uppnås.

2.6.3 Riskreducering

Riskreducering involverar prioritering, värdering och implementering lämpliga kontroller. Riskreducering tillsammans med en sund intern riskkontrollsprocess är livsnödvändig för vilken organisation som helst. Riskkontroll innefattar hela kedjan av policy, procedurer och system som en institution behöver för att kunna hantera alla risker i sin verksamhet. Viktigt här är att undvika intressekonflikter och att själva riskkontrollen har en oberoende ställning gentemot affärsenheter och liknande Dhillon, (2007). Underlåtenhet att inse vikten av riskreducering och riskkontroll resulterar bland annat i:

- Bristande förmåga hos ledningen att hantera tillsyn och ansvar
- Otillräcklig bedömning av risken
- Otillräcklig kommunikation av information mellan ledningsnivåerna inom organisationen, speciellt kommunikationen uppåt gällande problem.
- Otillräcklig eller ineffektiva revisionsprogram och övervakning.

När det gäller riskreducering och identifieringen av kontroller finns en rad olika valmöjligheter att beakta.
Gör ingenting – här accepteras risken och beslut tas att inget göra åt risken.
Undvik risken – risken är känd och strategin för att undvika risken blir att överge en viss funktion i systemet eller att systemet stängs ned.
Förebygg risken - effekten av risken begränsas genom att använda någon form av kontroll för att minimera den negativa effekten av risken.
Risk planering – här tas en riskplan fram för att reducera risken genom att prioritera, implementera och upprätthålla en uppsättning av kontroller.
Erkännande av risk – här erkänner organisationen att sårbarheten finns och undersöker hur den skall hanteras och vidta korrektiva åtgärder.
Riskförsäkring- organisationen införskaffar ett försäkringsskydd och överför därmed risken på någon annan.

Implementeringen av kontroller sker i olika steg utifrån de identifierade riskerna i riskbedömningsfasen. De risker som anses oacceptabla hanteras först. Kontroller implementeras sedan utifrån deras effektivitet och genomförbarhet. Kontrollernas kostnadsfördelar bedöms också innan kombinationen av formella, informella och tekniska skyddsåtgärder bestäms(ibid.).

2.6.4 Kontinuitetsplanering

Enlig Dhillon, (2007) är kontinuitetsplanering en typ av formell kontrollfunktion. Kontinuitetsplanering är del av riskreducering som innebär att organisationen är förberedd och kan förutse, reagera på och återhämta sig från händelser som hotar säkerheten av information och organisationens informationstillgångar samt därefter kunna återställa organisationen till ett normalläge Whitman & Mattord, (2007).

Haverblad, (2006) kopplar ihop IT-verksamheten och kontinuitetsplanering genom att beskriva kontinuitetsplan för IT. Syftet med en kontinuitetsplan för IT är att kärnverksamheten skall påverkas så lite som möjligt och ekonomiska förluster minimeras, om en allvarlig störning eller incident skulle ske, genom att ha rutiner för att kunna hantera en allvarlig störning. Om det finns kritiska IT-tjänster för verksamheten är det också kritiskt att det finns en kontinuitetsplan för dessa. Kontinuitetsplanen för IT är en del av den övergripande kontinuitetsplanen som bör finnas för hela organisationen. Planen beskriver organisation, ledning och vilka som måste kontaktas och informeras. Den skall också bland annat innehålla beskrivning av manuella reservrutiner där det är möjligt att använda sådana och vad som krävs för dessa skall fungera.

All den information som krävs för att kunna återskapa och återstarta tjänster måste finnas med i planen. Planen skall också innehålla planer för olika tänkbara scenarier som kan uppstå samt planer för att avhjälpa avbrott och återstart för respektive scenario enligt Whitman & Mattord, (2007).

2.7 Ledningens uppfattning av risk och dess strategiska påverkan av IT ur ett informationssäkerhetsperspektiv.

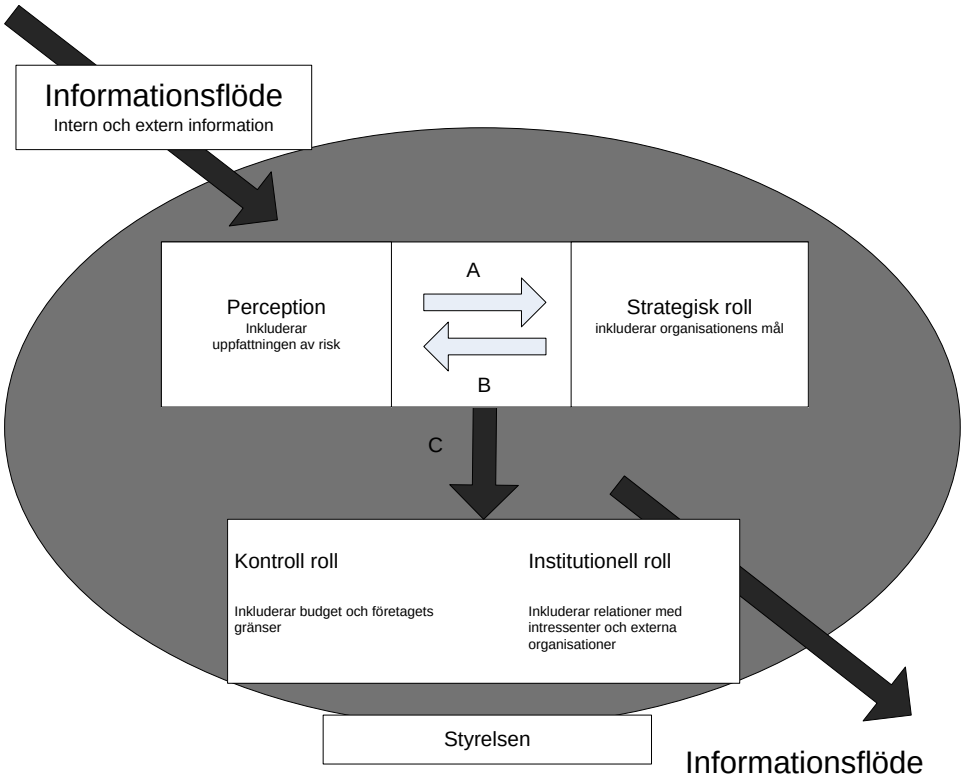
För att kunna förstå hur högre chefer i organisationers ledning uppfattar risk har jag utgått från McFadzean et al.,(2007)studie ”*Perception of risk and the strategic impact of existing IT on information security strategy at board level”.* Denna studie är uppbyggd på flera av de tyngsta namnen inom ledning av informationssäkerhet och risker. Studien visar att företagsledningens engagemang för informationssäkerhet var starkt beroende på två faktorer, uppfattningen om risk och IT:s strategiska värde för organisationen. Även om studien utgår från styrelsen i företag anser jag att studien ändå kan användas i min teoretiska referensram eftersom det dock finns likheter i rollerna oavsett om ledningen finns i företag eller i en offentlig organisation. Eftersom studien är väldigt omfattande och bygger på McFadzean et al., (2007) utgår från de roller och ansvar styrelsemedlemmar har i ett företag och hur de påverkar informationssäkerheten (se figur 2.5).

De utgick från tre roller som ledningen har:

Strategiska rollen. Denna inkluderar att bestämma parametrar för organisationens aktiviteter och att gå igenom förslag för strategiska och operationella mål.

Kontroll rollen. Denna innebär att se till att anpassa ledningens åtgärder med delägarnas intresse men även att utvärdera budget och planer, övervaka omgivningen och benchmarka mot konkurrenterna. Ur min synvinkel kan liknande aktiviteter även ske i offentliga organisationer.

Institutionella rollen, Denna omfattar införskaffandet av kritiska resurser, bygga relationer med sina intressenter och medla mellan interna och externa koalitioner.



Figur 2.5 De olika rollerna McFadzean et al., (2007)

Modellen kan förklaras enligt följande: information införskaffas av ledningen från både interna och externa källor, varje chef uppfattar informationen på olika sätt. Detta inkluderar deras uppfattning om risk, vilket kommer att ha en påverkan styrelsens strategiska roll (pil A). Till exempel, besluten som tas under ett screening förfarande för strategiska och operationella mål kommer att influeras av deras uppfattning av risk. Ju högre risk desto större nödvändighet för striktare säkerhetskontroller.

På samma sätt kommer organisationens intentioner att ha en påverkan på riskuppfattningen (pil B). Chefer vars organisation använder informationssystem som ett strategiskt vapen kommer att se risk på ett annat sätt än de som använder informationssystem för sina operativa behov. Chefers uppfattning om risk och deras strategiska roll inom styrelsen kommer att påverka deras kontroll och institutionella roll (pil C). Budget och styrnings beaktanden kommer att vara beroende på risknivån och organisationens mål. Ett företag som använder sitt informationssystem som ett konkurrensmedel i en riskfylld miljö kommer exempelvis att spendera mer pengar på säkerhet än ett företag som använder sitt informationssystem för sina operativa behov i en lågrisk miljö. Dessutom kommer intressenter som aktieägare att kräva striktare ansvar av chefer, speciellt när det gäller finansiella, styrnings och säkerhetsrutiner.

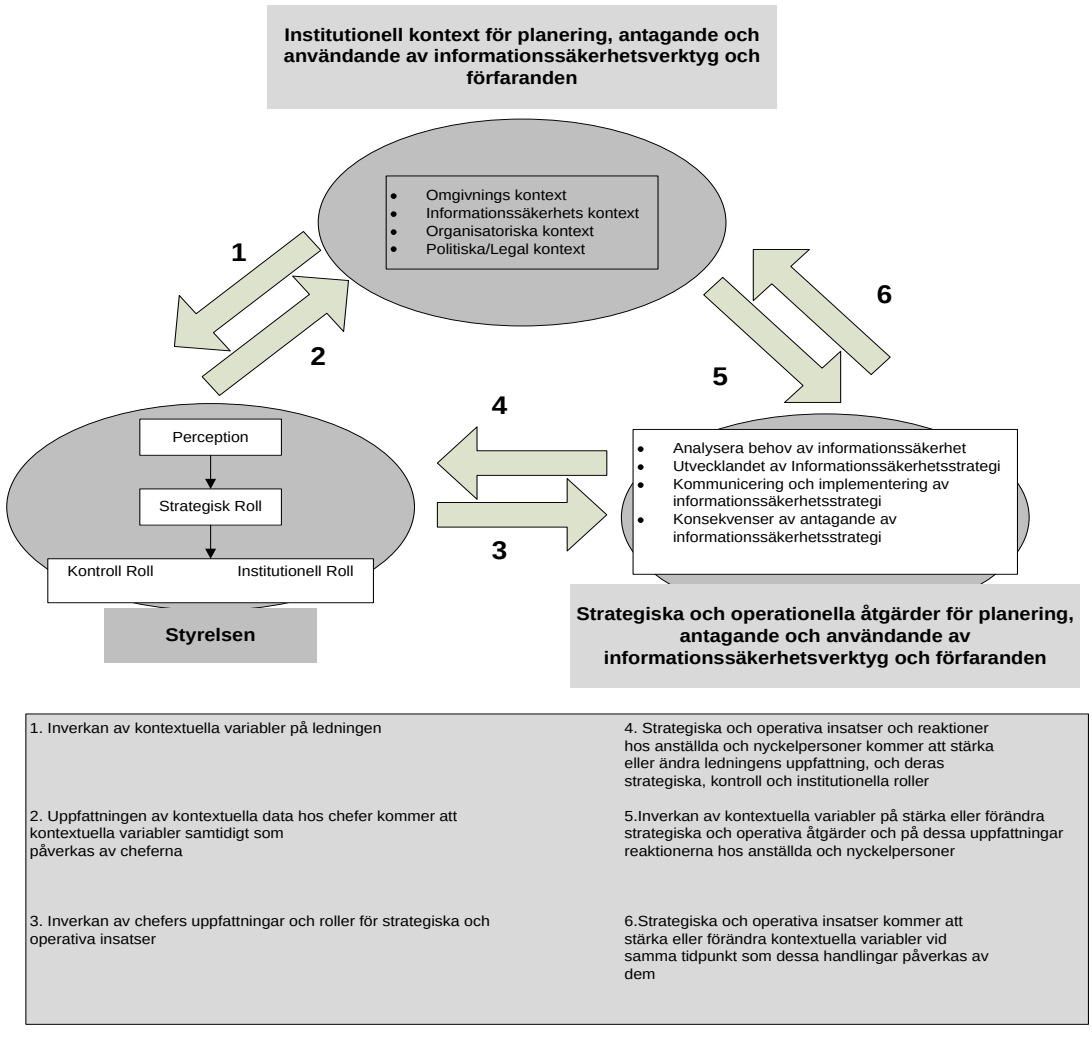
2.7.1 Organisationens kontextuella faktorer

Organisationens kontextuella faktorer fann McFadzen et al., (2007) inkludera både interna och externa variabler se figur 2.6. Dessa omfattade frågor som lagar och föreskrifter, externa och interna hot såsom stöld, åtkomst attacker(denial of service), virus och dataförlust, organisationskulturen samt den ställning information och säkerhetssystem har inom organisationen. Dessa faktorer hade en direkt påverkan på styrelsens uppfattning om

risk (pil 1). Under tiden chefer utvärderar och tolkar de kontextuella faktorerna kan de oavsiktligt påverka deras egen omgivning (pil 2). Till exempel att påvisa behovet av striktare säkerhetsåtgärder kan göra att ledningen oavsiktligt uppmuntrar en förändring av kulturen, vilket leder till en mindre pålitlig och öppen miljö. Som diskuterats ovan fann McFadzean et al., (2007) att styrelsen intar tre olika roller, den strategiska rollen, den kontrollerande rollen och den institutionella rollen. Deras resultat visar på att toppledningens uppfattning av risk har en direkt inverkan på dessa roller. Dessutom påverkade både, deras riskuppfattning och deras styrelseroller, de strategiska och operationella insatserna hos deras underställda (pil 3).

På samma sätt påverkas dessa insatser chefer genom att forma deras uppfattning av risk och deras beslut angående informationssäkerhet (pil 4).

Strategiska och operationella insatser som planering, antagandet och användandet av informationssäkerhetsverktyg och förfaranden, kommer också att influeras av organisationens kontextuella faktorer (pil 5). Till exempel säkerhetssystem kan behöva ändras om nya och oväntade hot uppstår mot organisationen. På samma sätt kan styrelsen och anställda när de genomför dessa strategiska och operativa åtgärder ofta påverka sin egen omgivning. Till exempel en förändring av kulturen eller kunders förväntningar på säkerhet eller varierande feedback (pil 6).



Figur 2.6 Organisationens kontextuella faktorer omarbetad enligt McFadzean et al., (2007).

Den institutionella kontexten

McFadzean et al., (2007) fann att det fanns fyra avgörande kontextuella variabler som påverkade uppfattningen av risk och informationssäkerhet.

Omgivningskontexten det vill säga variabler som inkluderar de externa faktorer som kan ha påverkan på organisationens informationssystem och säkerhet. Organisationens intressenter som kunder och aktieägare kan påverka de parametrar som styrelsen satte för säkerheten.

Informationssäkerhetskontexten det vill säga interna och externa hot, den befintliga rollen säkerhet har inom organisationen, existerande informationssäkerhetsinfrastrukturer och processer, informationssäkerhetspolicys och rutiner, teknik, befintlig säkerhetspersonal samt existerande övervakning, kontroll och återkopplingsmekanismer. Risken för interna och externa hot spelade exempelvis en stor roll för beslutsfattande runt säkerhet inom organisationen. Utöver detta fann författarna att utvecklingen och implementering av säkerhet sågs som en iterativ och dynamisk process, på grund av omgivningens föränderliga natur.

Organisatoriska kontexten, omfattar organisationens mål och strategier, färdigheter och kunskap, kultur och förtroende, struktur och anställdas utbildning. Det visade sig att organisationens mål och strategier hade stor inverkan på informationssäkerhet. Till exempel kommer organisationer med innovationskultur och informationsdelning att utveckla en annan informationssäkerhets procedurer än de organisationer som inte är beroende av informationsdelning.

Politiska/legala kontexten, studien fann att fyra starka politisk/legala faktorer som påverkade utvecklingen av säkerhet. Dessa är riktlinjer, regel efterlevnad (compliance), försäkring och säkerhetsstandards. Enligt respondenterna släpade många företag efter när det gällde processer som gjorde att de uppfyllde regel efterlevnad (compliance) och lagkrav medan andra fann att riktlinjer var användbara för att strukturera och hantera interna risker. Några respondenter hade upptäckt att försäkringsbolag numer drog sig för att försäkra vad som de såg som stora risker.

2.7.2 Strategiska och operativa insatser

McFazean et al., (2007) fann att som respons på förändringar i omgivningen och den strategiska kontrollen analyserade ledningen behoven av informationssäkerhet, utvecklade en informationssäkerhetsstrategi kommunicerade och implementerade konsekvenserna av strategin i olika steg.

Analys av informationssäkerhetsbehoven (se figur 2.6)
Det visade sig att det var fem viktiga områden som inkluderades i analysen av behoven för informationssäkerhet och de är:

- Risk analys, utvecklingen av ramar för riskhantering och genomgång av säkerhetsrevisioner.
- Värdet av verksamheten och säkerhetsmålen. Vikten av att länka informationssäkerhet med organisationens mål.
- Teknik, behovet av teknisk expertis i form av interna eller externa IT specialister
- Säkerhetsstandard som inkluderade riktlinjer och säkerhetsstandards och regel efterlevnad(compliance)
- Intressenter, både anställda och kunder sågs som potentiella hot för organisationens säkerhet.

Utveckla en informationssäkerhetsstrategi (se figur 2.6)
McFadzean et.al., (2007) fann en rad av faktorer som beaktades vid utvecklingen av en informationssäkerhetsstrategi.

- *Interna frågor*. Dessa inkluderade komplexiteten i själva interaktionen människa och teknik, komplexiteten i säkerhetsrutinerna och distributionen och delningen av information, användarvänligheten och effektivitet, medarbetarnas tillfredställelse, egenmakt och förtroende, insourcing kontra outsourcing, övervakning och kontroll system samt kvaliteten.
- *Finansiella frågor*. Fastän detta är en viktigt att beakta vid utvecklingen av säkerhet, så fann författarna att kostnaden ofta doldes inom IT budgeten och därför hade högsta ledningen ingen kännedom om hur mycket organisationen satsades på säkerhet årligen. Detta stämde också in på de organisationer som såg informationssäkerhet som en investering istället för en kostnad.
- *Kontinuitets- och backup planer*. Dessa ansågs inkludera: test av kontinuitetsplanen under realistiska former, design av säkerhetsprocedurer för att garanter personal redundans, backup av data på off-site ställe; etablering av roller och ansvar i händelse av en katastrof skulle inträffa; skapandet av interna och

externa kommunikationslinjer i händelse av ett stort hot eller katastrof; och säkerställandet av återställnings- och backup system är tillgängliga för organisationens kritiska system.

- *Innovation, lärande och tillväxt*. Kreativitet och innovation sågs viktig drivkraft för några av organisationernas verksamheter. Det fanns en oro hos några chefer att sträng säkerhet skulle förhindra informationsdelning och således nya idéer. Utöver detta fann författarna att de flesta organisationer satte upp säkerhetsträning och medvetenhetsprogram.
- *Intressenter*. I många fall kan organisationens kunder och leverantörer påverka organisationens nivå av säkerhet. Generellt krävde intressenterna robusta säkerhetssystem men att detta var tvunget att balanseras med användarvänlighet.

Kommunicering och implementering av säkerhetsstrategi (se figur 2.6)
McFadzean et.al., (2007) fann en rad av frågor som var involverade med kommunikationen och implementeringen av informationssäkerhetsstrategin och dessa var:

Verksamhetsprocesser. Koordineringen mellan verksamhets och säkerhets åtgärder var viktiga under implementeringsfasen. VD för en finansiell organisation föreslog att det är en balans mellan tekniska frågor och ledningsfrågor. Beslut måste handla om ”rättigheter och skyldigheter hos anställda som ska jobbar med säkerhets- och verksamhetsprocesser.

Medarbetarna. Informationssäkerhetsprocesser måste vara accepterade av medarbetare för att bli effektiva. Detta kan uppnås genom utbildnings- och medvetenhetsprogram, utveckling av policydokument och praktiserandet av åtgärder för att upprätthålla kontinuitet.

System och teknologi. Teknik används ofta för att tvinga medarbetare att undergå de nödvändiga säkerhetsprotokollen. Till exempel, smartcards kan vara den enda möjligheten för att kunna ta sig in i en byggnad. Följaktligen, måste varje medarbetare göras uppmärksam på sina befogenheter och ansvar genom de protokoll och förfaranden som införs.

Utbildning och medvetenhet. Många organisationer som vidtalades hade någon form av säkerhetsutbildning för sina anställda. Utöver detta ansågs kommunikation och medvetenhet vara viktiga.

Kontinuitetsprocesser. Många organisationer som författarna intervjuade hade implementerat kontinuitets- och backup processer. Men de sträckte sig alltifrån enkla kontinuitetsplaner för enkla intrång till sofistikerade planer med rollspel av ett katastrofscenarios.

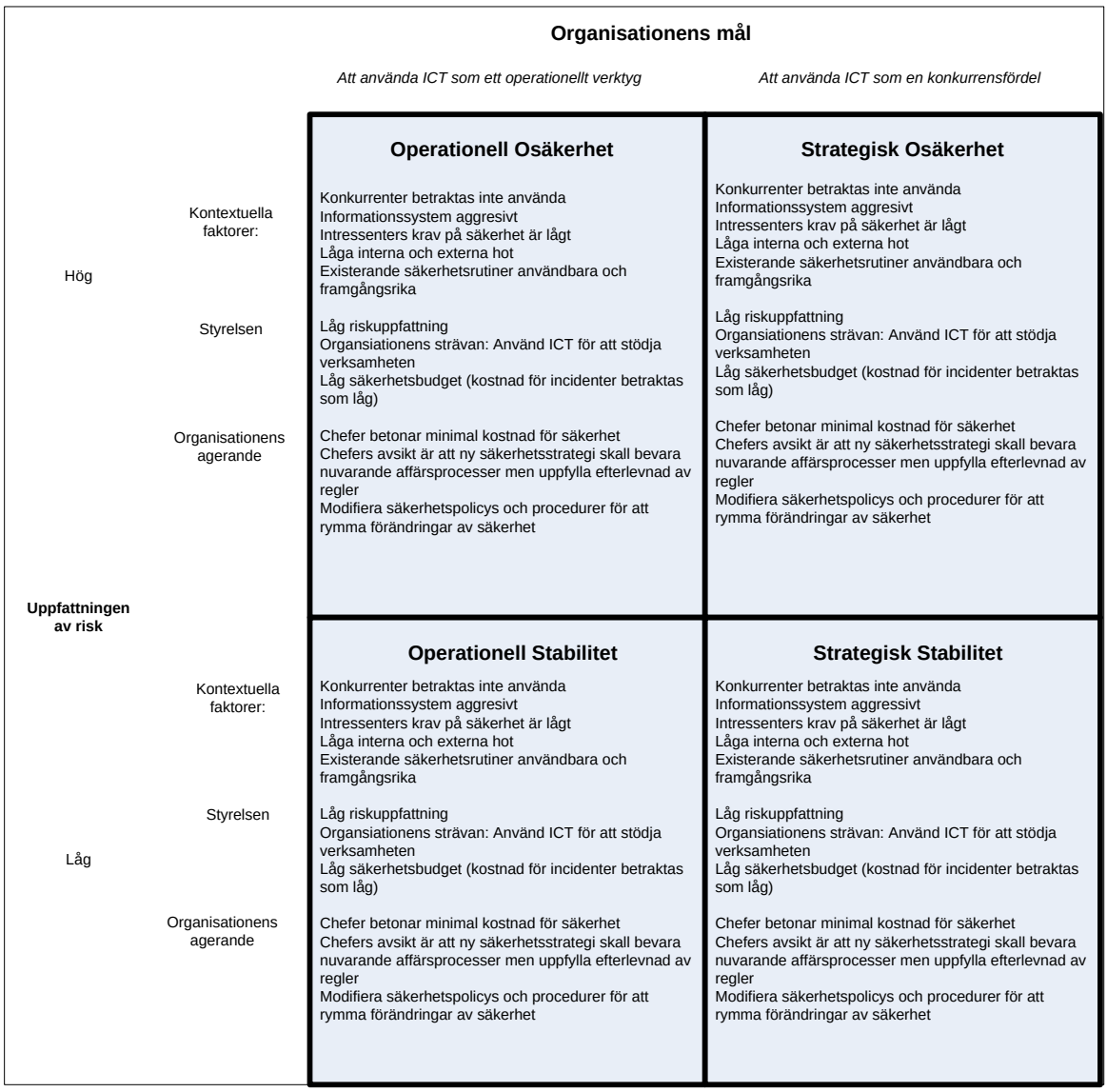
Utvärdering av konsekvenser av att anta informationssäkerhetsstrategi (se figur 2.6)
Åter fann McFadzean et al., (2007) en rad av potentiella konsekvenser av att anta en informationssäkerhetsstrategi. Strategin påverkade både interna och externa faktorer. På grund av den föränderliga naturen hos omgivningen, utvecklades planeringsprocessen, antagande av och implementering av informationssäkerhetsverktyg och förfaranden konstant. En respondent svarade att det var en ständig kamp att hålla ribban på säkerheten så pass hög att hackers och andra skulle anse att det var för kostsamt att attackera organisationen.

2.7.3 Riskmatrisen

Enligt McFadzean et al., (2007) tyder det mesta på att en spridning på riskuppfattning existerar hos högre chefer och styrelsemedlemmar. Några ser en överträdelse av säkerhet som en försumbar risk och om den skulle inträffa skulle det inte få ödesdigra följder. Å andra sidan finns det många chefer som kontinuerligt undersöker deras organisation efter luckor i deras skydd.

Det fanns också olikheter hur organisationer använde sina informationssystem. Det fanns skillnader på hur strategiskt viktigt informationssystemet var för organisationen. Och många i studien använde sina informationssystem i strategiskt syfte, för att stödja sina affärsprocesser, på ett sådant sätt så att det slutligen gav konkurrensfördelar. Utöver detta lyckades dessa företag att skapa innovativa nya produkter, utveckla kreativa nya processer och system samt nyttig uppfinningsrik strategi för framtiden (ibid.).

McFadzean et al., (2007) har skapat en matris indelat i fyra kvadranter för att illustrera förhållandet mellan den strategiska vikten av IT och riskuppfattningen hos ledningen enligt figur 2.7



Figur 2.7 Riskuppfattnings matrisen McFadzean et al., (2007).

Den horisontala axeln syftar på den strategiska vikten av befintligt informationssystem på grund av att detta kan ha inflytande på beslutsprocessen för informationssäkerhet. Till exempel ett företag som ser sig som i frontlinjen för internetförsäljning. Denna aspekt av deras verksamhet är viktigt och avgörande del av organisationen. Därmed skulle denna policy ha en avsevärd påverkan på organisationens informationssäkerhets strategi McFadzean et al., (2007). Med andra ord kan sådana organisationer behöva inta en ledande roll vad gäller dess säkerhetsmedvetenhet och processer för att upprätthålla ryktet och förtroendet hos sina kunder.
Den vertikala axeln syftar på uppfattning av risk. Ledningens uppfattning av risk kommer att påverka deras egna roller och handlingar inklusive utveckling av organisationens informationssäkerhetsstrategi (ibid.).

Operationell stabilitet (se figur 2.7)
I denna kvadrant är både uppfattning av risk och den strategiska vikten av befintligt informationssystem låg. Organisationer i denna kvadrant använder inte sina informationssystem och teknik som ett strategiskt verktyg. Istället används de för att förbättra effektiviteten i verksamheten och administrationen. Förutom det kan tekniken användas för att upprätthålla existerande affärsverksamhet för att undvika nackdelar gentemot deras konkurrenter McFadzean et al., (2007).
I denna kvadrant görs IT investeringar på applikationer som stödjer verksamhetsprocesser.

Uppfattningen av risk hos ledningen och andra intressenter är låg I denna kvadrant. Vilket resulterar i lägre budget för informationssäkerhet och följaktligen kommer informationssäkerheten som introduceras i denna organisation att se till att regler efterlevs och lagkravföljs samt att verksamhetsprocesser stöds. Dessa verksamhetsprocesser kommer sällan att ändras så att de tillgodoser säkerheten. Istället implementeras tekniska skyddsåtgärder som brandväggar och antivirusskydd för att tillgodose regel efterlevnad (compliance). Informationssäkerhetsprocessen kan modifieras men kommer aldrig genomgå radikala förändringar.

Strategisk stabilitet (se figur 2.7)
I denna kvadrant uppfattas risk som låg men den strategiska vikten av befintligt informationssystem är hög. Här är de tekniska applikationerna inom organisationen kritisk, för framtida framgång, för verksamheten. De stödjer befintliga processer och skapar nya processer för att hjälpa organisationen att nå konkurrens fördelar. Utöver detta kan några av dessa företag ha innovativa och nya applikationer eller processer som i framtiden kan ge organisationen en fortsatt konkurrens fördel. Investeringar inom IT och informationssäkerhet utgår från de applikationer som är kritiska för att kunna upprätthålla både nuvarande framtida affärsstrategi.

Precis som med operationell stabilitet figur 2.7 så uppfattas risk som låg av ledningen och andra intressenter vilket resulterar i en mindre budget för informationssäkerhet. Därmed tenderar regel efterlevnad att garanteras av användandet av teknik istället för förändring av affärsprocesser.

Operationell osäkerhet (se figur 2.7)
I denna kvadrant är uppfattningen av risk högre men den strategiska vikten av nuvarande informationssystem låg se figur 2.7. Precis som i operationell stabilitet använder organisationer i denna kvadrant deras teknik för att förbättra effektiviteten i verksamheten och administrationen såväl som att stödja existerande processer som verksamheten är beroende av.

Som reslutat av den högre riskuppfattningen kan ledningen höja budgeten för informationssäkerhet. Utöver detta kan förändringar av säkerheten ske inom organisationen genom att använda informationssäkerhetsteknik likväl som att modifiera processer för att garantera säkerhet och regel efterlevnad.

Strategisk osäkerhet (se figur 2.7)
I denna kvadrant är både riskuppfattningen och den strategiska vikten av nuvarande informationssystem höga. Som i strategisk stabilitet är de tekniska applikationerna inom dessa organisationer kritiska, för befintliga och framtida framgång, och för att kunna förse organisationen med en konkurrens fördel. Dessa skulle kunna vara internetföretag, de förlitar sig nästan helt på informationsteknologi för att kunna genomföra sin fundamentala verksamhet som att köpa och sälja varor och tjänster. När informationsteknologin går fel i dessa företag kan det ha allvarliga konsekvenser. Som ett reslutat av den höga riskuppfattningen kommer ledningen och andra intressenter ge en hög informationssäkerhetsbudget. Utöver detta görs förändringar inom organisationen genom att använda informationssäkerhetsteknik likväl som radikalt förändra processer för att garantera säkerhet och regel efterlevnad. Följaktligen förändras förfaringssätt och säkerhetsteknik implementeras för att garantera en miljö som är så trygg och säker som bara är möjligt McFadzen et al., (2007) .

2.8 Min teoretiska syntes

Med min teoretiska syntes avser att förklara och belysa mitt val av ovan redovisade teorier. Det är för att kunna visa relevansen och skapa en naturlig koppling för läsaren till empiri, analys och slutsatser.
Genom att utgå från systemteori och synen på organisationer som öppna system samt hur de påverkas och påverkar sin omvärld, där situationsteorin säger att organisationen måste anpassa sig för att nå jämvikt med sin omgivning. Vidare kan organisationer delas olika nivåer enligt Dhillons stekta ägg analogi Figur 2.2.

I omgivningen och inom organisationen finns risker och hot som behöver hanteras på något sätt. För att förstå hur stödjer jag mig på teorier runt risker där fokus läggs på riskhantering. Som ett resultat av riskhanteringsprocessen finns underlag för organisationen att reducera risken och förbättra kontinuiteten i sin verksamhet genom att kontinuitetsplanera. Behovet av informationssäkerhet och utvecklingen en informationssäkerhetsstrategi är kopplade till kontextuella faktorer och hur ledningen uppfattar risk samt den strategiska vikten IT har för organisationen. För att förstå hur prioritering görs söker jag stöd i beslutsteorier om rationellt beslutsfattande.
För att förstå hur konsekvenser bedöms och hanteras, söker jag stöd i administrationsteori och beslutsteori.

3 Metod

I detta kapitel redogör jag mitt val av arbetsmetod och vetenskapligt tillvägagångssätt.

3.1 Vetenskapligt arbete

Oavsett om det handlar om vetenskapligt eller icke-vetenskapligt rapportskrivande så syftar dessa till att utveckla kunskap. Därför är det viktigt att kunna värdera om undersökningen är ett vetenskapligt arbete Lundahl & Skärvad, (1999). Vetenskapliga undersökningar karaktäriseras något förenklat till att vara:

- Inriktade på att ge teoretiska bidrag
- Upplagda och genomförda med vetenskapliga arbetsmetoder(ibid.) .

Ejvegård, (2009) menar att ett vetenskapligt arbete skall vara sakligt, objektivt och balanserat. Utöver detta måste insamlingen av data och hur den sammanställs ha skett på ett vetenskapligt sätt i syfte att ”utveckla, verifiera och falsifiera teorier” Lundahl & Skärvad, (1999). I ett vetenskapligt arbete skall forskaren grunda sina analyser, tolkningar och slutsatser utifrån empiriska data. Det är också viktigt att beskriva de metoder som forskaren använde sig av för att komma fram till sina resultat.
I ett vetenskapligt arbete utgör vetenskapsteori de ramar som forskaren måste hålla sig inom för att arbetet skall kunna ges ett vetenskapligt värde . Beroende på utgångspunkten för arbetet kommer dessa att se annorlunda ut Lundahl & Skärvad, (1999).

3.2 Val av forskningsansats

Patel & Davidson, (2003) redovisar tre olika sätt hur en forskare kan relatera teori till verklighet och detta utgör den forskningsansats som forskaren väljer.

Deduktion kännetecknas av ett arbetssätt som innebär att forskaren utifrån allmänna principer och befintliga teorier drar slutsatser om verkligheten och försöker bevisa något. Från teori härleds hypoteser som forskaren försöka falsifiera eller verifiera med resultat hämtad från empirin.

Induktion kännetecknas av att forskningen har en upptäckande karaktär. Forskaren försöker studera forskningsobjektet utan att först ha förankrat sin undersökning i vedertagen teori. Istället formulerar forskaren en teori utifrån den information och empiri som samlats in och försöker finna det som är typiskt för studieobjektet. Studieobjektet kan utgöras av en grupp människor, en speciell situation eller tid.

Abduktion kan sägas utgöra en kombination av deduktion och induktion. Utgångspunkter blir induktion av ett fall så formulerar forskaren en teori som sedan testas deduktivt mot nya fall och utvecklar teorin ytterligare Patel & Davidson, (2003).

Utifrån dessa möjliga ansatser har jag valt att använda mig av en deduktiv ansats då jag utifrån vedertagen teori prövar min frågeställning empiriskt för att sedan tolka och forma mina slutsatser.

3.3 Val av undersökningsmetod

Holme & Solvang, (1997) menar att när det gäller att studera samhället ställs forskaren inför en komplex och mångfaldig verklighet. Det är inte möjligt att med ett enda metodverktyg att kunna fånga denna verklighet. När kommer till att ta sig an samhällsvetenskapliga frågeställningar står valet mellan i två ”jämbördiga” metoder, den kvantitativa och den kvalitativa metoden.

De har sina likheter i att de har båda samma syfte, att förstå det samhälle vi alla lever i och hur enskilda människor, grupper och institutioner agerar och påverkar varandra Skillnaden mellan dem ligger enkelt uttryckt i att forskaren i kvantitativa undersökningar omvandlar informationen till siffror och mängder som sedan analyseras statistiskt. I kvalitativa undersökningar handlar det om forskarens egen uppfattning och tolkning av informationen som ligger lyfts fram som exempelvis tolkning av referensramar, motiv, sociala processer och sammanhang. Där är det inte alltid möjligt eller lämpligt att omvandla dessa till siffror (ibid.).

Holme & Solvang, (1997) säger att vid kvantitativa metoder så ligger fokus på hur representativ informationen är som forskaren samlat in, huruvida den har mätt det forskaren ville mäta det vill säga är pålitlig (reliabel). Detta har inte samma centrala plats när det gäller kvalitativa undersökningar då syftet med en kvalitativ studie är att skapa större förståelse av vissa faktorer och då blir inte representativiteten lika fokuserad. Vad som är mer viktigt är att hitta undersökningsenheter som man utifrån vissa underliggande sociala förhållanden räknar med att kunna ge en mer nyanserad bild av den företeelse forskaren vill studera. Kvalitativa undersökningar karaktäriseras av en närhet till de enheter man vill studera vilket gör att problemet med att få giltighet (valid) mindre jämfört med en kvantitativ studie samtidigt som andra problem följer med valet av kvalitativ studie. Som att forskaren kan ha missförstått situationen, misstolkat de svar och signaler som respondenterna ger. Den närhet till enheterna som studeras kan också skapa förväntningar på ett visst beteende och svar från respondenterna (ibid.)

Eftersom jag vill få förståelse om en rad underliggande faktorer som i sin tur påverkar informationssäkerhet och den sociala process, som enligt min mening prioritering utgör, ser jag den kvalitativa undersökningsmetoden som bäst lämpad. Detta eftersom kvalitativa undersökningar kännetecknas av att forskaren försöker förstå hur människor upplever sig själva, sin tillvaro, sin omgivning och det sammanhang de ingår i enligt Lundahl & Skärvad, (1999).

3.4 Val av undersökningsansats

Lundahl & Skärvad, (1999) beskriver olika typer av undersökningar. Valet av undersökningsansats beror på syftet med undersökningen, val av metodteori, omfattning och i övrigt det sättet som är lämpligt och genomförbart för att skaffa data. Med utgångspunkt från att undersökningen kan skiljas mellan experimentella och icke-experimentella undersökningar. Experiment är lämpligt vid undersökningar som syftar till en förklaring då forskaren kan förändra ingående variabler som han tror leder till vissa effekter och hålla omständigheterna kring experimentet konstanta och kontrollera andra orsaksvariabler än den som undersöks. När det gäller icke-experimentella undersökningar som fallstudier och survey undersökning handlar det istället om att den information som samlas in ska vara standardiserad och att alla respondenter svarar på samma frågor vilket möjliggör en kvantitativ bearbetning och analys av svaren. Surveyundersökningar genomförs ofta som stickprovsundersökningar. Fallstudien är en undersökningsmetod som omfattar ett eller ett fåtal fall som studeras mera detaljerat och i flera dimensioner och genomförs ofta med syftet att formulera hypoteser, utveckla teorier eller exemplifiera och illustrera. Fallstudier kan användas för att både utveckla teorier och testa teorier, särskilt vid studie av komplexa problem. Fallstudien har sin fokus på de frågeställningar som beskrivs i syftet men har till nackdel att det kan vara svårt att dra generella slutsatser Lundahl & Skärvad, (1999). Yin, (2006) ger också stöd för vilken typ av undersökning som skall användas. Enligt honom så är det forskningsfrågan och dess formulering avgörande. Är frågan av ”hur” och ”varför” karaktär passar fallstudien bra som undersökningsmetod.

En annan distinktion är graden av kontroll och tillgång forskaren har till situationer där ett visst beteende uppvisas. Om forskaren vill studera en aktuell händelse och inte behöver ha kontroll över beteendet passar fallstudie som undersökningsmetod. Studier kan vara beskrivande, explorativa eller förklarande Yin, (2006) och fallstudien kan precis som de andra typerna av undersökningarna vara vilken som av dessa.
Eftersom jag vill undersöka hur och varför prioritering av informationssäkerhet görs där prioritering utgör en komplex social process av individers perception och organisatoriska kontexter där jag inte har kontroll över deras beteende. Utifrån detta resonemang ser jag att en beskrivande och förklarande fallstudie kan vara mycket passande för det område jag vill undersöka.

3.5 Validitet

Enligt Lundahl & Skärvad, (1999) är det så att i de flesta utredningssammanhang blir datainsamlingen en viktig del av utredningsarbetet. Datainsamling innebär ofta någon form av mätning och då är det viktigt att veta med vilken precision mätningen skall göras. Nivån för precision är kopplad till bland annat:

- Vilken precisionsnivå som behövs med andra ord vad skall mätningen användas till?
- Vilken precisionsnivå som är möjlig att uppnå rent mättekniskt?
- Vilken precisionsnivå som är möjlig med hänsyn till ekonomiska begränsningar?

Validiteten i en mätning kan definieras som frånvaro av systematiska fel och skiljer på inre validitet och yttre validitet. Inre validitet föreligger när mätinstrument som exempelvis frågeformuläret i en intervjuundersökning eller enkätundersökning mäter vad som var tänkt och avsett att mäta. Det råder då en hög grad av överensstämmelse mellan den teoretiska och den operationella definitionen. Yttre validitet uppstår då mätinstrumentet som till exempel en enkät ger en dålig indikation på det problem forskaren sökt svar på. Det är sålunda dålig överensstämmelse mellan vald indikator det vill säga svaren på enkäten och det förhållande han söker att bedöma Lundahl & Skärvad, (1999).

Jag har försökt att skapa hög validitet för min undersökning genom att välja respondenter som i sitt arbete kommer i kontakt med frågor som rör mitt problemområde och har de kunskaper och erfarenhet som är nödvändiga för att för att kunna svara på mina undersökningsfrågor. Intervjuerna gav också möjlighet att förklara och förtydliga frågorna om frågorna uppfattades på ett sätt som inte avsågs.

3.6 Reliabilitet

Med reliabilitet avses frånvaron av slumpmässiga mätfel. Undersökningar med god reliabilitet kännetecknas av att själva mätningen inte påverkas av vem det är som utför mätningen eller de omständigheter under vilka de sker. Om det finns få slumpmässiga fel i en undersökning har mätningen i liten utsträckning påverkats av tillfälligheter anses den ha god reliabilitet. Reliabilitet är en förutsättning för validitet. Ett perfekt mätinstrument kan bli värdelöst om det används på ett felaktigt eller slarvigt. Att med hjälp olika standardiseringsförfaranden säkerhetsställa att mätningen görs på identiska sätt så långt det är möjligt, är ett sätt att öka reliabilitet och så långt som möjligt undvika slumpens inverkan på mätningen Lundahl & Skärvad, (1999).

Jag har försökt uppnå hög reliabilitet genom att använda mig av en intervjuguide för att säkerställa att samtliga intervjuer ske på samma sätt. Jag skickade ett utdrag av MSB rapporten några dagar i förväg till respondenterna så att de kunde sätta sig in läget och vara mer förberedda. Alla intervjuerna spelades in digitalt för att säkra informationen för vidare analys. Respondenterna har efter sammanställning fått möjlighet att läsa igenom och komplettera och förtydliga sina svar om de så önskade.

3.7 Urval av respondenter

Urvalet av kommuner med tanke på den avgränsning som jag gjort är förhållande vis stort, Sverige har idag 290 kommuner . Komplexiteten i kommuners organisation påverkar deras arbete med informationssäkerhet därför anser jag att det för min studie är viktigt att finna kommuner som har en viss grad av komplexitet i deras organisation. Detta för att uppnå så hög validitet som möjligt.
Att sedan finna respondenter som aktivt arbetar med informationssäkerhetsfrågor i sin profession bidrar till hög reliabilitet. Därför har jag valt att använda informationssäkerhetspolicy och erfarenheten hos den som ansvarar för att driva frågan som kriterier för mitt urval.

3.8 Fallstudiens utförande

Jag genomförde en litteraturstudie inom det område som jag var intresserad av för att få tillgång till teorier inom mitt valda ämnesområde som omfattar ledning av informationssäkerhet, riskhantering, kontinuitetsplanering samt beslut inom organisationer. Utifrån dessa teorier har jag format mitt problemområde, problemställning samt forskningsfråga och syfte.

3.9 Design av fallstudien

Jag kände mig rätt fri i valet av respondenter med tanke på det stora antalet kommuner som finns. För att kunna skapa mig en grundläggande uppfattning om hur kommuner arbetar med informationssäkerhet så valde jag inleda med att undersöka två kommuner i närområdet. Syftet var att på ett förtroendeingivande sätt samla in grunddata för mer djupgående fallstudie eftersom området informationssäkerhet kan anses vara känsligt både ur ett personligt och organisatoriskt perspektiv. Syftet var att också att etablera en personlig kontakt och förtroende för djupgående studier. På grund av detta fann jag att en surveyundersökning som enkät inte vara lämplig.
I det första steget handlar det om att skapa en grundläggande förståelse hur mognadsgraden för informationssäkerhet är hos organisationen, där ett av kriterierna är arbetet med policys för informationssäkerhet det andra är erfarenheten hos den som ansvarar för att driva frågan.
Eftersom jag i mitt syfte ville förstå hur och varför prioritering av informationssäkerhet sker, fanns i mitt andra steg kriteriet att nå respondenter som antingen själva fattade beslut om säkerhet och informationssäkerhet alternativt rapporterade till dessa beslutsfattare. Av praktiska skäl visade det sig att det var lättare att få tillgång till de som rapporterade till beslutsfattare. Eftersom det bara var endast en av dessa två kommuner som hade en utarbetad och fastställd informationssäkerhetspolicy, således bedömdes ha den mognadsgrad som jag efterfrågade, utgör denna kommun mitt fall.
I det andra steget vände jag mig till samma respondent som i första steget plus ytterligare två som arbetade med informationssäkerhet inom kommunen på olika nivåer. I vissa hänseende kan jag säga att min fallstudie är en replikation.

3.10 Val av datainsamlingsmetod

Metoden för att samla in sina data kan antingen ske genom att göra observationer eller använda frågemetoder. Observationer kan vara lämpligt när forskaren exempelvis vill titta på beteenden som prioritering. Kritiker menar att, för att verkligen förstå skeenden i sociala situationer är det nödvändigt att aktivt, öppet och engagerat delta i situationen, annars kan beteendet bara förstås ytligt eller till och med missuppfattas Lundahl & Skärvad, (1999). Det finns olika sorters intervjuer beroende på graden av standardisering. Hög standardiseringsgrad finns i intervjuer där frågorna och ordningsföljden mellan frågorna är bestämda på förhand. Frågorna och upplägget måste följas av flera olika personer i undersökningen. Med en ostandardiserad intervju kan frågeformuleringar och ordningsföljd väljas fritt och förutsättningslöst intervjuaren ges därmed bättre möjlighet till flexibilitet och anpassad till rådande situation vid genomförandet av intervjun. Mellanformen av intervjuer är den så kallade semistandardiserade intervjun där vissa förutbestämda frågor ställs till alla respondenter och följs sedan upp med följdfrågor. Standardisering har sitt syfte att möjliggöra en kvantitativ bearbetning av svaren och motsats blir då ostandardiserade intervjun som ger möjligheten till en kvalitativ bearbetning Lundahl & Skärvad, (1999).
Det viktiga är dock att oavsett typ av intervju att den information som erhålls av respondenten ger den information som täcker den målsättning som undersökningen syftar till. Den ostandardiserade intervjun är mest lämpad vid explorativa och teoriskapande undersökningar och standardiserade intervjuer lämpar sig bättre vid hypotes och teoriprövande Lundahl & Skärvad, (1999). Intervjuer kan genomföras på olika sätt, som personlig intervju på plats eller som en telefonintervju.

Jag genomförde personliga intervjuer och kompletterade mina svar med telefonintervju och e-post. Områdets känsliga natur, tidsbegränsningen och kostnaden låg som grund för valet av min metod för datainsamling. Intervjuerna bestod av ostandardiserade frågor eftersom jag var ute efter kvalitativa, mjuka data och det passar bäst för min fallstudie. Intervjuerna spelades in för att sedan kunna användas för min analys.

3.11 Analysmetod

Analysen tog fart redan under intervjuerna, utifrån de svar jag fick från respondenterna tolkade jag min teori och kunde värdesätta deras svar för att direkt kunna ställa följdfrågor. Intervjuerna transkriberades därefter genom att lyssna igenom varje intervju ett flertal gånger och skriva ned deras svar. Därefter sammanställde jag detta med mina anteckningar under intervjuerna för att få en så korrektbild som möjligt av intervjuerna. Genom att koppla respondenternas svar till de olika kategorier som jag ställt upp i min teori, kunde jag tolka och jämföra empiri och teori och där finna överensstämmelser. Där det var möjligt kopplade jag också in direkta citat på utsagor från respondenterna i enlighet med Patel & Davidson, (2003).

4 Empiri

Efter överenskommelse med respondenterna skall de hållas anonyma. Fallstudien består av kvalitativa intervjuer som jag valt att återge i sammanfattad form. Transkribering av intervjuerna finns i bilaga3.

4.1 Intervju 1

Intervju med Kommunen A:s Informationssäkerhetssamordnare.

Jag intervjuade honom vid två tillfällen, först mer generellt och den andra gången mer djupgående om Kommun A:s arbete med informationssäkerhet. Min förhoppning var att han skulle kunna ge en bild över det övergripande arbetet med informationssäkerhet och den roll kommunledningen spelar för att stötta och skapa förutsättningar för detta arbete.

4.1.1 Bakgrund och allmänt om informationssäkerhet

I Kommun A är informationssäkerhetssamordnaren en roll och inte en tjänst, vilket innebär att uppgifterna är del av hans ordinarie arbetsuppgifter som kommunens nya IT-samordnare. Placeringen av informationssäkerhetssamordnaren har fram till nyligen varit på IT-avdelningen, något som han förklarar beror på att säkerhetsarbetet till en början handlade om IT-säkerhet ansågs bäst skötas av IT-avdelningen. När sedan IT-säkerhet utvecklades till informationssäkerhet i samband med att MSB förändrade innebörden av begreppet ser han att den rollen bör bättre placeras på ledningsnivå. Nuvarande placering innebär att han som informationssäkerhetssamordnaren hamnar i en jävsituation när han skall utreda IT-avdelningen som är hans egen avdelning. Förutom jävsituation så förvirrar placering också eftersom det är oklart att det är han som har det övergripande ansvaret och bör involveras i projekt som berör informationssäkerhetsfrågor i olika perspektiv. Kommunens informationssäkerhetsarbete regleras i huvudsak av följande lagar, förordningar och principer:

- Sekretesslagen
- Säkerhetsskyddslagen
- Offentlighetsprincipen
- Tryckfrihetsförordningen

Säkerhetsarbetet i kommun A samordnas av Kommunledningskontoret och dess säkerhetsgrupp som består av säkerhetsansvarig, säkerhetssamordnare, säkerhetshandläggare, försäkringssamordnare och informationssäkerhetssamordnare. Utöver dessa befattningar som utses av kommunchefen får gruppen till sig adjungera ytterligare personer som kan vara lämpliga som exempelvis sakkunniga i specifika frågor eller verksamheter.

Gruppen har till uppdrag att samordna kommunens gemensamma säkerhetsarbete, se till att underliggande riktlinjer och rutiner utarbetas, ge råd och stöd till förvaltningar och kommunens bolag, ge stöd till förvaltningarna och kommunens bolag i sitt arbete med att ta fram riskanalyser och handlingsplaner, planera och erbjuda förtroendevalda, säkerhetsombud och andra anställda utbildning och övning.

Gruppen skall också ge förslag till kommunstyrelsen på mål och budget för säkerhetsarbetet samt att följa upp de mål och budget som finns för säkerhetsarbetet. Att sammanställa och följa upp skadestatistik inom det interna skyddet, följa upp effekterna av de åtgärder som vidtagits och slutligen göra en översyn och vid behov revidera riktlinjerna för säkerhetsarbetet

Informationssäkerhetssamordnaren berättar att arbetet med informationssäkerhet så här långt handlat mycket om råd och stöd till kommunens alla verksamheter och informationsspridning där han informerat samtliga förvaltningar och verksamheter om vikten av informationssäkerhet. Syftet är att höja medvetenheten hos medarbetarna vilket är något sker på initiativ från respektive förvaltningschef då något fastställt

utbildningsprogram för att öka medvetenheten saknas. Han förklarar att öka medvetenheten är den del av informationssäkerhet som kommunen arbetar aktivt med generellt. Området skydd är något som främst IT-avdelningens personal hanterar då den tekniska säkerheten är väl etablerad där med att väga säkerhet kontra användarvänlighet.

Responsen han får i kontakten med förvaltningar och bolag är blandad, de flesta tycker att det är bra och säkerhetsfrågor är viktiga men när det skall övergå i handling så sorteras informationssäkerhet tyvärr undan i prioritet.

De riktlinjer och styrdokument som finns i kommunen idag togs fram efter att Krisberedskapsmyndigheten nuvarande Myndigheten för Samhällskydd och Beredskap (MSB) tog upp frågan med kommunen. Vissa dokument saknades, det fanns en IT-säkerhetspolicy men den var inte tillräcklig.

Att använda standards i arbetet med informationssäkerhet ser han som positivt. BITS (Basnivå för informationssäkerhet) som är en standard från MSB, är en början för att kunna ta tag i arbetet och ger bra vägledning för att kunna ta med alla aspekter. Den är också lättanvänd och väl anpassad för kommunens behov.

Begreppet informationssäkerhet
På frågan om vad begreppet informationssäkerhetsbegreppet innebär så säger han att för honom handlar det om alltifrån ärendehantering, sekretessfrågor till fysisk säkerhet och teknisk säkerhet . Att begreppet omfattar administrativa delar som hur ärenden skall hanteras samt tekniska delar som brandväggar och virusskydd. Han säger ”säkerhet i sig bygger på sunt förnuft men på grund av att säkerhetsområdet är så brett så kan det ses som ett komplext problem”.

4.1.2 Ledningen av informationssäkerhet

På frågan om ledningens roll för informationssäkerheten så svarar han att kommunstyrelsen har beslutat om att organisera säkerhetsgruppen med medlemmarna som kommer från olika delar av verksamheten och där bland annat personer från kommunledningskontoret och gruppen svarar inför kommunstyrelsen i vissa beslut och andra beslut har de mandat att fatta själv alternativt kan de gå till kommunledningen för att få ett godkännande. Tyngre beslut som säkerhetspolicy skall gå via kommunstyrelsen och kommunfullmäktige för beslut. Varje förvaltning är sin egen myndighet med sin egen nämnd som fattar beslut . Säkerhetsgruppen tillhör kommunledningsförvaltningen och kommunstyrelsen och behöver beslut därifrån för att kunna påverka de andra förvaltningarna och nämnderna. Beslut behöver således upp i hierarkin för att kunna falla ned någon annanstans.

Prioritering av informationssäkerhet
När det gäller prioritering mellan de olika säkerhetsområdena säger han att skydd mot olyckor och interna skyddet prioriteras högre på grund av att det är mer konkret och lättare att ta på och syns exempelvis när en stor övning tillsammans med räddningstjänsten genomförs i verksamheten. Informationssäkerhet är mer abstrakt och synliggörs inte så mycket.

Idag så prioriterar kommunledningen det övergripande säkerhetsarbetet på den nivå att kommunen uppfyller de lagar och krav som ställs. Kommunen har endast rekommendationer kring informationssäkerhetsområdet från MSB. Den dag MSB ställer upp med hårdare krav som skall uppfyllas av kommunerna så kommer de att vara tvungen att fokusera mer på området. Idag så tillsätts det för små resurser för att kunna vidareutveckla informationssäkerhetsområdet. Idag så landar arbetet med informationssäkerhetsområdet på den nivån att komunen ser till att arbeta fram styrdokument och i viss mån informerar om informationssäkerhet framför allt på ledningsnivå säger informationssäkerhetssamordnaren.

Det strategiska värdet av informationssäkerhet
Ur en strategisk synvinkel är informationssäkerhet viktig för kommunen för att det handlar om främst om trovärdigheten för kommunen.

Informationssäkerhet kopplat mot organisationens mål, visioner och mål
Vad gäller hur kommunens övergripande mål, visioner och strategier avspeglar sig i arbetet med informationssäkerhet svarar han att det inte märks mycket exempelvis målet uthållig kommun kan omfatta säkerhet där kommunen skall vara uthållig på det sätt att den skall kunna verka oavsett situation och miljö. Att säkerhet är ett långsiktigt kontinuerligt arbete har kommunledningen börjat förstå i och med att det är dags att precis revidera kommunens riktlinjer för säkerhet.

Han säger ”att i de olika verksamhetsplaner som finns idag tas inte informationssäkerhet eller säkerhetsfrågor med. De är inte en del av vardagen, och har fått komma in i ledningsrummen som en naturlig punkt. Att IT-chefen nu finns med i ledningsgruppen för kommunledningskontoret tror han kan bidra med att förändra detta till det bättre framöver”.

IT-avdelningens synsätt att alltid tänka ur ett säkerhetsperspektiv och att proaktivt säkra upp är något som behöver spridas hos alla i organisationen. Ett sätt att tänka när nya processer och rutiner arbetas fram. Han pekar på att inom kommunen så har ju den administrativa säkerheten, framförallt kraven på sekretess kunnat hanteras förr och säkerhetsställas som hos socialtjänsten. Även om det kan skilja sig avsevärt mellan de olika förvaltningarna och bolagen så upprätthåller de en god sekretess och medarbetarna har bra kännedom om lagrum som styr hanteringen. Problemet som han ser det är att uppfattningen att IT-säkerhet är en teknisk fråga och att den nya innebörden av informationssäkerhet och det ansvar som verksamheterna har i att säkra sin egen information inte är klar för dem.

4.1.3 Informationssäkerhet och beslutsfattande

Beslut som rör informationssäkerhet har hittills skett på tjänstemannanivå förutom den gemensamma säkerhetspolicyn för kommunen. Verksamhetsnära frågor behandlas på kommunchefnivå. Beslutsprocessen skiljer sig inte vad gäller informationssäkerhet gentemot andra områden annat än att informationssäkerhet kan uppfattas mer abstrakt och därför upplevs svårare vilket kan leda till att beslut skjuts upp. Utvärdering av alternativ sker mycket enligt satisfiering där bra nog räcker. Förklaringen ligger mycket i att det inte finns någon fastställd hotbild. Arbetet med risk och sårbarhetsanalysen har påbörjats och förväntas kunna leverera hotbild och identifiering av risker.

Omvärldsfaktorer
Omvärldsfaktorer spelar in skärskilt när det sker in organisationens närhet framför allt vad det gäller tiden att fatta beslut och verkställa det. Kommun A är hittills förskonad hot och annat som skadegörelse vilket gör att det råder en öppenhet generellt, vilket också påverkar fokusen på säkerhetsarbetet, med uppfattningen att det inte finns några hot och risker.

Kultur
Kulturens roll spelar in och på hur pass riskpräglad organisationen är, enligt informationssäkerhetssamordnaren så förstår kommunens medarbetare inte alltid värdet av den information kommunen sitter på och värdet på de tillgångar som kommunen förfogar över och att det är skyddsvärt.

Strukturen
Organisationsstrukturen påverkar på ett sådant sätt att som kommun är vidden på säkerhetsfrågorna och behovet av skydd väldigt bred. Det varierar allt mellan minimala insatser till 24-7 för att få verksamheten att fungera. På frågan om den kommunala byråkratin svarar han att den ser mer som garanti för demokrati och som positiv för att kunna fatta bra beslut.

4.1.4 Informationssäkerhet och risk

Risk och sårbarhetsanalysen som pågår nu är idag det enda sätt som kommunen utvärderar hot och risker. Ledningens riskmedvetenhet bedömer han före denna genomgång att vara väldigt varierande. Förhoppningen är att kommunen vid genomgång med respektive verksamhetsledning i detta arbete skall kunna höja riskmedvetenheten generellt när denna utvärdering är genomförd.

4.1.5 Kommentar på rapporten från MSB

På frågan om bilden som beskrivs i rapporten så säger han ”den stämmer rätt bra in på kommunen och förklaringen ligger i att ledningen prioriterar frågan för lågt och endast lägger minimala insatser för att kunna uppfylla lagen men inte mer”. Kontinuitetsplanering sker i viss mån praktiskt men det dokumenteras inte på något sätt och är inte sammanhållen. På IT-avdelningen finns vissa lösrykta dokument som reservrutiner och annat men ingen sammanhållen dokumentation. Någon övergripande kontinuitetsplanering finns inte idag. Att inte ingångsvärden leveras hänger ihop med kunskapsbrist att någon medvetet skulle undanhålla dessa från verksamheten är för honom helt främmande. Mycket sker i oförstånd. Men det hänger också ihop med att regering och MSB inte ställer krav på kommuner dessutom när det är finns ett lagkrav utan bara rör sig om rekommendationer. Så länge det inte är lag på det kompromissar kommunen.
De risker som han ser som allvarligast idag så säger han det är många men ett är lösenordshantering, single sign-on samt kunskap och förståelse om exempelvis sekretesslagens innebörd. Incidenthantering fungerar men rutinen behöver uppdateras . Största bristen resurser för att jobba aktivt med frågan.

4.2 Intervju 2

Intervju med Kommun A:s IT-chef
IT-avdelningen i Kommunen består av tre enheter, IT-service, IT-drift och webbenhet. IT-avdelningens uppdrag är att bland annat:

- *Att på ett verksamhetsinriktat och kostnadseffektivt sätt, stödja kommunens olika verksamheter i IT-relaterade ärenden, som bland annat, teknisk drift, support, inköp eller allmän rådgivning.*
- *Att följa branschens utveckling och kunna omsätta detta till verksamhetsnytta.*
- *Samordna IT, telefoni och informationssäkerhetsfrågor.*
- *Underhålla och utveckla kommunens webbplatser*

Genom att intervjua Kommun A:s IT-chef hoppades jag få en bild av IT-stödets roll inom kommunen och deras arbete med informationssäkerhet och deras beredskap för att hantera avbrott och kriser relaterade till kommunens informationssystem. IT-chefen berättar att han har arbetat mer än sju år i sin befattning som IT-chef, ansvaret för IT har han haft längre eftersom började som ensam IT-samordnare för kommunen 1989 och allteftersom har det anställts fler IT-tekniker och idag finns 22 tekniker anställda på kommunens IT-avdelning. IT-chefen har inte någon formell utbildning inom informationssäkerhet utan den kunskap och erfarenhet han har idag kommer från egen förkovring och någon enstaka kurs genom sitt arbete. Fokus har dock legat på teknik sidan och IT-säkerhet eftersom han i grunden är IT-tekniker.

Rollen som IT-chef berättar han innebär att han är avdelningschef för IT-avdelningen med budget ansvar och till sin hjälp har han en underställd chef som sköter drift och service frågor. Hans roll när det kommer till informationssäkerhet berättar han innebär mycket att verkställa det som förväntas av IT-avdelningen när det gäller på grundläggande informationssäkerhet från verksamheterna vilket innebär att upprätthålla en basnivå för säkerheten. Han säger att det kommer förhållandevis lite krav från verksamheterna så därför försöker IT-avdelningen utifrån sin kännedom vidta åtgärder på eget initiativ för att kunna upprätthålla en basnivå vad gäller IT-säkerhet och informationssäkerhet.

4.2.1 Bakgrund och allmänt om informationssäkerhet

Här kommer jag in på kommunens informationssäkerhetskontext och vilket värde informationssäkerhet har strategiskt.

IT-avdelningens roll
Det innebär att ta fram informationssäkerhetspolicy, riktlinjer och instruktioner för förvaltning och användare . IT-chefen säger ”att när det gäller ansvarsbiten för informationssäkerhet så ligger ansvaret för den tekniska delen hos IT-avdelningen men den administrativa delen ansvarar de olika verksamheterna själva för”. IT-avdelningen

kan ge råd till verksamheterna och väcka frågan om säkerhet i systemet men i slutändan är det verksamheten själv som äger informationen och ansvaret att klassa informationen och säkra den. I dag saknas ofta den insikten hos verksamheterna själva trots att det finns system som kan anses vara kritiska. I vissa av verksamheterna som hos socialtjänsten finns insikten och där finns manuella reservrutiner framtagna trots brist på resurser. Underhåll av dessa rutiner kräver också insatser då förändringar i IT-system görs. IT-chefen berättar att IT-avdelningens roll som rådgivare till övriga verksamheterna kan utvecklas mycket mer än hur den används idag när det gäller informationssäkerhet. Allt bygger på att verksamheternas egen insikt om sitt eget ansvar för sin informationssäkerhet och möjlighet att använda IT-avdelningen som bollplank för dessa frågor.

IT-chefen berättar att standarder som exempelvis BITS används inte på sätt som den skulle kunna göra framförallt vid upphandlig av system. Verksamheten skulle kunna använda standarden vid i kravspecifikationen som att systemet skall uppfylla lägst BITS Basnivå. Anledningen är enligt honom okunskapen att de kan ställa dessa krav vid upphandling.

Han bekräftar att anledningen att kommunen tog fram de styrdokument som finns idag var påtryckningar från staten om att kommuner skulle ha en informationssäkerhetssamordnare utsedd. MSB, bedrev också en kampanj och erbjöd utbildning. Förutom staten pekade också säljföretag som besökte kommunen behovet att ta fram dessa dokument. När det från början handlade om IT-säkerhet var det naturligt att låta IT-avdelningen vara ansvarig och en arbetsgrupp kallad IT-säkerhetsgruppen tog fram dokumenten.
Gruppen finns inte kvar idag och efter att IT-säkerhet utvecklades till informationssäkerhet har arbete har stannat upp. Placeringen av informationssäkerhetssamordnaren inom IT-avdelningen var lämplig då eftersom det var en roll och inte en tjänst. Han ser idag problemet med jäv och liknande och säger att det hade varit bättre om informationssäkerhetssamordnaren fanns placerad närmare ledningen alternativt på en säkerhetsavdelning. Han ser att det finns behov att någon centralt driver frågan mot ledning och politiker men att resurser och mognad hos kommunen att tillsätta en sådan tjänst inte funnits tidigare.

Hans uppfattning är att kommunen arbetar mest med de delar av informationssäkerhet som handlar om skydd i form av tekniska lösningar men också området program där en översyn av utbildningsprogram för nyanställda för att förbättra hantering av IT och information görs. Viktigast just nu är att öka medvetenheten hos medarbetarna men givetvis skall alltid lagrum följas av kommunen.

Begreppet informationssäkerhet
På frågan om vad begreppet informationssäkerhet innebär så svarar han att det handlar om att se till att rätt information och data skall finnas tillgängligt till rätt personer när helst de behöver det och att allt är rätt och riktigt. Konfidentialitet, tillgänglighet och riktighet finns i ryggmärgen hos alla som jobbar på IT-avdelning när det gäller exempelvis att öppna upp access till system och information.

Det strategiska värdet av informationssäkerhet
När det gäller den strategiska vikten av informationssäkerhet säger han att IT-avdelningen anser den vara viktig men saknar beslut av vissa framtagna dokument som bl a pekar ut ansvaret för prioritering av verksamhetssystem och som legitimerar it-avdelningens agerande vid eventuell större driftstörning. IT-avdelningen har förvisso en bild av vilka system som är viktiga eftersom de också har kännedom om de olika verksamheterna och dessutom en mycket klar bild om vilka system som krävs för att hålla igång IT-infrastrukturen.

4.2.2 Ledningen av informationssäkerhet

Prioritering av informationssäkerhet
Frågan om ledning av informationssäkerhet och synen på denna säger han att det är väldigt sällan det kommer upp i diskussion med kommunchef frågor som rör informationssäkerhet. Det har hittills rört sig om de incidenter som uppstått och hittills varit få. Han berättar vidare den rutin för incidenthantering som kommunen använder fungerat bra. Kommunchefen har ambitionen att ägna sig mer åt säkerhet och IT-chefen rannsakar sig själv och säger att på grund av att han som ny i ledningsgruppen har varit lite osäker på forumets roll och inte drivit frågan som han kanske borde. Det råder också viss osäkerhet om vem inom kommunledningskontoret som skall driva informationssäkerhetsfrågan där informationssäkerhetens multidiciplinära natur starkt påverkar denna oklarhet.

Kunskap hos ledningen
Kunskap och medvetenheten hos chefer säger han har förändrats något i och med att nya chefer rekryterats. De kommer från näringsliv och andra myndigheter ställer allt mer frågor om informationssäkerhet än vad som gjorts tidigare han menar att dessa nya chefer ifrågasätter mer kanske på grund av att det lätt blir så när man kommer in i en ny organisation. Hittills har det varit få frågor som kommit från de chefer som arbetat länge inom kommunen. Han ser en viss passivitet hos vissa av de äldre cheferna i frågor som rör informationssäkerhet. Detta kan förklaras av att kopplingen mellan IT och informationssäkerhet ses så stark, istället för att de utgår från behovet hos själva informationen förväntar de sig en tekniska lösningen. IT-chefen berättar att han ser mycket positivt med det nya sättet att tänka som de nya cheferna har med sig och ser också att kommunen som organisation börja mogna för att ta hand om dessa frågor.

Informationssäkerhet kopplat mot organisationens mål, visioner och strategier
Han berättar att han idag är osäker på hur verksamheterna själva väver in säkerhetsaspekter i verksamhetsplanerna.

4.2.3 Informationssäkerhet och beslutsfattande

Som han ser det skiljer sig inte beslutsprocessen för informationssäkerhetsfrågor åt gentemot mot andra frågor utan är en del av verksamhetsansvaret och de beslut som tas i och med detta. Mycket av besluten som fattas bygger på satisfierande, att hitta ”bra nog” lösningar, när det gäller informationssäkerhet. Detta beror på mycket den hotbild ledningen ser mot kommunen, som idag inte visar på några allvarliga hot. Kommunens mål, visioner och strategier kan enligt IT-chefen påverka beslut som rör informationssäkerhet eftersom de anger ramarna för vad informationssäkerhet och hanteringen av informationen måste uppfylla för att kommunen skall kunna nå sin målsättning och visioner. Inför ett beslut som rör informationssäkerhet har det tidigare enligt IT-chefens erfarenhet varit så att många beslutfattare förlitar sig mycket på att IT-avdelningen sköter informationssäkerhetsfrågor och uppfattningen att informationssäkerhet handlar om IT-säkerhet gör att verksamheten inte tar i frågan själv och lägger beslut åt sidan.

Omvärldsfaktorer
Omvärldsfaktorer spelar givetvis in och kan få betydelse för beslut, skärskilt om det sker omedelbara hot och risker i omgivningen. Detta kan snabba upp processen och prioritering av beslutet.

Kulturen
På frågan om hur kulturen påverkar beslut om informationssäkerhet så svarar han att organisationskulturen påverkar eftersom att många inom kommunen stödjer sig på att det mesta ju är offentlig handling och risktänkandet finns inte alltid med. Det mesta skall ju vara öppet för medborgarna. Detta påverkar i sin tur valet säkerhetslösningar.

Organisationsstruktur
Strukturen spelar in eftersom att varje nämnd är ju egna myndigheter som har sina respektive lagrum och förordningar att ta hänsyn till och dessa nämnder tolkar ju informationssäkerheten utifrån den egna verksamheten och inte tar hänsyn till den centrala hållningen från kommunen. Att trögheten i den kommunalbyråkrati, när det gäller att ta beslut, kan medföra en risk att det tar alldeles för lång tid medger han. Men å andra sidan så granskas det av fler människor och därmed kan det leda till ett bättre beslut i slutändan, vilket IT-chefen menar uppväger den eventuella risken.

4.2.4 Informationssäkerhet och risk

IT-chefen berättar att IT-avdelningen själva kontinuerligt har en omvärldsbevakning för att identifiera hot och risker som kan drabba kommunens IT-infrastruktur. Kommunen som organisation med sina verksamheter ligger sällan först som måltavla för angrepp enligt hans uppfattning . Idag görs ingen övergripande analys av hot och risker vilket medför att kopplingar IT och informationshantering allmänt kan förbises. Riskmedvetenheten runt informationssäkerhet hos kommunledningen är enligt IT-chefen bra, åtminstone inom kommunledningskontoret,

eftersom nuvarande kommunchef upplevs ha en bra uppfattning om risker i omvärlden. Dock har han svårt att uttala sig om hur det ser ut på andra förvaltningar.

4.2.5 Kommentar till rapporten från MSB

Vad gäller rapporten från MSB så säger han att det finns många likheter med situationen i Kommun A och den enkla förklaringen är att det helt enkelt händer för lite incidenter för att mer fokus skall läggas på informationssäkerhet. Som läget är idag så saknas katastrof och kontinuitetsplaner hos kommunen. Vad gäller ansvar för avbrott och insikt om beroende av IT-stödet säger att han det givetvis varierar mellan de olika förvaltningarna och bolagen.

Hans uppfattning är att de som har insikt om riskerna också inser att arbetet med att åtgärda bristerna är för stora som att exempelvis ta fram manuella reservrutiner. Därför intar de en mer passiv ställning och förlitar sig på IT-avdelningen skall ordna saken.

IT-chefen säger ”Systemägarrollen är klar hos förvaltningar men de ställer inte krav och levererar inte ingångsvärden till IT-driften om acceptabla avbrottstider för deras system. Därför kan IT-driften i bästa fall göra en kvalificerad gissning om hur pass känsligt systemet är”.

När det gäller driftfrågor och nödvändig personal för att kunna avhjälpa så tar IT-avdelningen, och har tagit, ansvar för detta genom att skapa redundans i teknik, personal och håller dokumentationen aktuell. Han ser det ytterst viktigt att IT-avdelningen signalerar till systemägare och kommunledningen att de inte har resurser för att uppnå dessa krav utifrån ingångsvärden. Idag har han inte någon bild över hur dessa ingångsvärden se ut, då de saknas. Därför finns ingen kontinuitetsplan och katastrofplan framtagen och avstämningen mot verksamheten är heller inte genomförd. Eftersom det finns system som inte ligger under IT-avdelningens driftansvar såsom styr- och reglersystem av fastigheter och vattenverk ställer han sig frågan hur pass hög är medvetenheten hos dessa förvaltningar om informationssäkerhet och deras beredskap för avbrott med tanke på personberoende och redundans.

4.3 Intervju 3

Intervju med Kommun A:s - Säkerhetsansvarig

Genom att intervjua den som leder kommunens säkerhetsgrupp hoppades jag att få en bild hur det övergripande säkerhetsarbetet i kommunen genomförs, hur säkerhet och informationssäkerhet prioriteras samt hur beslut om säkerhetsfrågor tas. Han berättar att rollen som säkerhetsansvarig innebär är att samordna kommunens säkerhetsarbete utifrån de fem säkerhetsområden som kommunen har fastställt och sedan rapportera detta till kommunchefen som formellt är tillika säkerhetschef. Rollen som säkerhetsansvarig har han haft sedan sommaren 2010, tidigare fanns denna roll på kommunledningskontoret. Eftersom det är en roll och inte en tjänst så är den en del av hans ordinarie arbetsuppgifter. Kommunchefen har delegerat samordningsansvaret för säkerheten till säkerhetsansvarig och han berättar som det ser ut idag så rapporterar han endast och ger råd till kommunchefen som sedan därefter fattar beslut. Nackdelen med detta är att kommunchefen har andra frågor på sitt bord och har inte den tid som vore önskvärt att ägna åt säkerhetsfrågor. Han ger exemplet att en grannkommun har utsett en separat säkerhetschef som verkar direkt mot kommunstyrelsen precis som de andra förvaltningscheferna. Han berättar att han har i samtal med denna person förstått att det upplägget underlättat säkerhetsarbetet betydligt.

4.3.1 Bakgrund och allmänt om informationssäkerhet

Här kommer jag in på kommunens informationssäkerhetskontext och vilket värde informationssäkerhet har strategiskt

Vad gäller områden som kommunen arbetar aktivt med så säger han det finns ju politiskt beslutade styrdokument men att få dessa dokument levande och del av vardagen har de inte riktigt lyckats med ännu. En delförklaring till detta är det historiskt låga intresse säkerhet i allmänhet haft hos tidigare kommunledning men att nuvarande kommunchef har en annan hållning och förstår bättre situationen. Just när det gäller informationssäkerhet så arbetas det inte så mycket eftersom tid har behövts läggas på andra områden men att ta fram policy och styrdokument och baserat på informationssäkerhetssamordnaren beskrivning så har det varit tungrott mycket på grund av okunskap på högre tjänstemannanivå som gjort arbetet svårt.

”Responsen från kommunledningen inte är så stor som säkerhetsgruppen skulle önska eftersom ledningen också har lagt andra arbetsuppgifter på den resurs, det vill säga informationssäkerhetssamordnaren, som skall jobba med detta vilket medför att arbetet med informationssäkerhet står nästan helt still sedan en tid.”

Detta har lyfts upp till kommunchefen som säger att säkerhetsarbetet är viktigt men idag har ännu ingen resurs vikts för arbetet med informationssäkerhet. Läget kan delvis förklaras av att historiskt har säkerhetsfrågor varit lågt prioriterade i Kommun A och det är först efter att nya lagar och lagkrav på vad kommunen var skyldig att göra som grunden till att den policy, riktlinjer och styrdokument som finns idag togs fram. Användandet av standarder som BITS i arbetet ser han som positivt men han överlåter detaljerna för arbetet med BITS på informationssäkerhetssamordnaren.

Begreppet informationssäkerhet
Innebörden av begreppet kommenterar den säkerhetsansvarige så här:
”Att se till att kommunen har ett stabilt system av gäller IT-stöd men också en administrativ plan hur problemet skall hanteras, att kommunen är förberedd så att inte hela verksamheten stannar upp helt. Det handlar om att se till att det finns manuella rutiner för att kunna driva verksamheten vidare.”

Det strategiska värdet av informationssäkerhet
Informationssäkerhet är enligt honom strategiskt viktigt för kommunen, att kunna säkerhetsställa information och informationsflöden exempelvis i händelse av kris. Men också för att kunna hantera mindre störningar och avbrott som sker i vardagen.

4.3.2 Ledningen av informationssäkerhet

Prioritering av informationssäkerhet
Han berättar att skillnaden mellan de olika säkerhetsområdena bygger på den lagstiftning som reglerar hur kommunen måste agera och vilka skyldigheter som kommunen måste uppfylla inom dessa lagrum. Området informationssäkerhet omfattas i sig inte av någon direkt lag och behandlas därför annorlunda. Han berättar att det handlar mer om en ambitionsnivå där kommunen har en ambition att inte lägga ned mer krut än vad som är nödvändig för att uppfylla det krav som lagen ställer. Han menar på att i tanken så prioriteras inte informationssäkerhet medvetet lägre än de andra säkerhetsområdena när det kommer till att fördela resurser . Men han säger att det haltar just nu vad gäller fördelningen av resurser för området informationssäkerhet då kommunen ännu inte fastställt hur stor del av tjänst området skall få uppta. Det finns fortfarande oklarheter om rollen informationssäkerhetssamordnare.
Eftersom de andra områdena som exempelvis internt skydd som delvis omfattas av mer konkreta lagkrav läggs det ned bitvis mycket av kommunens resurser . Kommunen har till och med lagt ambitionsnivån högre än vad lagen kräver för att man från kommunledningens sida vill värna om skyddet av sina fastigheter och tillgångar. Att information skulle utgöra en viktig tillgång ser kommunledningen inte lika tydligt och det beror mycket enligt honom på att informationssäkerhet är ett svårt område för många att greppa och förstå. Att området är abstrakt bidrar också samt saknar konkreta krav i form av lagstiftning kan förklara det läge som råder just nu. Resursfrågan säger han varierar inom de olika säkerhetsområdena beroende på lagkrav, informationssäkerhet får inte de resurser som krävs idag men att detta är något ledningen tittar på och försöker förändra.

Kunskap hos ledningen
Han berättar att kunskap och medvetenhet hos cheferna när det gäller informationssäkerhet är lite svårt att bedöma. Han kan bara utgå ifrån den kontakt som han själv haft med chefer och då förfaller det finnas en del att önska. Informationssäkerhet är inget som medarbetarna ute i verksamheterna går och tänker på dagligen utan det betraktas mer som att sådana saker skall bara fungera och sköts av någon annan i kommunen typ IT-avdelningen.

Informationssäkerhet kopplat mot organisationens mål, visioner och strategier
Säkerhet behöver också komma in i verksamheternas planering, idag syns det i princip inte alls i verksamheternas planer, därutöver behöver varje säkerhetsområde införlivas som en naturlig del i arbetet/planen och redovisas årligen utifrån de strategiska målen som kommunen har. För att detta säkerhetsarbete skall bli verkligt är det nödvändigt att verksamheterna i sina verksamhetsplaner berättar hur de arbetar aktivt med säkerhetsfrågor. Ansvaret att jobba med dessa frågor ligger på verksamheten självt och inte säkerhetsgruppen vilken skall fungera som rådgivare och katalysator.

4.3.3 Informationssäkerhet och beslutsfattande

Säkerhetsansvarige säger att har han svårt att se att beslutsprocessen om informationssäkerhet skulle skilja sig gentemot andra områden. På frågan om kommunen söker satisfierande lösningar så säger han att så inte alltid är fallet och ger exemplet på brandskydd i skolor där kommunen valde en högre ambitionsnivå än vad lagen kräver och han pekar på att givetvis påverkade det facto att andra skolor inom länet nyligen hade brunnit ned till grunden.

Omvärldsfaktorer
Omvärldsfaktorer spelar in på beslut speciellt när det sker i en närhet berättar han.”Det är svårt att få gehör för något som vi tror skall hända

Om det sker händelser i kommunens närhet så är det lättare att motivera och han ger exemplet utbrottet av bakterier i dricksvattnet som skedde i Östersund nyligen. Motivationen att satsa resurser på en reningsanläggning är nu högre än före incidenten.

Kulturen
Kulturella faktorer spelar in beslut det här att med att ”det händer inte oss”, men han säger andra faktorer spelar in. Att kommunen hittills har förskonats de problem som finns i andra delar av Sverige när det gäller hot, våld och skadegörelse gör att det råder ett öppet klimat inom kommunen.

Organisationsstruktur
Han säger också att kommunen ligger lite efter när det gäller organisering som skulle passa säkerhetsarbete bättre, med exempelvis en säkerhetschef på samma nivå som förvaltningschef direkt underställd kommunstyrelsen som i en närliggande kommun, vilket skulle underlätta arbetet avsevärt och kunna verka övergripande. Kommunens byråkrati påverkar inte negativt utan han upplever det går snabbt enligt få upp beslut i kommunstyrelsen så länge ärendet är välmotiverat och av vikt.

4.3.4 Informationssäkerhet och risk

Det pågår en risk och sårbarhetsanalys inom kommunen för närvarande där oönskade händelser och risker kartläggs och resultatet kommer vara vägledande för vilka av säkerhetsområdena som kommunen behöver arbeta med framöver och hittills har data och it legat högst som oönskad händelse. Ingen medveten riskhantering sker idag utan det handlar mer om att ta smällen när den kommer.

4.3.5 Kommentarer till rapport från MSB

Han tycker att rapporten från MSB och den bild som den beskriver stämmer in rätt väl på kommunen och säger att det på många ställen processen stannar upp och när kommunen då startar up igen så är de tillbaka på ruta ett. Vad gäller katastrofplan och kopplingen på informationssäkerhet så säger han att kommunen har en organisation för att hantera katastrofer men att planer för allt inte finns. Någon kontinuitetsplan som innefattar kommunens informationssäkerhet finns inte men om kommunen skulle hamna i ett krisläge kommer organisationen för att hantera kriser att aktiveras. Dock finns ingen plan om prioriterade system och informationssäkerhet idag.

Att det saknas ingångsvärden för prioriterade system håller han med om försvårar för IT-avdelningen att förbereda sig och snabbt komma igång efter avbrott. Han menar att dessa ingångsvärden kommer att rapporteras in när krisen redan är ett faktum som det ser ut nu. Tankar om att ta fram dessa värden och styrdokument finns hos de som arbetar med säkerhet men har stannat upp i kommunen.

Orsaken till att det ser ut som det gör hänger ihop med en historik av lågt intresse tidigare av höga tjänstemän som inneburit att de som arbetat med säkerhet inte getts möjlighet att informera kommunledningen. Det är givetvis också en resursfråga men framförallt bristen på kunskap hos ledningen om vikten av dessa förberedelser.

Ansvaret att ta fram kontinuitetsplaner och katastrofplaner ligger säkerhetsgruppen genom säkerhetssamordnare och informationssäkerhetssamordnare tillsammans med det nätverk av säkerhetsombud ute i respektive verksamhet. Idag har det blivit så att verksamheterna prioriterar bort informationssäkerhet gentemot andra områden mycket beroende på att det inte finns direkta lagkrav och då kan verksamheten fokusera på andra områden i sin verksamhet eftersom de inte bryter mot lagen.

4.4 Intervju 4

Intervju med Kommun B:s samordnare för IT-säkerhet och informationssäkerhet

4.4.1 Bakgrund och allmänt om informationssäkerhet

Enligt respondenten och de dokument jag tagit del av så arbetar Kommun B aktivt med säkerhet och det finns övergripande säkerhetspolicy med underliggande riktlinjer och styrdokument för att hantera säkerhet. Policyn antogs av kommunfullmäktige och samordnar säkerhetsarbetet inom hela den kommunala organisationen. På förvaltning och bolagsnivå integreras säkerhetsarbetet i den befintliga organisationen. Samtliga anställda inom kommun B ska aktivt arbeta för ökad säkerhet och är skyldiga att påpeka de brister till sin överordnade.

I Kommun B är kommunstyrelsen ytterst ansvarig för att säkerhetspolicy efterlevs.
De olika nämnderna är ansvariga för säkerheten i respektive verksamhet och bolagsstyrelsen för säkerheten i de kommunala bolagen. Ledningarna i förvaltningarna och bolagen är ansvariga för att, politiska säkerhetsmål och riktlinjer, förankras och efterlevs i verksamheterna. Säkerhetsgruppen är en samarbetsgrupp i de säkerhetsfrågor som berör förvaltningar och kommunens bolag men ska även arbeta med förebyggande säkerhetsarbete för alla kommunens innevånare. Säkerhetssamordnaren ansvarar för övergripande planering, samordning och uppföljning av interna arbetet med säkerhet och trygghet.

Respondenten i Kommun B arbetar som samordnare för IT-säkerhet och informationssäkerhet på kommunens IT-kontor och är medlem i kommunens säkerhetsgrupp. Gruppen rapporterar deras arbete via säkerhetschef till kommunstyrelse och till förvaltnings- och bolagschefer. Säkerhetsgruppen består av företrädare från räddningstjänsten tillsammans med de tre största förvaltningarna och de två största bolagen . Som stöd för gruppens arbete finns säkerhetshandläggare som utses på varje förvaltning och kommunägt bolag.
Han berättar att han har en teknisk bakgrund inom datateknik och har tidigare arbetat med IT-drifts frågor och har arbetat på sin nuvarande position ca ett och halvt år. Hans erfarenheter av informationssäkerhet kommer från hans tidigare arbete och en kortare utbildning i informationssäkerhet som han genomgått under sin tid vid

kommunen. Han har som uppdrag att ta fram en informationssäkerhetspolicy men mycket arbete kvarstår han beskriver att han arbetar parallellt med andra arbetsuppgifter och har inte den tid han behöver för att ta fram policyn.

Beskrivning av organisationens arbete med informationssäkerhet allmänt
Det finns enligt honom ingen klar övergripande definition av informationssäkerhet inom kommunen och det är lite oklart vem det är som skall ta fram och förmedla denna definition till de olika förvaltningar och bolagen. Det finns inget beslut fattat av kommunledningen ännu.
Arbetet med informationssäkerhet sker inte samordnat och övergripande, det kan se annorlunda ut på olika förvaltningar. Det sker på eget initiativ i så fall att någon ser till att informationen är tillgänglig, korrekt och inte att fel personer tar del av den. När det gäller IT-säkerhet så sker det arbetet från det centrala IT-kontoret för att tillse god IT-säkerhet och idag ligger mycket fokus på den tekniska sidan av säkerhet.

Användning av standards
Kommun B använder sig av standarden BITS i det arbete som inletts med säkra upp de verksamhetssystem som finns idag men mycket arbete återstår.
Vad gäller ansvarsfördelningen så säger säkerhetspolicyn att kommunstyrelsen ytterst ansvarig för säkerhet säkerhetspolicy följs. De olika nämnderna är ansvariga för säkerheten i respektive verksamhet och bolagsstyrelsen för säkerheten i de kommunala bolagen. Ledningen i förvaltningarna och bolagen är ansvariga för att politiska säkerhetsmål och riktlinjer förankras och följs ute i verksamheterna. Säkerhetsgruppen är en samarbetsgrupp i de säkerhetsfrågor som berör förvaltningar och kommunens bolag men ska även arbeta med förebyggande säkerhetsarbete för alla kommunens innevånare.

I kommunens säkerhetspolicy så finns kopplingar och hänvisningar till de lagar som påverkar verksamheter och säkerhetsarbetet, exempelvis:

- Kommunallagen
- Lagen om skydd mot olyckor
- Lagen om kommuners och landstings åtgärder inför och vid extra ordinära händelser i fredstid och höjd beredskap
- Säkerhetsskyddslagen
- Lagen om skydd för samhällsviktiga anläggningar

Eftersom informationssäkerhetspolicyn inte är framtagen ännu finns ingen koppling mot vilka lagrum som kan påverka informationssäkerheten.

Risk och sårbarhet
Säkerhetsgruppen har för något år sedan genomfört en risk och sårbarhetsanalys enligt SBA metoden för störningar av elektroniska kommunikationer. Respondenten säger att det dock saknas risk och sårbarhets analyser som gäller informationssäkerhet utifrån ett samordnat kommunövergripande perspektiv något som han hoppas förändras i och med att informationssäkerhetspolicyn är framtagen.

5 Analys

I analyskapitlet sammanfattar och analyserar jag de viktigaste delarna från reslutatet av undersökningen och kopplar dessa till teorin.

5.1 Övergripande analys mellan kommunerna

När det gäller organisation och ansvarsfördelning av säkerhetsarbetet är det rätt lika mellan de olika kommunerna, det är kommunfullmäktige som fastslår policy, därefter går ansvaret ned i organisationen på förvaltningar och de kommunala bolagen att integrera säkerhetsarbete med den dagliga verksamheten. En central säkerhetsgrupp driver det övergripande säkerhetsarbetet inom olika områden med medlemmar eller i kontakt med medlemmar från olika förvaltningar för att få tillgång till sakkunniga.
En skillnad mellan säkerhetsgrupperna är att i den mindre kommunen finns en informationssäkerhetssamordnare. Det verkar som om Kommun A har bättre grepp om vad informationssäkerhet innebär och det faktum att Kommun B saknar en informationssäkerhetspolicy bidrar detta till den fokus på teknik som Kommun B har. Det verkar dock vara så att i båda kommunerna så är ambitionen i policy och styrdokument större än vad som sker i verkligheten. Mycket arbete verkar återstå när det gäller arbetet med framförallt informationssäkerhet. Andra skyddsområden får större fokus idag som exempelvis skydd mot olyckor och det beror mycket de lagkrav som finns för de olika skyddsområdena.
Beredskap för incidenter av informationssäkerhet varierar mellan de båda kommunerna. Kommun B säger sig inte ha så hög beredskap för incidenter och har mycket arbete kvar. Kommun A säger däremot att deras incidenthantering fungerar .

5.2 Bakgrund och allmänt om informationssäkerhet

Begreppet informationssäkerhet
Det framkom i intervjuerna att när MSB ändrade sin definition från IT-säkerhet till informationssäkerhet i standarden BITS så fick det till konsekvens att innebörden är oklar för många chefer och beslutsfattare.
Ur respondenternas svar går att utläsa följande skillnader.

”… att det handlar om att se till att rätt information och data skall finnas tillgängligt till rätt personer när helst de behöver det och att allt är rätt och riktigt …”. IT-chef Kommun A.

”… alltifrån ärendehantering, sekretessfrågor till fysisk säkerhet och teknisk säkerhet…” Informationssäkerhetssamordnare Kommun A.

” …att kommunen skall kunna verka oavsett situation och miljö…” Informationssäkerhetssamordnare Kommun A.

” … att se till att kommunen har ett stabilt system vad gäller IT-stöd men också en administrativ plan hur problemet skall hanteras, att kommunen är förberedd så att inte hela verksamheten stannar upp helt. Det handlar om att se till att det finns manuella rutiner för att kunna driva verksamheten vidare…” Säkerhetsansvarig Kommun A.

Här beskriver respondenterna med egna ord sin uppfattning om innebörden av begreppet informationssäkerhet. I deras uttalande går det att identifiera de nyanser som speglar deras respektive bakgrund och deras roll i kommunens säkerhetsarbete. IT-chefen speglar, enligt min mening, en teknisk syn och den säkerhetsansvarige en administrativ syn. Informationssäkerhetssamordnaren ligger någonstans mittemellan utifrån den uppdelning som görs enligt SIS HB 550 figur 2.3. Jag ser också kopplingar mot informationssäkerhetskontexten som McFadzean et al., (2007) tar upp och tolkar detta som att innebörden i begreppet inte är vedertaget inom Kommun A.

De gemensamma dragen i respondenternas beskrivning speglar den syn som finns inom situationsteorin Bakka et al, (2006) att en organisation måste anpassa sig efter omgivningen och de förändringar som sker.

IT-avdelningens roll
Haverblad (2006) beskriver att det viktigt att inte isolera risk och säkerhetsmedvetandet till IT-verksamheten utan detta måste finnas på alla nivåer inom organisationen. IT-chefens beskrivning av IT-avdelningens arbete med att på eget initiativ upprätthålla en basnivå för informationssäkerhet utifrån deras förståelse av de olika verksamheterna och den tydliga bild de har av vilka system som krävs för att hålla igång IT-infrastrukturen. Jag tolkar det som att risk och säkerhetsmedvetandet är idag isolerat inom IT-verksamheten som Haverblad (2006) varnar för.

Ett exempel på detta ur empirin:
”det kommer förhållandevis lite krav från verksamheterna så därför försöker IT-avdelningen utifrån sin kännedom vidta åtgärder på eget initiativ för att kunna upprätthålla en basnivå vad gäller IT-säkerhet och informationssäkerhet”. IT-chefen Kommun A

Trots att ansvarsrollerna finns definierade i kommunens instruktion för förvaltningarna, så är situationen som det ser uti citatet ovan. IT-chefen menar att det kan bero på att förvaltningsledningarna inte förstått förändringen från IT-säkerhet till informationssäkerhet.

IT-avdelningen har genom sitt proaktiva förhållningssätt enligt min bedömning alla förutsättningar att klara av en avbrottssituation som MSB (2009) pekar på finns på IT/Driftsnivå. IT-avdelningen försöker utifrån sitt perspektiv göra så mycket de kan men när systemägare inte levererar accepterade avbrottstider för sina respektive system och kommunledningen inte har beslutat vilka informationssystem som anses vara prioriterade kommer IT-avdelningen inte så mycket längre. Ur ett kontinuitetsperspektiv får detta en konsekvens eftersom ansvaret med ta fram instruktioner och styrdokument inte kan slutföras eftersom denna information ligger som grund för att ta fram instruktionerna som rör kontinuitet och drift.
Enligt Von Solms & Von Solms (2004) kan konsekvensen av att verksamheterna inte förstå att informationssäkerhet är en verksamhetsfråga och inte en teknisk fråga innebära att kommunen inte når en fullständig lösning eller att kommunen lägger resurser på fel saker. Respondenternas svar visar på att insikten om detta inte riktigt nått ledningen.

McFadzean et.al.(2007)beskriver hur de olika kontexterna påverkar högsta ledningen. Att kommunen efter att nya lagkrav startade upp arbetet med att ta fram nya dokument och riktlinjer för sina säkerhetsområden visar på hur den politisk/legala kontexten McFadzean et al., (2007) påverkar en organisation. Arbetet som kom igång med att den IT-säkerhetsgrupp som IT-chefen och informationssäkerhetssamordnaren berättar om där arbetsgruppen utan några egentliga resurser lyckades ta fram policy och andra styrdokument som instruktioner för användare och förvaltning men sedan stannar arbetet upp. McFadzean et al., (2007) definierar i sin riskmatris organisationer som tillhör kvadranten *operationell stabilitet*. Vilket i sin tur innebär att dessa organisationer försöker uppnå informationssäkerhet endast genom att tillgodose de lagkrav som finns.

5.3 Ledningen av informationssäkerhet

Prioritering av informationssäkerhet
I intervjuerna har det framkommit att informationssäkerhet inte prioriteras högt av kommunledningen i jämförelse mellan de olika säkerhetsområdena. Det beror framförallt på de lagkrav som de övriga fyra omfattas av också anger tydligt vad som krävs av kommunen. Informationssäkerhet omfattas inte lika tydligt av lagkrav . Eftersom kommunen har en uttalad ambitionsnivå att göra vad lagen kräver och inte mer, betyder det att lite fokus läggs på området informationssäkerhet just nu. Här finns kopplingar mot McFadzean et al.,(2007) när det gäller politisk/legala kontexten och jag tolkar det som att kommunen påverkas starkt av förändringar av lagkrav.

”Den dag MSB ställer upp med skall krav på kommunerna så kommer man att vara tvungen att fokusera mer på området. Idag så tillsätts det för små resurser för att kunna vidareutveckla informationssäkerhetsområdet”. Säger Informationssäkerhetssamordnaren Kommun A

Historiskt har säkerhet varit lågt prioriterat av kommunledningen, det var först efter att nya lagkrav 2004 som arbetet med att ta fram dagens riktlinjer och styrdokument påbörjades och vissa av dessa riktlinjer skall nu

revideras. Här finns kopplingar mot informationssäkerhetskontexten McFadzean et al., (2007) och jag tolkar det som att kommunen inte prioriterar säkerhetsarbetet på grund av att det inte funnit någon reell hotbild mot just kommuner vilket motiverar de små strategiska och operativa insatser för att utreda behovet av informationssäkerhet.
I intervjun med informationssäkerhetssamordnaren framkommer det att medvetenheten generellt om informationssäkerhet har ökat hos de olika verksamheterna men att prioriteringen sjunker ju närmare verksamheten kommer till att avsätta resurser. Detta visar Dhillons, (2007) påstående att när beslut når den operationella nivå brister det i ägandeskapet i frågan.
Att informationssäkerhet uppfattas som abstrakt bidrar enligt respondenterna då åtgärder inom de andra säkerhetsområdena blir så mer konkreta som en stor övning med räddningstjänsten istället för dokument som förvaras i en server hos IT-avdelningen.

Det strategiska värdet av informationssäkerhet
IT och informationssäkerhet anses som strategiskt viktig för att kunna säkerhetsställa informationsflöden i händelse av kriser men också för att kunna hantera mindre störningar och avbrott. Ur en strategisk synvinkel är informationssäkerhet viktig för kommunen för att det handlar om trovärdigheten för kommunen och dess informationssystem. Förståelsen för det strategiska värdet av informationssäkerhet finns framförallt hos medarbetare inom IT-avdelningen. Förhoppningsvis kommer frågan upp på agendan hos förvaltningscheferna under året.
Min fallstudie visar att kommunen använder sina informationssystem för att stötta sin verksamhet och effektivisera processer och administration, inte för att skapa konkurrensfördelar, detta förklarar enligt McFadzeans et al., (2007) nivån på engagemanget för informationssäkerhet. Utifrån riskmatris i figur2.7 (ibid.) tyder jag detta som att kommunen kan placeras i kvadranten operationell stabilitet och då kommer inte resurser i någon större omfattning att prioriteras till detta arbete.

Informationssäkerhet kopplat mot organisationens mål, visioner och strategi
Respondenterna beskriver att det idag finns väldigt liten koppling mellan informationssäkerhet och kommunens övergripande mål och strategier. Det kan skymtas en aning i kommunens mål att vara en uthållig kommun men annars lyser säkerhet och informationssäkerhet med sin frånvaro. Här finns kopplingar till Dhillon, (2007) och analogin om stekta ägget, figur 2.2, eftersom jag tolkar att det idag inte finns tillräcklig sammanlänkning eller alignment mellan det formella, informella och tekniska systemen inom kommunen. I intervjuerna har det framkommit att säkerhet och informationssäkerhet behöver bli en del i vardagen och införlivas i verksamhetsplaner och redovisas utifrån de strategiska målen. Detta visar också McFadzeans et al., (2007) där de startegiska och operativa insatserna som analys av informationssäkerhetsbehoven omfattar kopplingen mellan informationssäkerhet och organisationens mål.
Jag tolkar det som att innebörden av dessa inte är något som är klart inom kommunen idag. Ett annat tecken på detta är planeringsprocessen för informationssäkerhet, som Whitman & Mattord, (2007) beskriver där mål, visioner och strategier bryts ned till kontinuitetsplaner och riskanalyser för att kunna uppfylla dessa, inte är vedertaget inom kommunen.

5.4 Informationssäkerhet och beslutsfattande

I min fallstudie har jag inte fått fram att beslutsprocessen runt informationssäkerhetsfrågor skulle skilja sig mot beslutsprocesser i andra frågor. Respondenterna svar pekar på att det handlar om beslutsförfaranden som påminner om Simons administrativa människa, Simon, (1997). Min tolkning är det sker med en nivå av begränsad rationalitet som både March, (1994) och Simon, (1997) pekar på. Utifrån Brunssons i Czarniawska, (1998) resonemang om irrationalitet kan jag se att Kommun A visar drag av irrationalitet främst på grund av att de inte tagit fler beslut och tolkar det som att ledningen inte vill ta i frågan och ägandet av frågan informationssäkerhet inte är tydlig som Dhillon, (2007) påpekar.

Kunskap hos ledningen
Samtliga respondenter svarar att kunskapen om informationssäkerhet inte så hög som vore önskvärt och informationssäkerhet är något som upplevs, främmande och ogripbart, samt något som IT-avdelning ansvarar för. Återigen syns kopplingar mot ägarskap av frågan informationssäkerhet och kopplingen att administrativa beslut som rör informationssäkerhet kräver kunskap om de processer och strukturer som krävs för att uppnå god informationssäkerhet Dhillon, (2007) men också ändringen av definitionen i BITS standarden. Jag tolkar detta som att kommunledningen inte besitter den nödvändiga kunskapen.

Omvärldsfaktorer
I intervjuerna har det framkommit att givetvis spelar omvärldsfaktorer in på beslut, framför allt hur pass snabbt beslutet tas och vilka resurser som avsätts. Sker händelser i kommunens närområde så får det betydelse för beslut. Kommun A är lyckligtvis förskonad av de hot risker som kommuner i andra delar av landet drabbats av. Kommunen och dess omvärld kan betecknas som stabil och heterogen samt mindre fientlig som beskrivs av Mintzberg, (1983) men det är tydligt att kontextuella omgivningsfaktorer och informationssäkerhetsfaktorer som beskrivs av McFadzean et. al., (2007) inte fått genomslag i kommunen eftersom de inte kommit igång med att ta fram en informationssäkerhetsstrategi.

Kulturen
Den kultur som finns inom kommunen med en öppenhet, och till viss del naivitet, och oförmåga att inse värdet av sin information och andratillgångar bidrar till att prioriteringen av informationssäkerhet är låg. Därför har få beslut om informationssäkerhet tagits. Detta kan förklaras av att den omvärld som kommunen verkar i inte är så osäker och fientlig som Mintzberg, (1983) pekar på. Kommunen har inte utvecklat sin säkerhetskultur tillräckligt som Dhillon, (2007) menar som en informell skyddsåtgärd.

Organisationsstruktur
Kommunens byråkrati kunde ha påverkat negativt men istället upplevs den av respondenterna som något positivt. Kommunens olika typer av verksamheter innebär en vidd av säkerhetsfrågor och behov som spänner över ett spektrum av åtgärder för att kunna säkerhetsställa att verksamheten kan bedrivas. Vad gäller själva säkerhetsorganisationen så beskriver respondenterna att det är nödvändigt med en person som driver informationssäkerheten övergripande i hela kommunen. Behovet att ha en särskilt utsedd säkerhetschef istället för att som idag kommunchef, tillika säkerhetschef, skulle förmodligen innebära att mer fokus skulle läggas på säkerhetsfrågor i kommunen. Att inte ge informationssäkerhetssamordnare mandat och medel för att kunna utföra sitt arbete anses enligt Von Solms & Von Solms, (2004) som en av de tio dödsynder för informationssäkerhet en organisation kan göra och här bryter kommunen mot den tionde dödsynden.

5.5 Informationssäkerhet och risk

Riskhantering och riskstrategier
Kommunen har idag ingen övergripande strategi för att hantera IT-relaterade risker men en riskanalys pågår och kommer att presenteras i en slutrapport. Detta visar början av en riskhanteringsprocess och kommer att leda till en åtgärdsplan och underlag för att begära resurser för att genomföra dessa åtgärder.
Att det inte finns någon vedertagen riskstrategi idag beror på att kommunen inte vet vilka risker och hot som finns i varje verksamhet, eftersom ingen övergripande riskanalys tidigare genomförts, detta kan förklaras av den låga riskmedvetenheten historiskt. Här finns direkta kopplingar mot de områden som McFadzean et al., (2007) pekar på för att utveckla en informationssäkerhetsstrategi där riskanalys är första steget. Ledningen hade kunnat begära en riskanalys men som säkerhetsansvarige uttrycker det så behöver säkerhet också komma in i verksamheternas planering, idag syns det i princip inte alls i deras verksamhetsplaner, varje säkerhetsområde behöver införlivas som en naturlig del i arbetet/planen och redovisas årligen utifrån kommunens strategiska målen. Kopplingen mot organisationens mål är också en viktig del i utvecklandet av informationssäkerhetsstrategi (ibid.). En riskanalys är också ett bra kommunikationsverktyg för ledningen och medarbetare som Baskerville, (1991b) pekar på .
Sammanfattningsvis visar detta att, uppfattning av risk som McFadzeans et al., (2007) i sin riskmatris, är låg hos kommunens ledning och därmed kunna vara en förklaring till det låga engagemanget. Kommunen kan placeras i kvadranten operationell stabilitet. Det skulle kunna förklara det låga engagemanget och den låga budgeten för informationssäkerhet.

Kontinuitetsplanering
Idag finns ingen övergripande kontinuitetsplan, inte heller någon IT-kontinuitetsplan som (Haverblad, 2006) eller Whitman & Mattord (2007) beskriver, vilket dels förklaras av det historiskt låga intresse kommunledningen haft tidigare för säkerhetsfrågor samt att nödvändiga ingångsvärden i form av accepterade avbrottstider för prioriterade informationssystem väntas komma först då krisen väl är ett faktum. Kommunens IT-avdelning saknar idag nödvändiga ingångsvärden och lista över de IT-system som är prioriterade. De kan därför inte gå vidare med någon dokumenterad IT-kontinuitetsplan som beskrivs av Haverblad (2006), endast lösrykta dokument och mental beredskap finns idag på IT-avdelningen.

Det kan också vara kopplat till att kommunen inte ännu utvecklat en informationssäkerhetsstrategi som McFadzeans et al., (2007) beskriver och därmed inte fått fokus på kontinuitetsplaner ännu.

Kommentar till MSB rapporten
I intervjuerna har det framkommit att bilden som beskrivs i MSB rapporten stämmer in väl på situationen för Kommun A. Anledningen att det blivit så är det låga intresse tidigare kommunchefer och höga tjänstemän haft. Detta har medfört att kommunen ligger efter när det gäller organisering av säkerhetsarbetet. Insikten ute i verksamheterna om beroendet av IT-stödet varierar men är alldeles för lågt för att vara acceptabelt. Det faktum att kommunen inte råkat ut för större avbrott och kriser bidrar till uppfattningen att hot och risker inte finns. Därför sätts inte fokus på att leverera exempelvis ingångsvärden för accepterade avbrottstider.
På säkerhetssidan har inneburit att arbetet i princip stannat av. Informationssäkerhetssamordnaren har fått ny tjänst som IT-samordnare och eftersom han då fått nya arbetsuppgifter har rollen och arbetet som informationssäkerhetssamordnare stannat upp.
Kopplingen mot McFadzean et al., (2007) finns på flera punkter. De kontextuella faktorer som rör kommunen begränsar de strategiska och operativa insatser som ledningen utför. Att kommunen kan placeras i kvadranten operationell stabilitet gör att ledningen inte har samma fokus som vore nödvändigt att ha om kommunen verkat i en miljö som strategisk osäkerhet.

6 Slutsatser

I detta kapitel redogör jag för de slutsatser och reflektioner för den forskningsfråga som jag sökte svar på i mitt syfte. Samt förslag till vidare forskning.
Min forskningsfråga löd, Hur och varför prioriteras informationssäkerhet som den gör i verksamheter, på detta kan jag nu svara följande: Generellt prioriteras informationssäkerhet lågt ute i de olika verksamheterna, undantaget är dock IT-avdelningen och deras Informationssäkerhetssamordnare. En av anledningarna till den låga prioriteringen är att medvetenhet om vad informationssäkerhet innebär är dålig ute i verksamheterna. Dock har det också ledningens syn stor inverkan på prioriteringen. För att höja den generella medvetenheten om vad informationssäkerhet innebär bör frågan drivas övergripande på kommunchefs nivå.

6.1 Diskussion

Lärdomar
Att skriva denna uppsats har varit otroligt lärorikt och utvecklande. Jag har återuppväckt den vetenskapliga ådran i mig och återigen funnit insikten om hur pass omfattande och svårt det är att skriva ett vetenskapligt arbete. Att skriva själv har sina fördelar och nackdelar, att skriva ensam förenklar förvisso arbetsgången men att skriva ensam innebär att vara just ensam. Ensam med sina tankar och funderingar, det svåraste har nog varit just detta. Så här i efterhand skulle jag inte råda någon att skriva ensam om det inte är absolut nödvändigt och i mitt fall hade jag inget val. Ämnet informationssäkerhet är för många känsligt och det gör att frågor som konfidentialitet och förtroende hos respondenter är av yttersta vikt för att kunna få tillgång till adekvat data. Jag anser att trots dessa svårigheter, har jag just genom att skapa förtroende hos respondenterna och att lova anonymitet, kunnat få fram adekvat information som gjort det möjligt att nå fram till ett godtagbart resultat.

6.2 Bakgrund och allmänt om informationssäkerhet

Kommun A har etablerade riktlinjer och en policy som behandlar informationssäkerhetsområdet men dessa är inte tillräckligt förankrade inom organisationen och har inte blivit levande. Informationssäkerhetskontexten är således under utveckling där kommun A endast inlett arbetet. Mycket av detta beror på att innebörden av begreppet informationssäkerhet kontra det tidigare begreppet IT-säkerhet inte har klarnat hos de olika verksamheterna. De har därför inte förstått att ansvaret för informationssäkerhet ligger hos dem och inte på IT-avdelningen som IT-säkerheten tidigare gjorde. IT-avdelningen gör enligt min bedömning, genom ett proaktivt förhållningssätt, så mycket de kan. Detta har lett till att den riskmedvetenhet, rörande informationssäkerhet, som finns i kommunen har isolerats till IT-avdelningen. Av analysen framgår också att det är framförallt med att öka medvetenheten hos alla anställda och skydd via tekniska lösningar som kommunen arbetar idag.

6.3 Ledningen av informationssäkerhet

I Kommun A förekommer en skillnad vad gäller resursfördelning mellan de olika säkerhetsområdena, något som skett på grund av omedvetenhet istället för ett medvetet val. Skillnaden mellan prioritering av kommunens olika säkerhetsområden förklaras främst av skillnaden i lagkrav på kommunen där krav på god informationssäkerhet inte lika tydligt ställs utan det handlar mer om rekommendationer och föreskrifter. Den politisk/legala kontexten är den kontext som jag ser varit mest betydande för utvecklingen av informationssäkerhet så här långt.

Därför ser jag det som ytterst viktigt att kommunchefen visar engagemang för att driva frågan. För att få förståelse hos verksamheterna behöver informationssäkerhet behandlas på kommunchefsnivå ur ett helhetsperspektiv uppifrån istället för gräsrotsperspektiv underifrån som görs idag genom säkerhetsombud vilket inte har fungerat. Att det är nödvändigt att göra informationssäkerhet en del av vardagen och införliva den i planeringen av verksamheten men då krävs också tydlig koppling mot kommunens vision, mål och strategier

eftersom den kopplingen nu är svag. Kopplingen mellan det informella, formella och tekniska systemet behöver ses över.

Då Kommun A enligt riskmatrisen kan sägas verka i operationell stabilitet och använder informationssystem för att stödja och effektivisera sina verksamhetsprocesser och administration, det strategiska värdet är lågt, och uppfattningen av risk också låg.

Av analysen framgår också att den organisatoriska kontexten påverkar också hur informationssäkerhet prioriteras och mest tydligt är att kommunen hittills varit förskonad allvarliga incidenter och kriser samt att det råder en kultur där det mesta är offentlig handling och öppet och tillgängligt för kommunens innevånare bidrar till att prioritering av informationssäkerhet är låg.

Organisationsstrukturen, framför allt organiseringen av nuvarande säkerhetsgrupp och placering av informationssäkerhetssamordnaren är inte optimal utan bör ses över.
I jämförelse med Kommun B med en säkerhetschef så borde Kommun B ha kommit längre med sitt informationssäkerhetsarbete än vad de hittills ha gjort så svaret verkar ligga i att ha en utsedd person som driver informationssäkerhetsfrågor övergripande inom kommunen. Kanske kan en kombination av Kommun A och Kommun B vara mest lämplig. En informationssäkerhetssamordnare som arbetar centralt och övergripande och direkt underställd säkerhetschef.

6.4 Informationssäkerhet och beslutsfattande

Själva beslutprocessen kring informationssäkerhetsfrågor är inte annorlunda än inom andra områden men informationssäkerhet upplevs som komplext och svårt att greppa av kommunledningen. Det är framförallt okunskap och oförmåga att se vilka konsekvenser som brister i informationssäkerhet medför som gör att resurser inte satts av men också bristen på ägarskap för informationssäkerhetsfrågan. Förutom detta så finns ett ointresse från tidigare kommunledning som inneburit att säkerhet generellt fått litet utrymme vilket har påverkat riskmedvetenheten men förhoppningsvis skall detta förändras då säkerhet skall tas upp av förvaltningschefsgruppen i år.

6.5 Informationssäkerhet och risk

Kommun A har inte kommit igång med en övergripande katastrof och kontinuitetsplanering och inte heller någon IT-kontinuitetsplan även om IT-avdelningen har på eget initiativ vidtagit vissa åtgärder i form av exempelvis alternativt driftställe. Eftersom övergripande risk och sårbarhetsanalys pågår och väntas resultera i hotbild och riskidentifiering inom alla säkerhetsområden beräknas arbetet med kontinuitetsplanering påbörjas efter att denna analys är klar. Kommun A är alltså i början av sitt säkerhetsarbete och har inte kommit igång med alla de nödvändiga strategiska och operativa åtgärder. Om frågan tas upp på förvaltningschefsnivå kommer förhoppningsvis nödvändiga beslut tas och resurser att sättas av.

Slutligen kan sägas att bilden som beskrivs av MSB är mycket trolig beskrivning av situationen för det flesta kommuner i landet. Trots svårigheten att generalisera från ett så begränsat material som en fallstudie innebär. Med mitt arbete har jag kunnat bidra med ny kunskap, ett möjligt varför, till det som presenteras i MSB rapporten vilket är mitt bidrag till forskningen kring informationssäkerhet.

6.6 Reflektioner

Att informationssäkerhet skulle vara ett område som inte prioriterades högt hos kommunen med tanke på det värde som finns i dess informationstillgångar är något förvånande. Att MSB som myndighet inte ställer högre krav på kommuner generellt var också oväntat. Det är så tydligt att kommunen inte vill bryta mot lagen och därför kommer de att vidta åtgärder för komma till rätta med brister om sådana påvisas. Därför borde MSB kunna göra mer för att påverka förändringar i lagstiftningen inom området, för att på så sätt tvinga kommuner att

vidta ytterligare åtgärder. Alternativt ställa högre krav på kommuner och andra myndigheter att tydligare redovisa sitt arbete med informationssäkerhet.

Med tanke på den omgivning som en kommun verkar i och som inte karaktäriseras som en fientlig och särskilt föränderlig miljö så borde etableringen av en hotbild och risker kunna vara förhållandevis enkelt att fastställa . Att innebörden av själva begreppet informationssäkerhet skulle vara av så central betydelse för att driva frågan på ledningsnivå visar på att det är av yttersta vikt att höja medvetenhet med denna som utgångspunkt.

Att kunna bedriva informationssäkerhetsarbete ur ett minimalistsikt perspektiv och endast ta fram styrdokument och riktlinjer för att följa myndighetens rekommendationer utan att levandegöra dessa dokument genom att förankra dem hos medarbetare och införliva dem i organisationens kultur inte är tillräckligt för att garantera god informationssäkerhet. Att inte förstå att det krävs så mycket mer arbete än att bara ta fram olika dokument är att lura sig själv.

Med tanke på att kommuners riskuppfattning och den strategiska vikt förmodligen i framtiden kommer att vara låg och därmed de resurser och insatser som kommer att läggas på informationssäkerhet inte vara betydande. Detta kan ju förändras med tanke på utvecklingen av elektroniska tjänster som kommuner i framtiden kan tänka sig använda sig av för att öka deras service till sina medborgare. Då skulle också den strategiska vikten av deras IT-system förändras.

6.7 Fortsatt forskning

Eftersom behovet av informationssäkerhet i framtiden som jag ser det bara kommer att öka efterlyser jag ytterligare forskning som belyser följande:

- *Är det möjligt att bedriva minimalistiskt informationsarbete ur ett helhetsperspektiv och hur i så fall?*
- *Vad kommer användningen av e-tjänster att få för följd för kommuners infromationssäkerhetsarbete?*

Det skulle också vara intressant om någon gick i mina fotspår och gjorde om min egen studie med enbart beslutsfattare som respondenter.

Begreppsförklaring

Ordlista hämtad från Terminologi för informationssäkerhet. SIS HB 550 Utgåva 3.

hot	möjlig, oönskad händelse med negativa konsekvenser för verksamheten
hotanalys	identifiering av vilka hot som kan finnas och vem eller vad som kan tänkas utlösa dessa hot, samt vilka resurser samt vilken tid och kompetens som angriparen kan tänkas disponera
hotbild	uppsättning hot som bedöms föreligga mot en viss (typ av) verksamhet
informationssäkerhet	säkerhet för informationstillgångar avseende förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet även ansvarighet och oavvislighet.
informationstillgångar	en organisations informationsrelaterade tillgångar
IT-säkerhet	säkerhet beträffande IT-system med förmåga att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling samt dator- och telekommunikation
katastrofplanering;	planering och förberedelser nödvändiga för att minimera förlust och säkra driften av kritiska delar av verksamheten i händelse av exceptionellt allvarlig störning
återställningsplanering	
kontinuitetsplan	dokument som beskriver hur verksamheten skall bedrivas när identifierade, kritiska verksamhetsprocesser allvarligt påverkas under en längre, specificerad tidsperiod
konsekvens; påverkan	resultat av en händelse med negativ inverkan
risk	kombination av sannolikheten för att ett givet hot realiseras och därmed uppkommande skadekostnad
riskanalys	process som identifierar hot mot verksamheten och uppskattar storleken hos relaterade risker
riskhantering	samordnade aktiviteter för att identifiering, styrning och kontroll av risk
skadekostnad	sammanlagt värde av ett angrepps konsekvenser
skydd	effekt av handlingar, rutiner och tekniska arrangemang som syftar att minska sårbarheten
skyddsåtgärder	handling,rutin eller tekniskt arrangemang som, genom att minska att sårbarheten möter ett identifierat hot
svaghet	brist i skyddet av en tillgång exponerad för hot
säkerhetskontroller	identifierad uppsättning skyddsåtgärder för att möta en organisations risker
säkerhetspolicy	generella krav på säkerhetsåtgärder eller handlingsregler för en organisation eller verksamhet
tillgång	allt som är av värde för organisationen

Referenser

Böcker:

Bakka, Fivesdal, Lindkvist., Organisationsteori: struktur –kultur -processer, femte uppl, 2006

Churchman,C.W, Systemanalys,1968,svensk översättning 1973

Czarniawska (red), Organisationsteori på svenska,1998

Fayol, Henri, Industriell och allmän administration, 1916 översatt 2008

Dhillon, Gurpreet, Principles of Information Systems Security, Text and Cases, 2007

Haverblad, Angelica, IT ur ett affärsperspektiv, 2006

Holme & Solvang, Forskningsmetodik, 1997

Jacobsen & Thorsvik, Hur moderna organisationer fungerar, 1995

Lundahl & Skärvad, Utredningsmetodik för samhällsvetare och ekonomer. 1999

March, James G, A primer to decision making, 1994

Mintzberg, Henry, The nature of managerial work, 1973

Mintzberg, Henry, Structures in fives, designing effective organizations, 1983

Scroderbek et.al, Management Systems, Conceptual Considerations Fourth Edition, 1990

Simon , Herbert A, Administrative Behavior Fourth Edition,1997

SIS HB 550 Utgåva 3, Terminologi för informationssäkerhet, 2007
Whitman. M & H.Mattord, Manangement of informationsecurity, Second Edition, 2008

Whitman.M & H.Mattord, Principles of incident response and disaster recovery, Second Edition, 2007

Whitman.M & H.Mattord, Principles of informationssecurity, Second Edition (2005).

Yin,Robert, Fallstudier: design och genomförande, 2006

Rapporter:

Samhällets informationssäkerhet lägesbedömning 2009, Myndigheten för samhällsskydd och beredskap

Avhandlingar:

Ocsarson, Per, Informationssäkerhet i verksamheter
- begrepp och modeller som stöd för förståelse avinformationssäkerhet och dess hantering i verksamheter,2001

Referenser

Artiklar:
Baskerville, Richard, Risk analysis as a source of professional knowledge, 1991a, Computers & Security, 10(1991) 749-764

Baskerville Richard, Risk analysis: an interpretive feasibility tool in justifying information systems security, 1991b, European Journal of Information Systems. Vol. 1, No. 2, pp. 121-130, 1991

Dhillon, Gurpreet, Challenges in managing information security in the new millennium, Information security management: global challenges in the new millennium, 2001

Dhillon & Backhouse, Information System Security Management in the New Millennium,2000 Communication of the ACM July 2000/Vol. 43, No. 7 ,125-128

Gerber & Von Solms, Management of risk in the information age, 2004 Computers & Security (2005) 24, 16, 30

McFadzean, Ezingeard , Birchall, Perception of risk and the strategic impact of existing IT oninformation security strategy at board level,2007 Online Information Review Vol. 31 No. 5, 2007pp. 622-660 Emerald Group Publishing Limited

Van Niekerk JF, Von Solms R, Information security culture: A management perspective, Comput. Secur. (2009), doi:10.1016/j.cose.2009.10.005

Von Solms & Von Solms, The 10 deadly sins of information security management, Computers & Security (2004) 23, 371,376

Figur guide:

Bilaga 1 Utdrag från rapporten från MSB

Samhällets informationssäkerhet
Lägesbedömning 2009

Kapitel 6 s.53-55

6.2.5 Offentlig verksamhet

6.2.5.1 Kontinuitetsplanering

Inom ramen för arbetet med lägesbedömningen utreddes hur kontinuitetsplanering hanteras i kommuner. Stora brister påvisades och de största är relaterade till planeringen för hur verksamheterna arbetar med att motverka och agera vid oplanerade avbrott. Brister i kommunernas kontinuitetsplanering har även konstaterats i det löpande arbetet som bedrivits av KBM respektive MSB, exempelvis vid aktivt stöd från myndigheten för att driva planeringsprocessen, samt i samband med länsstyrelsernas utbildning i informationssäkerhet riktad mot kommuner.

Inom kommunerna finns i de flesta fall policydokument med definierade ansvarsroller och inriktning för hur arbetet med informationssäkerhet ska genomföras. Policydokumenten ger dock som regel ingen direkt ledning vad gäller kontinuitetsplaneringens omfattning. Inte i något fall har ledningen angett om det finns särskilda skäl att upprätta en katastrofplan. Dessutom saknas som regel inriktning för hur kontinuitetsplaneringen ska samordnas mellan ledning, verksamhet och IT-stöd. Ansvaret för att hantera avbrott ligger tydligt i linjeorganisationen men samtidigt saknas insikten om hur beroende den egna verksamheten är av IT-stödet. Olika ansvarsroller gällande informationssäkerhet finns definierade men i flera fall är innebörden oklar, detta gäller särskilt systemägarrollen.

Kommunen måste fungera även om det uppstår en störning i form av ett avbrott. Därför är det viktigt att identifiera vilka verksamheter i kommunen som är helt nödvändiga för att kunna undvika oacceptabla konsekvenser för medborgarna. I de flesta kommunerna har planeringsprocessen för att hantera avbrott påbörjats. Förankrade och fastställda acceptabla avbrottstider för verksamheterna är avgörande ingångsvärden för kontinuitetsplaneringen när det gäller kommunens viktigaste IT-system. Dessa värden saknas i många av de kartlagda kommunerna. Beräkning av avbrottstid baseras exempelvis på vilken servicenivå som ska upprätthållas vid ett avbrott, kritiska tidpunkter eller hur den extra arbetsanhopningen efter ett avbrott ska hanteras. I vissa fall har avbrottstider bestämts utan dessa ingångsvärden.

Planering för hur verksamheterna ska kunna bedrivas vid ett avbrott med hjälp av olika reservrutiner för informationshantering saknas genomgående. Arbetet har inte påbörjats eller genomförts vid någon av de tio besökta kommunerna. Brist på reservrutiner medför att risken för att flera viktiga samhällsfunktioner inom kommunen kan få en väsentligt lägre servicenivå gentemot allmänheten i händelse av oplanerade avbrott. Beroende på när i tiden ett avbrott inträffar kan konsekvenserna öka. Bedömning av genomförbarheten i verksamheternas reservrutiner är grunden för att kunna avgöra om servicenivån är acceptabel eller inte.
På IT/driftnivån finns i de flesta fall förutsättningar för att hantera en avbrottssituation. Svagheterna är att befintlig systemdokumentation inte är sammanhållen eller helt aktuell, därutöver finns svårigheter att hantera personberoendet. Kontinuitetsplaner finns i de allra flesta fall på IT/driftsnivå. Dessa är dock inte koordinerade med verksamheternas krav i de fall nödvändiga ingångsvärden från verksamheterna saknas.
Det finns stora svårigheter att hålla planeringen aktuell samt att få kontinuitet i hela planeringsprocessen. Vid de besökta kommunerna har vid flera tillfällen processen startats upp men successivt tappat fart. Omtag görs då i planeringen vilket i många fall leder till att tidigare erfarenheter och kunskaper inte beaktas i planeringsprocessen.

Bilaga 2 Intervjuguide

Frågor till informationssäkerhetssamordnaren

Bakgrund

1. Hur länge har du varit informationssäkerhetssamordnare?
2. Din bakgrund, erfarenhet och utbildning inom informationssäkerhet?
3. Förklara rollen som informationssäkerhetssamordnare?

Informationssäkerhet

4. Du är som informationssäkerhetssamordnare ansvarig för att driva informationssäkerhetsfrågan i kommunens vad innebär begreppet informationssäkerhet för dig?
5. Upplever du att informationssäkerhet är ett komplext problem och i så fall på vilket sätt?
6. Ur en strategisk synvinkel hur pass viktigt är det för kommunen med informationssäkerhet?
7. Vad låg till grund när kommunen tog fram informationssäkerhetspolicy och övriga styrdokument?
8. Vilken respons får du för dina argument i kontakten med de olika förvaltningarna/bolagen?
9. Vilken är din uppfattning om hur kunskapen och medvetenhet om informationssäkerhet är bland chefer för de olika verksamheterna?
10. Informationssäkerhet har många olika dimensioner vilka anser du är viktigast för er?

The Strategic/Corporate Governance Dimension; The Governance/Organisational Dimension; The Policy Dimension; The Best Practice Dimension; The Ethical Dimension; The Certification Dimension; The Legal dimension; The Insurance Dimension; The Personnel/Human Dimension; The Awareness Dimension; The Technical Dimension; The Measurement/Metrics (Compliance monitoring/Real time IT audit) Dimension; The Audit Dimension.

11. Ansvaret för informationssäkerhet ligger på respektive verksamhet men vad är din bild av insikten hos de olika verksamheterna om deras beroende av IT-stöd ser ut?
12. Hur kommer det sig att den övergipande informationssäkerheten ligger under IT-avdelningens ansvar?

Ledning av informationssäkerhet

13. Vad är din bild om hur kommunledningen ser på informationssäkerhet?
14. Hur avspeglar sig kommunens övergripande mål, vision och strategier i arbetet med informationssäkerhet enligt din mening?
15. Enligt kommunens säkerhetspolicy skall kommunens alla informationssystem uppfylla minst BITS Basnivå. Hur ser du på att använda standards för att säkerhetsställa informationssäkerhet?
16. Ledning av informationssäkerhet kan delas in på planering, policy, program, personal, skydd och projektledning vilka av dessa områden arbetar ni aktivt med idag?
17. Upplever du att chefer inom verksamheterna själva tar informationssäkerhet på allvar och på vilket sätt?
18. Vilka är enligt dig de största utmaningarna för dig som samordnare för att få en fungerande informationssäkerhet inom organisationen?
19. Hur ser du på ledarskapets roll för att skapa och upprätthålla god informationssäkerhet?
20. Anser du att det idag sätts av tillräckligt med resurser för säkerhet i allmänhet och informationssäkerhet i synnerhet?
21. Hur följer ni upp och mäter informationssäkerhet idag?
22. Hur påverkar detta kommunens nivå av informationssäkerhet idag?

Beslut

23. Hur hanteras beslut som rör informationssäkerhet inom kommunen?
24. Skiljer sig processen åt jämfört med andra områden?
25. Hur spelar kommunens mål, strategier visioner in vid beslut som rör informationssäkerhet?
26. Hur mycket spelar politiska faktorer in?
27. Hur mycket spelar omvärldsfaktorer in?
28. Vilka omvärldsfaktorer tar ni hänsyn till vid beslut i frågan?
29. Hur spelar informationssäkerhetens något komplexa natur in på beslut?
30. Hur påverkas ni som beslutsfattare av vidden på området informationssäkerhet när det gäller informationsinhämtning och behandling av den samma?
31. Hur utvärderas konsekvenser för informationssäkerhet?
32. Hur utvärderas alternativa lösningar för informationssäkerhet?
33. Vad är din uppfattning om hur prioriteras informationssäkerhet av kommunen ledning?
34. På vilket sätt mäter ni investeringskostnaden för informationssäkerhet?
35. Vilken roll spelar IT-avdelningen inför beslut som rör informationssäkerhet?
36. Hur följer ni upp beslut som rör informationssäkerhet idag?
37. Vilken roll anser du kulturen har när gäller fatta beslut
38. Hur spelar kommunens organisationsstruktur in på beslut som rör informationssäkerhet?
39. Kommunens byråkrati kan ibland leda till att det tar tid innan beslut fattas och övergår i ren handling vilka effekter kan det få för ett område som informationssäkerhet?

Risk och sårbarhet

40. På vilket sätt utvärderas hot, risker och sårbarheter inom kommunen idag?
41. Hur pass riskpräglad är kulturen inom kommuner anser du?
42. Hur skulle du beskriva kommunledningens riskmedvetenhet när det gäller säkerhet generellt inom kommunen?
43. Hur skulle du beskriva riskmedvetenheten när det gäller informationssäkerhet?
44. Hur kan detta ha påverkat beslut som rör informationssäkerheten?
45. I rapporten Samhällets informationssäkerhet ges en bild av läget för informationssäkerhet inom kommuner, hur väl stämmer den in på er?
46. Vilka risker ser du idag som allvarligast när det gäller kommunens informationssäkerhet?
47. Har ni idag vidtagit någon medveten strategi för att hantera risker som rör informationssäkerhet?
48. Hur ser er kontinuitetsplanering ut idag när det gäller informationssäkerhet?
49. Vilka faktorer anser har störst inverkan för att förklara den situation som råder när det gäller?
50. Hur ser du på utvecklingen av kommunens informationssäkerhet framöver vilka är viktigaste stegen framöver?

Frågor till Säkerhetsansvarig

Bakgrund

1. Hur länge har du lett säkerhetsgruppen?
2. Din bakgrund, erfarenhet och utbildning inom informationssäkerhet?
3. Förklara säkerhetsgruppens roll och din roll att leda den?

Informationssäkerhet

4. Säkerhetsgruppens skall bland annat driva informationssäkerhetsfrågan i kommunen vad innebär begreppet informationssäkerhet för dig?

5. Upplever du att det görs skillnad på de olika säkerhetsområdena i form resurstilldelning?
6. Vilken respons får du för dina argument i kontakten med kommunens ledning?
7. Ur en strategisk synvinkel hur pass viktigt är det för kommunen med informationssäkerhet?
8. Vad låg till grund när kommunen tog fram informationssäkerhetspolicy och övriga styrdokument?
9. Vilken är din uppfattning om hur kunskapen och medvetenhet om informationssäkerhet är bland chefer för de olika verksamheterna?
10. Informationssäkerhet har många olika dimensioner vilka anser du är viktigast för er?

The Strategic/Corporate Governance Dimension; The Governance/Organisational Dimension; The Policy Dimension; The Best Practice Dimension; The Ethical Dimension; The Certification Dimension; The Legal dimension; The Insurance Dimension; The Personnel/Human Dimension; The Awareness Dimension; The Technical Dimension; The Measurement/Metrics (Compliance monitoring/Real time IT audit) Dimension; The Audit Dimension.

11. Ansvaret för informationssäkerhet ligger på respektive verksamhet men vad är din bild av insikten hos de olika verksamheterna om deras beroende av IT-stöd ser ut?
12. Hur kommer det sig att den övergipande informationssäkerheten ligger under IT-avdelningens ansvar?

Ledning av informationssäkerhet

13. Beskriv hur kommunledningen ser på informationssäkerhet?
14. Hur avspeglar sig kommunens övergripande mål, vision och strategier i arbetet med informationssäkerhet enligt din mening?
15. Enligt kommunens säkerhetspolicy skall kommunens alla informationssystem uppfylla minst BITS Basnivå. Hur ser du på att använda standards för att säkerhetsställa informationssäkerhet?
16. Ledning av informationssäkerhet kan delas in på planering, policy, program, personal, skydd och projektledning vilka av dessa områden arbetar ni aktivt med idag?
17. Upplever du att chefer inom verksamheterna själva tar informationssäkerhet på allvar och på vilket sätt?
18. Vilka är enligt dig de största utmaningarna för dig och säkerhetsgruppen för att få en fungerande informationssäkerhet inom organisationen?
19. Hur ser du på ledarskapets roll för att skapa och upprätthålla god informationssäkerhet?
20. Anser du att det idag sätts av tillräckligt med resurser för säkerhet i allmänhet och informationssäkerhet i synnerhet?
21. Hur följer ni upp och mäter informationssäkerhet idag?
22. Hur påverkar detta kommunens nivå av informationssäkerhet idag?
23. Hur ser du på din egen bakgrund (räddningstjänsten) och vad den kan bidra till katastrofplanering och kontinuitetsplanering

Beslut

24. Hur hanteras beslut som rör informationssäkerhet inom kommunen?
25. Skiljer sig processen åt jämfört med andra områden?
26. Hur spelar kommunens mål, strategier visioner in vid beslut som rör informationssäkerhet?
27. Hur mycket spelar omvärldsfaktorer in?
28. Vilka omvärldsfaktorer tar ni hänsyn till vid beslut i frågan?
29. Hur spelar informationssäkerhetens något komplexa natur in på beslut?
30. Hur påverkas ni som beslutsfattare av vidden på området informationssäkerhet när det gäller informationsinhämtning och behandling av den samma?
31. Hur utvärderas konsekvenser för informationssäkerhet?
32. Hur utvärderas alternativa lösningar för informationssäkerhet?
33. Vad är din uppfattning om hur prioriteras informationssäkerhet av kommunen ledning?
34. På vilket sätt mäter ni investeringskostnaden för informationssäkerhet?
35. Hur följer ni upp beslut som rör informationssäkerhet idag?
36. Vilken roll anser du kulturen har när gäller fatta beslut
37. Hur spelar kommunens organisationsstruktur in på beslut som rör informationssäkerhet?

38. Kommunen byråkrati kan ibland leda till att det tar tid innan beslut fattas och övergår i ren handling vilka effekter kan det få för ett område som informationssäkerhet?

Risk och sårbarhet

39. I rapporten Samhällets informationssäkerhet ges en bild av läget för informationssäkerhet inom kommuner, hur väl stämmer den in på er?
40. Vem ansvarar idag för katastrofplanering och kontinuitetsplanering
41. Hur ser er kontinuitetsplanering ut idag när det gäller informationssäkerhet?
42. På vilket sätt utvärderas hot, risker och sårbarheter inom kommunen idag?
43. Hur pass riskpräglad är kulturen inom kommuner anser du?
44. Hur skulle du beskriva kommunledningens riskmedvetenhet när det gäller säkerhet generellt inom kommunen?
45. Hur skulle du beskriva riskmedvetenheten när det gäller informationssäkerhet?
46. Hur kan detta ha påverkat beslut som rör informationssäkerheten?
47. Vilka risker ser du idag som allvarligast när det gäller kommunens informationssäkerhet?
48. Har ni idag vidtagit någon medveten strategi för att hantera risker som rör informationssäkerhet?
49. Vilka faktorer anser har störst inverkan för att förklara den situation som råder när det gäller?
50. Hur ser du på utvecklingen av kommunens informationssäkerhet framöver vilka är viktigaste stegen framöver?

Frågor till IT-chef

Bakgrund

1. Hur länge har du varit IT-chef?
2. Din bakgrund, erfarenhet och utbildning inom informationssäkerhet?
3. Förklara rollen som IT-chef?

Informationssäkerhet

4. Du är som IT-chef ansvarig för att leverera informationssäkerhet i kommunens vad innebär begreppet informationssäkerhet för dig?
5. Ur en strategisk synvinkel hur pass viktigt är det för kommunen med informationssäkerhet?
6. Vad låg till grund när kommunen tog fram informationssäkerhetspolicy och övriga styrdokument?
7. Vilken är din uppfattning om hur kunskapen och medvetenhet om informationssäkerhet är bland chefer för de olika verksamheterna?
8. Informationssäkerhet har många olika dimensioner vilka anser du är viktigast för er?
    - The Strategic/Corporate Governance Dimension;
    - The Governance/Organisational Dimension;
    - The Policy Dimension;
    - The Best Practice Dimension;
    - The Ethical Dimension;
    - The Certification Dimension;
    - The Legal dimension;
    - The Insurance Dimension;
    - The Personnel/Human Dimension;
    - The Awareness Dimension;
    - The Technical Dimension;
    - The Measurement/Metrics (Compliance monitoring/
    - Real time IT audit) Dimension;
    - The Audit Dimension.

9. Ansvaret för informationssäkerhet ligger på respektive verksamhet men vad är din bild av insikten hos de olika verksamheterna om deras beroende av IT-stöd ser ut?
10. Hur kommer det sig att den övergipande informationssäkerheten ligger under IT-avdelningens ansvar?
11. Vilken roll spelar IT-avdelningen när det gäller informationssäkerhet?

Ledning av informationssäkerhet

12. Beskriv hur kommunledningen ser på informationssäkerhet?
13. Hur avspeglar sig kommunens övergripande mål, vision och strategier i arbetet med informationssäkerhet enligt din mening?
14. Enligt kommunens säkerhetspolicy skall kommunens alla informationssystem uppfylla minst BITS Basnivå. Hur ser du på att använda standards för att säkerhetsställa informationssäkerhet?
15. Ledning av informationssäkerhet kan delas in på planering, policy, program, personal, skydd och projektledning vilka av dessa områden arbetar ni aktivt med idag?
16. Upplever du att chefer inom verksamheterna själva tar informationssäkerhet på allvar och på vilket sätt?
17. Vilka är enligt dig de största utmaningarna för dig som IT-chef för att få en fungerande informationssäkerhet inom organisationen?
18. Hur ser du på din egen roll som chef ledare och vilken typ av ledarskap du bör bedriva för att skapa och upprätthålla god informationssäkerhet
19. Hur ser du andra på andra förvaltningschefers roll för att hjälpa till med detta?
20. Anser du att det idag sätts av tillräckligt med resurser för säkerhet i allmänhet och informationssäkerhet i synnerhet?
21. Hur har de extra medel som MSB tillförde kommunerna för att höja beredskapen haft inverkan på informationssäkerheten och hur i så fall?
22. Vilken avdelning/förvaltning bär kostnaden för informationssäkerheten idag och hur syns kostnaden i kommunens budget?
23. Hur följer ni upp och mäter informationssäkerhet idag?
24. Hur påverkar detta kommunens nivå av informationssäkerhet idag?

Beslut

25. Hur hanteras beslut som rör informationssäkerhet inom kommunen?
26. Skiljer sig processen åt jämfört med andra områden?
27. Hur spelar kommunens mål, strategier visioner in vid beslut som rör informationssäkerhet?
28. Hur mycket spelar omvärldsfaktorer in?
29. Vilka omvärldsfaktorer tar ni hänsyn till vid beslut i frågan?
30. Hur spelar informationssäkerhetens något komplexa natur in på beslut?
31. Hur påverkas ni som beslutsfattare av vidden på området informationssäkerhet när det gäller informationsinhämtning och behandling av den samma?
32. Hur utvärderas konsekvenser för informationssäkerhet?
33. Hur utvärderas alternativa lösningar för informationssäkerhet?
34. Vad är din uppfattning om hur prioriteras informationssäkerhet av kommunen ledning?
35. På vilket sätt mäter ni investeringskostnaden för informationssäkerhet?
36. Vilken roll spelar IT-avdelningen inför beslut som rör informationssäkerhet?
37. Hur följer ni upp beslut som rör informationssäkerhet idag?
38. Vilken roll anser du kulturen har när gäller fatta beslut
39. Hur spelar kommunens organisationsstruktur in på beslut som rör informationssäkerhet?
40. Kommunen byråkrati kan ibland leda till att det tar tid innan beslut fattas och övergår i ren handling vilka effekter kan det få för ett område som informationssäkerhet?

Risk och sårbarhet

41. På vilket sätt utvärderas hot, risker och sårbarheter inom kommunen idag?
42. Hur pass riskpräglad är kulturen inom kommuner anser du?

43. Hur skulle du beskriva kommunledningens riskmedvetenhet när det gäller säkerhet generellt inom kommunen?
44. Hur skulle du beskriva riskmedvetenheten när det gäller informationssäkerhet?
45. Hur kan detta ha påverkat beslut som rör informationssäkerheten?
46. I rapporten Samhällets informationssäkerhet ges en bild av läget för informationssäkerhet inom kommuner, hur väl stämmer den in på er?
47. Hur kan det komma sig att det ser ut som beskrivs i lägesbedömningen?
48. Vilka risker ser du idag som allvarligast när det gäller kommunens informationssäkerhet?
49. Har ni idag vidtagit någon medveten strategi för att hantera risker som rör informationssäkerhet?
50. Hur ser er kontinuitetsplanering ut idag när det gäller informationssäkerhet?
51. Vilka faktorer anser har störst inverkan för att förklara den situation som råder när det gäller?
52. Hur ser du på utvecklingen av kommunens informationssäkerhet framöver vilka är viktigaste stegen framöver?