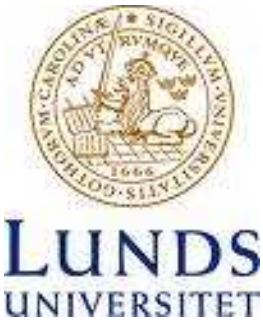


Institutionen för Informatik

Informationsläckor och organisationer

Kandidatuppsats, 15 högskolepoäng, SYSK01 i Informatik

2011-06-08
SYSK01

Författare: Tobias Håkansson 880914
Henrik Johnsson 870923

Handledare: Hans Lundin

Examinator: Agneta Olerup
Markus Lahtinen

Abstrakt

Titel:	Informationsläckors betydelse för organisationer
Författare:	Tobias Håkansson, Henrik Johnsson
Utgivare:	Institutionen för Informatik
Handledare:	Hans Lundin
Examinator:	Agneta Olerup Markus Lahtinen
Publiceringsår:	2011
Uppsatstyp:	Kandidatuppsats
Språk:	Svenska
Nyckelord:	informationsläckage, informationshantering, handlingsplaner

Abstrakt

Informationsläckage har blivit ett allt större problem sedan näringslivet blivit allt mer konkurrenskraftigt. Fenomenet informationsläckage är ett diffust och komplext ämne eftersom det kan ske på många olika sätt vilket gör det svårt för organisationer att skydda sig emot det. Denna undersökning innefattar studier på myndigheterna Lunds Kommun och Försvarsmakten, där vi undersöker vilka handlingsplaner som finns för att hantera och bemöta informationsläckage, samt vilka konsekvenser informationsläckage kan innebära. Tillvägagångssätt har varit att samla in litteratur som varit lämpad för ämnet och passat med vår forskningsfråga. Resultatet visar att våra informanter är medvetna om informationsläckage och förhåller sig till det, samt att de använder sig av handlingsplaner för att bemöta ett informationsläckage, dock i olika utsträckning.

Innehållsförteckning

Figurförteckning

Tabellförteckning

Förord

Vi vill tacka de som har hjälpt oss på vägen att slutföra denna uppsats. Vi vill främst tacka de informanter som ställt upp och deltagit i vår undersökning från Försvarsmakten och Lunds Kommun. Vi vill ge ett särskilt tack till vår kontaktperson på Försvarsmakten, Ross W Tsagalidis, som hjälpt oss på vägen. Vi vill även tacka vår handledare, Hans Lundin, för hans stöd under arbetsprocessen.
Tack!

1 Inledning

Den här uppsatsen ämnar undersöka fenomenet informationsläckage. Vi har valt att undersöka detta ämne eftersom att det är något som ständigt är relevant. Informationsläckage har fått stor uppståndelse sedan Wikileaks publicerade känslig information. Detta fenomen är något som påverkar alla organisationer i högsta grad, så väl positivt som negativt. Vi har däremot valt att fokusera på hur organisationer påverkas negativt av informationsläckage och därför vill vi undersöka det.

1.1 Bakgrund

Information är något som är av stort värde för organisationer samtidigt som det är något av det svåraste att skydda. För organisationer har hotet alltid funnits att information kan avslöjas och spridas. Exempel på informationsläckage kan vara för tidigt läckta årsredovisningar, publikationer eller arbetsdokument som inte bör läckas eller som endast är menat för ”stängda dörrar”. Information som är känslig då den kan skada personer eller organisationer om den läcks. Informationsläckage har alltid varit ett problem i det konkurrenskraftiga näringslivet. Detta i kombination med att tekniken har förbättrats och att information har transformerats från fysisk pappersform till digital form bidrar till att det är lättare att föra vidare informationen till tvivelaktiga mottagare. (Pereira, 2005)

Informationsläckor har fått stort medialt intresse den senaste tiden då ”whistleblower”-organisationen Wikileaks publicerade sekretessbelagd information. Med en ”whistleblower”-organisation menas en organisation som tar emot läckt information och publicerar den för omvärlden (Nationalencyklopedin, 2011). Wikileaks är en icke-vinstdrivande mediaorganisation vars mål är att föra fram viktiga nyheter och information till allmänheten (Wikileaks, 2011). Men för andra organisationer har dessa informationsläckor inneburit förödande konsekvenser, dock har det debatteras om informationsläckorna främjar världen i ett större perspektiv. Exempel på det är information som beskriver hur amerikanska spioner har sålt hemlig information till sovjetiska underrättelsetjänstschefer, vilket har varit en olämplig konsekvens för den Amerikanska regeringen (Gellman & Harrell, 2010).

Det har diskuterats att journalister och organisationer som Wikileaks måste förstå att regeringar och organisationer måste skydda sina informationskällor och sin information. Detta för att om människor med tillgång till känslig information skulle prata offentligt kan

andra människor förlora sina jobb, frihet eller förlora livet. Organisationer eller regeringar kan förlora sina anseenden och trovärdighet. Offentliggörande av hemliga militära planer kan vara förödande för ett lands säkerhet. Medan andra debatterar för att dessa informationsläckor är demokratiska rättigheter som är nödvändiga att släppa. Detta har satt press på att organisationer måste hantera risken för informationsläckage på ett bättre sätt. (Karhula, 2011)

Organisationer och företag hanterar stora mängder information, information som kan vara känslig om den uppdagas av utomstående. Informationsläckage inom organisationer är vanligt. Dessa läckor kan ske genom en s.k. insiderattack. Insiders kan vara nuvarande eller tidigare anställda eller entreprenörer som har eller har haft behörig tillgång till organisationens system och nätverk. De är bekanta med intern policy, procedurer och teknologier och kan utnyttja kunskapen att underlätta attacker och samarbeta med externa hot. Det förekommer att anställda inom en organisation försöker förflytta och avslöja känslig information. (Liu, Zhang, Cui & Wu , 2008) Enligt en global undersökning utförd av Deloitte 2006 (Melek & Mackinnon, 2006) utgör insiderbedrägeri och informationsläckage 28% respektive 18% av interna brott. Interna användare med varierande tillstånd och förmånsnivåer som karaktäriseras av deras position inom organisationen utgör den mest kritiska faktorn gällande informationsläckage. Mer än hälften av insiderdatabrott sker inom organisationer där åtkomst av information nås via organisationens datorer. Eftersom interna säkerhetsbrott orsakas av legitima och behöriga användare kan inte vanliga säkerhetsåtgärder effektivt upptäcka och förhindra detta. Det är just dessa scenarier som är svåra att förebygga och hantera, eftersom dessa användare har tillgång till informationen. (Bishop, Okhravi, Rahimi & Lee, 2010)

1.2 Problembeskrivning

Informationsläckage är ett komplext problem vilket gör det svårt att kontrollera. Det är svårt att kontrollera eftersom det ofta är behörig personal som är skyldig till läckorna. Den ansvarige för säkerheten av information måste ofta se förebyggandet från den skyldiges synvinkel för att få full förståelse för hur läckan kan ske och hur den då kan förebyggas (Bishop, et al, 2010). Det är komplext då informationsläckage kan ske på så många olika sätt, såväl avsiktligt som oavsiktligt. Det finns även många andra aspekter som ibland kan vara svåra att ta hänsyn till eller kontrollera där det kan krävas tydlig policy för hur de anställda ska hantera information. (Abbadi & Alawneh, 2008)

Ett problem för organisationer är att de måste förhålla sig till hur deras situation ser ut och hur dagens teknik används. Därför måste de använda metoder som är anpassade efter deras behov. Det kan vara svårt att avgöra då teknik och situationer för informationsläckage förändras och är så olika beroende på vilken organisation det är. Problemet för organisationer är även att konsekvenserna av informationsläckage kan medföra förlust såväl ekonomiskt som ur ett anseendemässigt perspektiv. (Liu, Zhang, Cui & Wu, 2008)

Det är intressant att undersöka påverkan av informationsläckage genom studier där vi vill undersöka fenomenet informationsläckage. Vi vill även undersöka hur informanter förhåller sig till fenomenet, detta eftersom de direkt eller indirekt berörs om det inträffar. Det är även intressant att undersöka hanteringen kring detta gällande förebyggande arbete och handlingsplaner vid inträffat informationsläckage. Det är även intressant för samarbetspartners och intressenter då de utbyter information och har kunskapsdelning. Det är dessa problem som är fokus för studien, och genom att göra en kvalitativ undersökning i form av frågeformulär som även innehåller scenariofrågor ska vi besvara detta. Den här undersökningen kommer att ge en insyn i hur valda organisationer är förberedda och hanterar informationsläckage liksom vilka konsekvenser som kan uppstå. Genom att strukturera upp studien efter tre teman; hot – åtgärder – konsekvenser, skapar vi en god bild för hur informationsläckage uppstår, vilka åtgärder som kan tas samt vilka konsekvenser informationsläckage medföra.

1.3 Forskningsfråga

För att förtydliga från problembeskrivningen lyder vår forskningsfråga som följande:

- Hur påverkas organisationer av informationsläckage?

Med följande underfråga:

- Vad finns det för handlingsplaner och policys vid informationsläckor och hur förebyggs detta?

1.4 Syfte

Vi har valt att fokusera på hur informationsläckage påverkar organisationer och vad de har för policys för informationsläckage och hantering av detta. Det vi vill ha ut från denna studie är ett resultat som visar hur våra valda organisationer arbetar med att förebygga och hantera informationsläckorna samt hur det påverkar våra valda organisationer.

1.5 Avgränsning

I vår undersökning kommer vi inte att beröra någon form av organisationsstruktur och hur strukturen påverkas av informationsläckage, utan snarare vilka policys och handlingsplaner de använder sig av. Liksom att vi inte kommer att beröra historisk utveckling av förebyggande åtgärder för informationsläckage. Kommersiella organisationer är något vi heller inte kommer att beröra i vår undersökning. Vi avgränsar oss till de icke-kommersiella organisationerna, Försvarsmakten och Lunds Kommun. Vår undersökning kommer inte att rikta sig till personal inom organisationer som inte använder sig av informationssystem eller inte använder sig av andra kommunikationsmedium som exempelvis e-mail.

2 Litteraturgenomgång

I det här kapitlet går vi igenom vald litteratur för ämnet informationsläckage efter tre olika teman; hot – åtgärder – konsekvenser. Litteraturen är menad att ge en större förståelse för det diffusa ämnet som vi sedan ska använda för att koppla till empiri.

Det har gjorts många studier kring fenomenet informationsläckage och för hur det kan påverka organisationer samt för hur organisationer ska förebygga och skydda sig mot informationsläckor. Vi kan dock se att det inte finns en studie som helt går i samma riktning som en annan för vilka metoder som bör användas för att skydda sig. Detta beror på att fenomenet är komplext i många avseenden, och vart begränsningen ska dras då det finns oändligt med skydd som organisationer kan använda sig av men som samtidigt kan påverka effektiviteten i en organisation (Liu, Zhang, Cui & Wu, 2008). Litteraturen vi valt är menat att skapa en uppfattning av ämnet informationsläckage och hur verkligheten förhåller sig till detta.

Fokus ligger på att få en förståelse för vilken påverkan informationsläckage kan ha och hur organisationer kan förebygga och hantera det. Här har vi hittat olika författare som har skrivit en hel del inom området, dock har vi inte funnit några riktiga auktoriteter eller förebilder inom området. Exempel på författare är Srivatsa och Byers som har funnit säkra metoder som har testats och undersökts för hur organisationer kan förebygga informationsläckage liksom orsaker till hur det kan uppstå. Dessa har vi valt att titta närmare på då speciellt Srivatsa även gjort tester för hur väl hans metoder slår ut. Vi har även tagit del av en stor rapport författat av Baker, Hutton, Hylender, Pamula, Porter och Spitler, som är skriven för Verizon med avseende på informationsläckage och dataintrång. En del artiklar som undersöktes grundades på algoritmer och modeller för metoder för att förebygga informationsläckage. Detta var inte relevant för vår studie eftersom det ansågs vara för tekniskt orienterat. En del andra artiklar går in på hur organisationer påverkas av informationsläckage, men i grunden är det förebyggande för informationsläckage och hur det kan ske som behandlas, liksom konsekvenser av informationsläckage. Detta är mer relevant för vår studie eftersom vår forskningsfråga är hur organisationer påverkas av informationsläckage och vilka förebyggande åtgärder som finns vilket vi senare ämnar ha som grund i diskussion. En stor anledning som ligger till grund för litteraturstudien är att vi vill veta hur andra har tolkat en situation eller händelse liksom för att få veta vad andra människor sagt och gjort. Slutligen summeras det en undersökningsmodell för att knyta samman de olika delarna som tas upp i litteraturgenomgången för att användas som grund i slutdiskussionen.

2.1 Hot till informationsläckage

Informationsläckage är när information som endast är avsedd för den egna organisationen avslöjas och publiceras utanför organisationen. Informationsläckage inträffar allt oftare eftersom konkurrensen i vårt samhälle är väldigt hård (Pereira, 2005). Att skydda sina digitala tillgångar i form av information är en av de största utmaningarna för säkerheten inom företag (Abbadi & Alawneh, 2008). Detta beror på att företag hanterar väldigt stora mängder information, information som kan vara känslig. Att skydda sig emot informationsläckage är en komplex uppgift eftersom många läckor sker genom att nuvarande eller tidigare anställda läcker informationen (Bishop, et al, 2010). Detta medför att det är svårt för organisationer att skydda sig emot dessa läckage eftersom de anställda har auktoriserad tillgång till informationen. Det är detta fenomen som kallas för en insider, där en person inom organisationen som har auktoriserad tillgång, läcker information utanför den egna organisationen. Läckaget kan ske genom att en anställd sparar ner information på ett usb-minne och förflyttar informationen utanför organisationen. Informationsläckagen behöver inte ske genom att någon sparar ner informationen på ett usb-minne, auktoriserad personal kan även ta en bild av ett dokument eller skriva av dokument för hand. Ett sådant scenario är svårt för en organisation att skydda sig emot. (Abbadi, et al, 2008)

Enligt Lag (1990:409) om skydd för företagshemligheter 1 § beskrivs företagshemligheter som information om affärs- eller driftförhållanden i en näringsidkares rörelse som näringsidkaren håller hemlig och vars röjande är ägnat att medföra skada för honom i konkurrenshänseende. Den beskriver information som uppgifter som har dokumenterats i någon form, inbegripet ritningar, modeller och andra tekniska förebilder, och enskilda personers kännedom om ett visst förhållande, även om det inte har dokumenterats på något sätt.

Lag (1990:409) om skydd för företagshemligheter 2 § fortsätter med att beskriva vad ett obehörigt angrepp är. Som ett obehörigt angrepp anses inte att någon anskaffar, utnyttjar eller röjer en företagshemlighet hos en näringsidkare för att offentliggöra eller inför en myndighet eller annat behörigt organ avslöja något som skäligen kan misstänkas utgöra brott, på vilket fängelse kan följa eller som kan anses utgöra annat allvarligt missförhållande i näringsidkarens rörelse. Som ett obehörigt angrepp anses inte heller att någon utnyttjar eller röjer en företagshemlighet som han eller någon före honom har fått ta del av i god tro.

Enligt Lag (1990:409) om skydd för företagshemligheter 3 §, 5 §, 14 § kan som straff fängelse på högst sex år förekomma, där skadestånd kan tillkomma för att ersätta den skada som uppkommit genom brottet genom att företagshemligheten obehörigen utnyttjats eller röjts. Inlösen kan även ske där informationen kan överlämnas mot lösen eller att handlingen

eller uppgifterna förstörs, ändras eller utsätts för annan åtgärd som är ägnad att förebygga missbruk.

Vidare måste offentliga organisationer som myndigheter förhålla sig efter Offentlighetsprincipen. Offentlighetsprincipen är en av hörnstenarna i demokratin. Myndigheter och deras organisationer måste vara öppna så långt det går, och därför är alla förhandlingar osv. öppna. Att det ska vara öppet är för att det ska finnas möjlighet att granska vad myndigheterna gör så att de inte utövar maktmissbruk. (Regeringskansliet, 2011)

"*Till främjande av ett fritt meningsutbyte och en allsidig upplysning skall varje svensk medborgare ha rätt att taga del av allmänna handlingar*" (Regeringskansliet, 2011)

Det finns även handlingar som inte är offentliga av den anledningen att det handlar om rikets säkerhet. De handlingar som inte är offentliga är följande enligt Tryckfrihetsförordningen (1949:105) 2§;

- rikets säkerhet eller dess förhållande till annan stat eller mellanfolklig organisation
- rikets centrala finanspolitik, penningpolitik eller valutapolitik
- myndigheters verksamhet för inspektion, kontroll eller annan tillsyn
- intresset att förebygga eller beivra brott
- det allmännas ekonomiska intresse
- skyddet för enskilds personliga eller ekonomiska förhållanden
- intresset att bevara djur- eller växtart

Enligt Tryckfrihetsförordning (1949:105) 11§ är allmänna handlingar följande;

- En handling innehåller information av något slag: en text, en bild, eller information lagrad på annat sätt, till exempel i en dator.
- En handling är allmän om den förvaras på en myndighet och har inkommit till myndigheten eller upprättats där.
- Allmänna handlingar ska enligt grundregeln vara offentliga och tillgängliga för alla att läsa.
- Minnesanteckningar och utkast till beslut betraktas normalt inte som allmänna handlingar.
- Säkerhetskopior undantas från begreppet allmän handling.

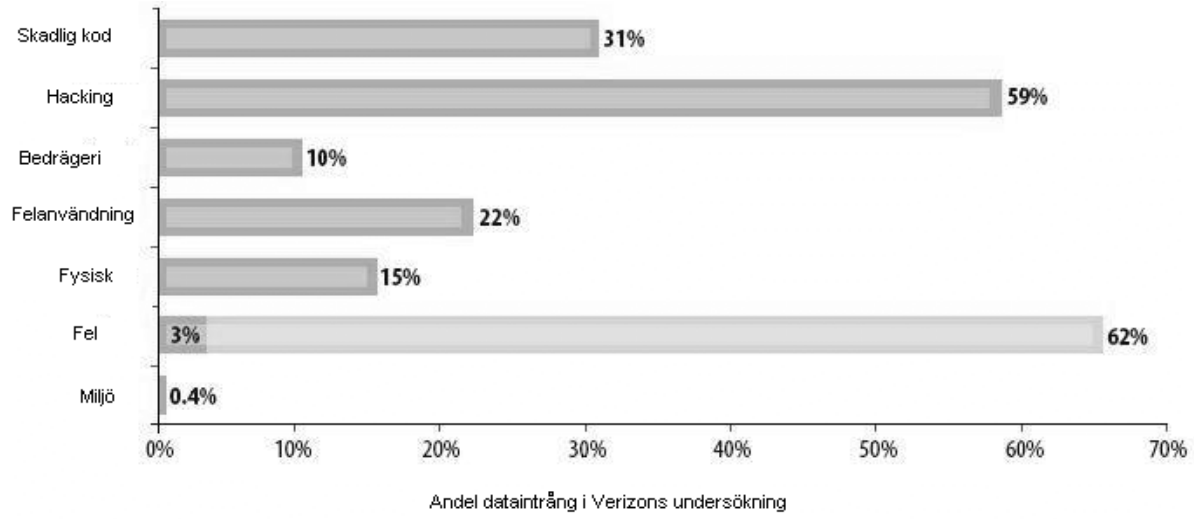
2.1.1 Kategorier av informationsläckage och hot

Det finns två olika kategorier som informationsläckage kan delas upp i, informationsläckage där informationen inte längre är under organisationens kontroll, alternativt försvinnande eller skada. Det händer även att dessa kategorier överlappar varandra. Detta är ett vanligt sätt att förlora data på, det sker ofta genom en hackerattack mot kunddatabasen. Den vanligaste konsekvensen av detta är identitetsstöld. Den hittills största enskilda attacken kom över 130 miljoner kreditkortsuppgifter från en av USA:s största betalningsprocessorer. Den andra

kategorin, försvinnande eller skada, leder till att den rätta versionen av data inte är tillgänglig för organisationen. Det har förekommit att stora företag har haft stora förluster av kunddata orsakat av haveri hos de ansvariga för lagringen av informationen. Om den senast sparade versionen av informationen blir fysiskt stulen överlappar kategorierna varandra. Ett exempel på detta är stöld eller förlust av dator som är ett vanligt förekommande problem för företag. Personen som använde den kan ha haft den senaste versionen av informationen på datorn. Detta kan leda till att organisationen inte kan få tillgång till den senaste versionen eller inte kan urskilja vilken som är den senaste versionen. (Liu, et al, 2010)

Typer av hot

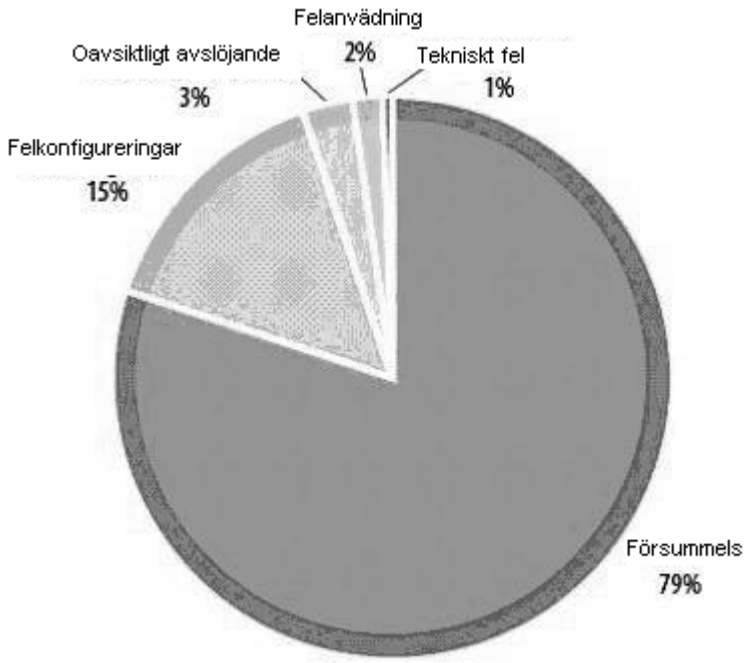
Organisationer ställer ofta frågor som hur uppstår säkerhetsluckor och hur vanliga de är. Det är en legitim fråga eftersom det inte är självklart hur dessa hot och luckor uppstår. I detta avsnitt kommer detta därför att avhandlas genom en undersökning gjord av Verizon som undersökt säkerhetsluckor och intrång, med bifogad statistik. I figur 2.1 finns en överblick av de olika typerna av hot som förekommer i Verizons undersökning. (Baker, Hylender & Valentine, 2008)



Figur 2.1 Typer av hot (Baker, W., et al., 2008, s 14).

Fel

Fel är ofta en bidragande faktor i de flesta fall av säkerhetsluckor. Dåliga beslut, felkonfigureringar, försummelser, motsträvighet, processhaveri, när något av detta inträffar i ett händelseförlopp leder det till att en incident inträffar. Eftersom att fel är utbrett saknar den lösa definitionen av det mening i ett större sammanhang. I undersökningen är fokus på dem fel som direkt lett till en kompromiss. (Baker, et al., 2008)

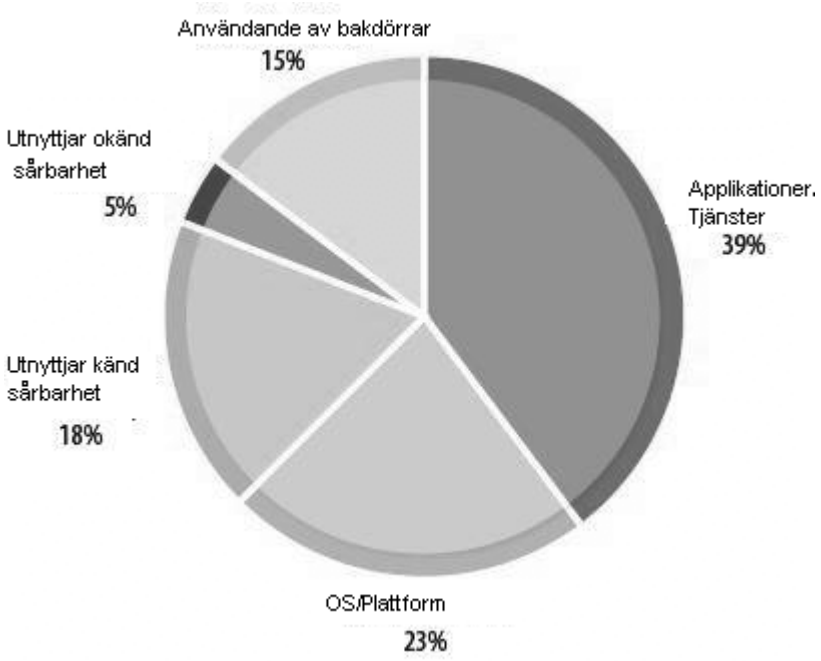


Figur 2.2 Typer av fel (Baker, W., et al., 2008, s 14).

Utifrån Figur 2.2 går det att urskilja att försummelser bidrar till en stor mängd luckor. Detta medför ofta att de standarder och säkerhetsprocedurer som tros ha blivit implementerade har i själva verket inte blivit det. Felkonfigureringar manifesterade i form av felaktiga system, hårdvaru- och mjukvaruinställningar. Dessa fel är något som är vanligt förekommande. Men de utgör bara en del av de fel som förekommer som leder till att data äventyras. Hackers brukar utnyttja dessa fel eftersom att de inställningar eller ibland bristen av inställningar underlättar för hackare att göra en attack. (Baker, et al., 2008)

Hackning

När det gäller termer kring avsiktliga attacker mot informationssystem, så är hackning det som leder till mest intrång av alla kategorier. Hackning är en metod som inte har samma begränsningar som vissa andra metoder har. Det behövs exempelvis inte fysisk kontakt, mänsklig interaktion och behörighet till systemet. Detta gör att det är något som favoriseras i cybervärlden. Det finns många verktyg som hjälper till att automatisera och snabba på hackningprocessen. I Figur 2.3 visas olika typer av hackning som observerats. (Baker, et al., 2008)

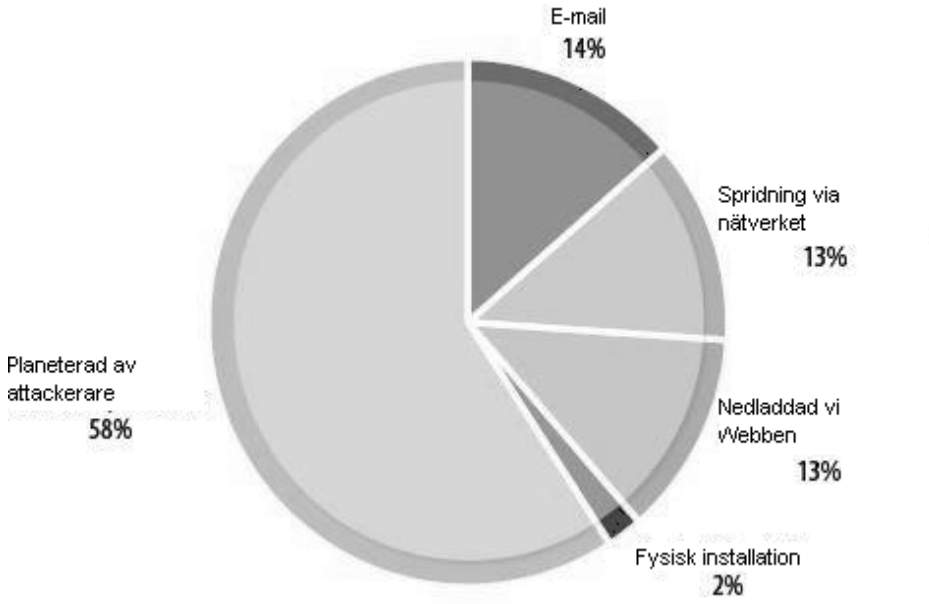


Figur 2.3 Typer av dataintrång (Baker, W., et al., 2008, s 15).

De vanligaste attackerna var att rikta sig mot applikationer och tjänster, vilket även är en trend som har blivit allt vanligare på senare tid, vilket går att urskilja i Figur 2.3. Tidigare har det varit operativsystem, plattformar och servrar som var mest utsatta för hackerattacker. Hackers som använder sig av så kallade bakdörrar är känsligt eftersom att de har tillgång till systemet som redan är kompromissat. Hackers som använder sig av denna teknik är ofta ute efter stora mängder information. (Baker, et al., 2008)

Skadlig kod

Skadlig kod utgör en stor del av hoten, och uppdagades ofta på system som var kompromissade, men dess roll i intrånget kunde inte fastställas. Genom åren så har skadlig kod oftast kommit in genom självkopierande e-mail och maskar som ligger på nätverket. Nyare trender inom skadlig kod är att de som skapar koden gör koden mer osynlig och har skiftat fokus för koden. Tidigare har målet med att hacka varit för äran, nu har fokus förändrats mot att hacka för ekonomisk vinnings skull. (Baker, et al., 2008)

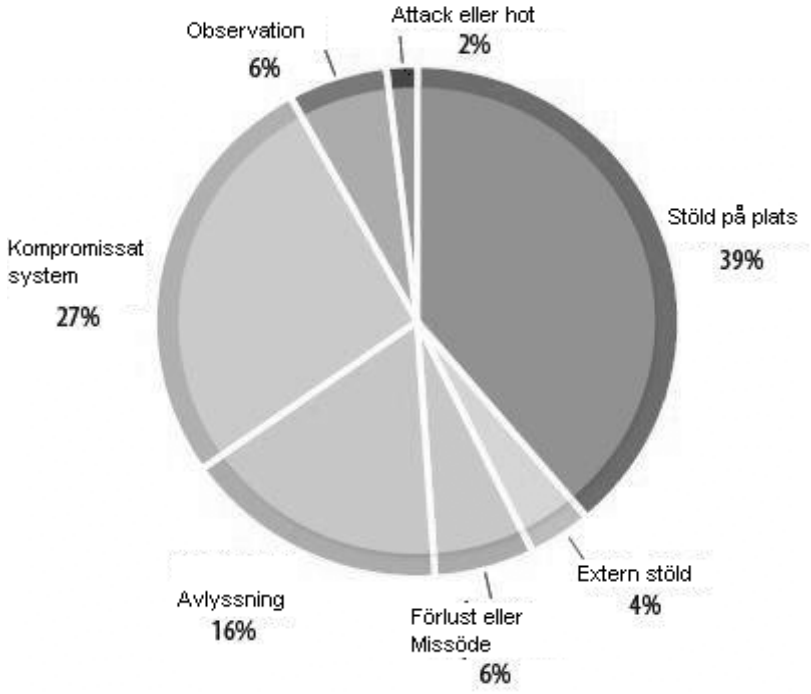


Figur 2.4 Andel skadlig kod som kommer in i systemet (Baker, W., et al., 2008, s 16).

Ett vanligare sätt är att plantera skadlig kod i ett redan kompromissat system genom en avlägsen attackerare, vilket går att urskilja i Figur 2.4. Hackerns mål med detta är att få kontroll över systemet. Genom att använda sig av denna metod går det att antingen samla in information för att spara ner den vid ett senare tillfälle, att skicka informationen till en avlägsen enhet, eller ge en avlägsen användare möjligheten att styra systemet. Oftast finns de olika möjligheterna inbyggda i den skadliga koden, vilket också är något som blir allt vanligare enligt nya trender som upptäckts. Den skadliga koden modifieras ofta för att hela tiden vara uppdaterad mot antivirusprogram, men det finns också skadlig kod som är skräddarsydd för ett specifikt system som ska angripas. (Baker, et al., 2008)

Felanvändning
Felanvändning eller missbruk refererar till användningen av en organisations resurser eller privilegier, för ett annat syfte än vad det är tänkt. Denna kategori passar bäst till insiders och partners eftersom de är förtrodda av organisationen, och är därför svårt att kontrollera. Det finns två större kategorier av felanvändning; skadligt och ickeskadligt. Skadligt inkluderar utnyttjande av rättigheter för att stjäla information eller för att sabotera systemet, medan ickeskadligt kan vara installation av personliga program eller att besöka olämpliga webbsidor. I dessa undersökningar så stod skadlig felanvändning för 19 % av dataintrången. De icke-skadliga felanvändningarna är betydligt färre och står bara för ett par av fallen. (Baker, et al., 2008)

Fysisk
Fysiskt hot för dataförlust eller intrång ligger förvånansvärt lågt på undersökningens lista enligt Verizons undersökning. Dataförlust som räknas till denna kategori behöver inte vara data som har kompromettерats, information som har gått förlorad antingen via krasch eller genom stöld räknas ändå som en datarisk. Även om informationen inte har hamnat i fel händer. (Baker, et al., 2008)



Figur 2.5 Andel fysiskt dataintrång (Baker, W., et al., 2008, s 17).

I Figur 2.5 går det att utläsa dataintrången, där det framgår att stöld från ett kompromissat system är vanligt. Något som även är vanligt är att hackers har åtkomst till systemet via fjärrstyrning. Avlyssning var något ovanligare bland den typen av intrång. Det som var absolut vanligast var förlorad information, genom kraschad hårdvara eller stöld. (Baker, et al., 2008)

Bedrägeri
Den här kategorin refererar till den medvetna förvrängning och bedrägeri genom tekniska och icketekniska medel. Detta kan exempelvis vara att använda sig av phishing för att göra bedrägeri. Vilket innebär att olagligt lura innehavare av elektroniska resurser såsom bankkonton att röja lösenord, betalkortsnummer eller annan känslig information. Ofta tar phishing formen av e-mail med uppmaningar till uppkoppling mot falska webbsidor (Nationalencyklopedin, 2011). (Baker, et al., 2008)

Miljö
Händelser av denna kategori är ett mycket större hot mot systemets tillgänglighet, än vad det är ett hot mot informationens integritet. I Verizons undersökning inträffade en incident av denna typ som resulterade i att ett system startade om. Detta resulterade i att systemets säkerhetsinställningar nollställdes och systemet var kompromissat. (Baker, et al., 2008)

2.1.2 Informationsläckage orsakat av dolda luckor

Informationsläckage behöver inte vara medvetet läckage. Det kan vara ett resultat av ovetskap om riskerna kring att utföra vissa uppgifter. Detta kan vara vardagliga arbetsuppgifter för användande i Microsoft Word. Byers (2004) menar att det finns känslig information som kan lagras dolt i ett Word-dokument. Typ av information som kan döljas och skickas med i dokumentet, kan vara användarnamn, sökvägar till server och text från helt orelaterade dokument. (Byers, 2004)

För att upptäcka den dolda informationen används speciella verktyg och metoder för att extrahera information från dokumentet, som användarnamn och sökvägar. Exempel på verktyg som kan användas är;

- *Antiword* är ett kommandotolksverktyg med öppen källkod som omvandlar ett Word-dokument till ren ASCII-text.
- *Catdoc* är snarlikt Antiword i de flesta aspekterna. För att se Word-dokument som är skickade till användarna genom peka-och-klika-orienterade program använder Unix-användare båda dessa verktyg.
- *Strings* är ett verktyg som tolkar data i vilken fil som helst och extraherar dessa segment som är utskrivningsbara strängar av vanlig text.
- *Perl* är ett skriptbaserat programmeringsspråk som är användbart för att manipulera data.

(Byers, 2004)

För att extrahera data ur dokument finns möjligheten att använda sig av olika tumregler och metoder. Att få ut intressant och användbar information kan dock vara svårt. Informationen står inte i klartext samt att det förekommer en del överflödig data i den information som extraheras. (Byers, 2004)

Antiword-metoden är inte den effektivaste då den sällan hittar gömd text. Denna metod är inte den farligaste för en organisation då den inte avslöjar användarnamn, sökvägar och annan metadata. (Byers, 2004)

En effektivare metod är string matching-metoden. Denna metod är ett större hot och kan avslöja användarnamn, sökvägar, skrivare och e-maildata. Denna metod är effektiv då information kan ses tydligt och det direkt går att tyda känslig information. Genom att använda sig av string matching-metoden går det även att hitta borttagen och ändrad text i dokument. (Byers, 2004)

Catdoc-metoden är en metod som påminner om string matching-metoden. Denna metod visar även dokumentets interna struktur samt raderad text. Tydligast är att där finns dolda ord genom att metoden antyder att där finns fler ord än vad Word anger som antal ord. (Byers, 2004)

2.1.3 Hot från insidan

Av alla problem som möter informationssäkerhetsspecialister, är insiderattacker det mest krångliga och förvirrande de möter. För att förhindra externa hot har det skett stor utveckling genom kryptering, åtkomstmekanismer och så vidare. Men för att hantera insiderattacker har utvecklingen inte varit så snabb. Detta beror på att det saknas förståelse för detta hot. Ett ramverk som underlättar förståelse för denna typ av hot är av stort värde för att kunna förebygga insiderattacker. (Schultz, 2002)

Det finns flera definitioner för termen "insiderattack". Tuglular och Spafford, (1997) menar att insiderangriparna är de som har vetskap om tekniken, har auktoriserad tillgång till systemet och därigenom kan kränka organisationens säkerhet. Andra menar att insiders sällan karaktäriseras av att de behöver kunskap om dataintrång. Detta eftersom de har tillgång till systemet och kan därför skada systemet eller att stjäla känslig information (Wang & Li, 2008). Enligt Schultz & Shumway (2001) kan en insiderattack definieras som ett medvetet missbruk av sin auktoritet och tillgång till systemet och nätverket. Einwechter (2002) definierar en insiderangripare som en person som har blivit anförtrodd tillgång och rättigheter i systemet, som istället för att hantera ärenden inom det ansvarsområde denne blivit tilldelad, manipulerar tillgång till ett system för att sedan utnyttja detta. Detta kan exempelvis vara att personen skadar systemet eller stjäl känslig information. (Schultz, 2002)

Enligt dessa definitioner menas att en insider oftast är anställda, entreprenörer, externa konsulter eller andra anställda som har tillgång till informationen. Eftersom det förekommer mycket outsourcing blir det allt svårare att fastställa om det är insiders eller outsiders. Många av de attacker som kallas för en insiderattack ligger i gränslandet mellan en insider- och outsiderattack. Enligt definitionerna är detta inte helt korrekt enligt verklighetsbilden. (Schultz, 2002)

2.1.4 Informationsläckage inom outsourcing

Dilemmat med informationsdelningsförlusten har fått stor uppmärksamhet på senare tid enligt Inkpen och Dinar. Företag som är inom kunskapsintensiva industrier behöver engagera samarbetsprojekt med forskning och utveckling inom industrin, för att upprätthålla deras konkurrensfördel. De behöver även öppna för kunskapssamarbete med samarbetspartners för att behålla detta. Inkpen & Dinar (1998), menar att ett sådant samarbete är av stor vikt för att erhålla större kompetens. Det har dock uppdagats att denna kunskapsspridning kan leda till läckage av kommersiellt känslig information (Norman, 2004). Verksamheter som deltar i kunskapsdelningssamarbete står inför utmaningen att dela så pass mycket information öppet utan att tappa kontrollen över informationsflödet så att verksamheter ökar det oönskade

informationsläckaget. Det går att ordnas genom att antingen sätta upp en noggrann styrningsstruktur och instrument för relationshantering, eller genom att försöka begränsa omfattningen av kunskapsdelningen (Oxley & Sampson, 2004).

Hoecht och Trott (1999) har utvecklat ett konceptuellt ramverk som länkar ihop organisationens forskningsarbete med teknik och utvecklingsstrategier, med den associerade risken med kunskapsförlust och informationsläckage, och de mest lämpliga kontroller och instrument för att hantera risken. Detta konceptuella ramverk identifierar de flesta viktiga moment och delar som kan orsaka ett läckage. Outsourcing medför att informationen är utom verksamhetens gränser. Detta medför alltså en högre grad av öppenhet, vilket i sin tur medför en högre risk för informationsläckage med tanke på att verksamheten och dess information blir mer utsatt. Risken för läckage anses vara högre för de verksamheter som använder sig av outsourcing än för de verksamheter som inte använder sig av outsourcing. (Hoecht & Trott, 2006)

Allt eftersom känslig information hålls inom organisationens gränser, minskar risken med oavsiktliga avslöjanden (Zucker, Darby & Yusheng, 1996), och kontrakt för anställda och specifika klausuler i dessa kontrakt kan användas för att avskräcka de anställda att svika arbetsgivarens förtroende. Den mest konkreta form av intern kontroll är den ideala byråkratiska kontrollen. Uppgifter och ansvarsområden, samt tillgång till information delas upp noggrant efter definierade regler och procedurer. Detta leder till att övervakning av prestationer och beteende underlättas. Problemet med tillit till individer i byråkratiska organisationer, löses teoretiskt på så sätt att minimering av diskretion leder till att behovet till tillit minskar. (Garsten & Grey, 1998) Byråkratisk kontroll må vara den mest robusta lösningen för att hantera problemet med informationsläckage, men det finns möjligheter för att detta kan ge höga kostnader för forskning och utveckling inom industrin. Det är dessutom mest lämpligt för rutinuppgifter och verksamhetsfunktioner som inte är relaterat till de konkurrenskraftiga delarna av en organisation, och där informationsläckage inte är ett problem. (Hoecht & Trott, 2006)

2.1.5 Myter och missförstånd angående insiderattacker

Det finns många olika myter och missförstånd kring fenomenet insiderattacker. Detta leder till ännu större förvirring för det redan diffusa ämnet. Schultz (2002) har sammanställt myter och missförstånd angående insiderattacker. Vi anser att dessa är högst relevanta och trovärdiga trots att denna artikeln publicerades 2002.

Myt 1: Fler attacker kommer från insidan än från någon annanstans.
Den här myten kommer från gammal FBI-statistik då fallet var så att fler attacker kom från insidan. Detta beror på att datorer för tjugo år sen var stordatorer, minidatorer och de hade inte alls den prestanda och saknade de nätverksmöjligheter som dagens datorer har. En annan faktor var att antalet personer som hade kompetens nog att utföra attacker var liten för tjugo

år sen. Det har på senare tid rapporterats att det är fler externa attacker som sker än interna. De som är under tron att det är fler attacker från insidan än externa attacker behöver kolla sina loggar för att se hur många attacker deras brandväggar faktiskt stoppar. Insiderattacker är dock oftast effektivare och är ett betydligt större hot än externa attacker. (Schultz, 2002)

Myt 2: Insiderattacksmönster är generellt snarlika externa attacker.
Personer som har expertisen med hackningsverktyg och -tekniker är i praktiken specialister på externa attacker. Insiders brukar generellt inte visa samma färdigheter och signaturer som externa hot gör. Insiders kan skaffa sig en fysisk tillgång till system. Fysisk tillgång eliminerar behovet för mer specialiserade och avancerade attackmetoder. Insiders har oftast avsikt att inte bli upptäcka, de undviker alarm och andra system som upptäcker intrång i systemet, system som vanligtvis upptäcker externa attacker. (Schultz, 2002)

Myt 3: Besvara en insiderattack är precis som att besvara en extern attack.
Att besvara en insiderattack är avsevärt annorlunda jämfört med att besvara en extern attack. En insider jobbar ofta i ett tätt samarbete med andra organisatoriska funktioner som mänskliga relationer och juridisk personal. Ledtrådar som visar exakt vad en insiderangripare har gjort och identiteten av denne, finns tillgängliga i andra källor än datorerna i sig. Enligt Schultz & Shumway (2001) är profilering av den misstänkta insidern den mest effektiva metod för att återskapa insiderattacken. Omvänd ingenjörskonst används för att göra detta. Att profilera ett misstänkt externt hot vore däremot en meningslös uppgift. (Schultz, 2002)

2.2 Åtgärder för informationsläckage

Idag så har känslig information blivit mer viktigt för finansiella avdelningar, medicinska organisationer, säkerhetssektorer och verksamheter världen över. När väl information har läckt så kan ägare av information förlora stort på detta. Enligt resultaten från undersökningen av ”*CSI Computer Crime and Security Survey 2007*” (Richardson & Peters, 2007) är alla hot mot skyddet av känslig information som hackerattacker, penetrering av system och oavsiktliga operationer, 59 % medvetna läckor från insiders och frekvensen för det ökar. Det finns många studier på förhindrande av informationsläckage för olika aspekter. Det kan handla om åtkomstkontrollsmekanismer som endast tillåter behöriga användare att använda känslig information. Dessa policys är dock restriktiva. Det kan även handla om att göra riskestimering och betalning av risk i informationsflöden, då risk är uppskattad baserat på trovärdigheten på mottagaren istället för mottagarens beteende. Men många studier för informationsläckage visar på att användares historiska beteende och deras plattforms säkerhetsegenskaper är två nyckelfaktorer. (Yin, Wang, Wang & Yu, 2010)

Att skydda sig emot informationsläckage blir allt svårare då läckan ofta är en person som har tillgång och rättigheter till att använda informationen. Det finns många säkerhetsmekanismer för att förebygga obehöriga att avslöja informationen. Dessa mekanismer kan vara

brandväggar, kryptering och verifiering. Dessa mekanismer skyddar inte i den grad som behövs, då informationen finns hos en behörig person. (Abbadi, et al, 2008)

Det arbetas kontinuerligt inom moderna organisationer med att försöka förebygga att dessa scenarier uppkommer. Detta görs exempelvis genom att vattenmärka eller kryptera informationen så att den endast fungerar inom sitt egna nätverk. Att kombinera förebyggande och kontrollerande funktionalitet med tillgänglighet och effektivitet är en komplex uppgift gällande informationssystem. (Liu, et al, 2008)

2.2.1 Förhållningssätt för förebyggande av informationsläckage

I modern tid finns data i stora mängder inom organisationer. En typisk organisation skickar och tar emot stora mängder data i form av e-mail, nedladdningar, sparande och flyttande på en daglig basis. Detta innebär att de har känslig information från kunder, partners och intressenter. Denna information förväntas vara skyddad. Dessvärre så råkar företag ut för stora läckage där personlig information och företagshemligheter läcker ut. Läckagen kan skada ett företag avsevärt, genom att företagets konkurrenskraftighet och anseende försämras. Att förebygga informationsläckage och förlust av information är ett komplext problem. Det är inget problem som går att hantera med hjälp av enbart en lösning. Därför bör verksamheter använda sig av metoder som passar den specifika organisationen bäst. (Liu, et al, 2010)

Verksamhetsdata existerar generellt i tre tillstånd:

- *Data i vila*: Detta betyder att data finns i filsystem, distribuerade klientdatorer och stora centraliserade databaser (Liu, et al, 2010). Här används exempelvis verktyg för att skanna nätverk på känsligt material. På så sätt kan organisationer bestämma i förväg vad som är känsligt eller ej. Därefter används mekanismer för att finna data som inte är krypterad och som finns tillgänglig på nätverket utan lämpligt behörighetsskydd. S.k. *Data Loss Prevention*-verktyg kan användas som automatisk krypterar, rapporterar eller tar bort sådana data. Dessa verktyg är dock ofta tunga att använda då de tar stor bandbredd eftersom de måste ta emot och analysera all data på nätverket. De är dessutom svåra att hantera. (Lawton, 2008)

- *Data vid slutpunkt*: Detta betyder att data finns i nätverkets slutpunkter, dvs. bärbara datorer, usb-minne, externa hårddiskar osv. (Liu, et al, 2010). Här kan exempelvis verktyg användas som övervakar data som rör sig mellan datorer och olika slutpunkter. De är designade för att förhindra att användare tar en digital eller papperskopia av känslig data. Dessa verktyg använder algoritmer för att avgöra om data som nås av applikationer på nätverkets datorer är känslig eller ej. Om den är det så kan systemet hindra hur den kan nås och används. Exempelvis kan de övervaka portar och applikationer och filtrera ut känsligt innehåll innan det kan skickas vidare. Dessa verktyg kan även rapportera händelser till en logg eller en säkerhetsansvarig person. (Lawton, 2008)

- *Data i rörelse*: Detta betyder att data är i rörelse och förflyttas från det interna nätverket till omvärlden via e-mail, ftp och andra mekanismer för att förflytta information (Liu, et al, 2010). Här används exempelvis verktyg som övervakar nätverkstrafik för känslig data som är i rörelse. Användare kan här själva konfigurera dessa verktyg så att när verktygen upptäcker känslig data som förflyttas kan användare blockera att överföringen sker. Dessa verktyg kan även registrera händelsen och rapportera till säkerhetsansvarig person. Även detta kan vara svårt att genomföra på stora volymer data över nätverk. (Lawton, 2008)

Data i de olika tillstånden behöver oftast olika metoder, policys för att hantera läckage. Funktioner för att hantera detta bör inkludera läckagerapportering och en handlingsplan för att hantera återställandet av incidenten. Fyra aspekter som bör hållas i åtanke i sin förebyggande modell är följande (Liu, et al, 2010):

- *Hantera*. Att förebygga informationsläckage och förlust av information är inte enbart ett tekniskt uppdrag. Det är ett arbete som även är beroende av definition av verksamhetsdata och att definiera och skapa policys för hur informationen hanteras.

- *Upptäcka*. Definiera hur pass känslig verksamhetsdata är, inventera data, lokalisera och städa upp i data. Detta inkluderar även att data säkras upp och eventuellt lagras på annan plats.

- *Övervaka*. Övervaka användandet av känslig data, för att förstå användandemönstret av de känsliga data. Detta görs för att få en överblick av hur verksamhetsdata används.

- *Skydda*. Upprätthålla säkerhetspolicys som förhindrar informationen att lämna verksamheten. Automatiskt skydd för känslig information genom hela verksamheten och dess nätverk, inkluderar även att all lagring av information ska vara krypterad. Restriktioner gällande utskrift, kopiering, åtkomst, förflyttning och nedladdning av känslig information. På detta sätt förhindras att information sparas ner på portabel media och förflyttas utanför organisationen.

(Liu, et al, 2010)

Informationen prioriteras efter kriterier som rankar den information som är mest kritisk om den skulle läckas. Detta baseras på vad som anses vara troligast att läcka och det som hade varit mest kritiskt om det läckt ut. Det baseras även på tidigare läckage och hur mycket information som finns och hur många som har tillgång till denna information. Att förebygga ett läckage är en taktisk uppgift och är grundat på mycket analys. Skyddet av information får inte påverka verksamhetens aktiviteter på sådant sätt att det stör. Det förebyggande arbetet och skyddsarbetet ska fungera så att det går obemärkt förbi av personal, och inte hindra dem från att utföra deras dagliga arbete. En organisation behöver flera metoder, strategier och

policys för att arbeta med att förhindra läckage. Det är viktigt att en organisation har en flexibel struktur för att bemöta informationsläckageproblemet som ständigt förändras. (Liu, et al, 2010)

2.2.2 Vattenmärkning – en tillämpning

En uppmärksammad teknik för att skydda sig mot informationsläckage är vattenmärkning av datafiler. Den huvudsakliga idén är att generera ett vattenmärke genom att använda en hemlig nyckel vald av avsändaren så att vattenmärket inte går att urskilja för den som inte vet nyckeln, dvs. mottagaren. Avsändaren lägger in ett vattenmärke i informationsobjektet, innan delningen med mottagaren sker. Därefter är det svårt för mottagaren att identifiera vattenmärket och ta bort det från objektet, däremot är det enkelt för avsändaren att ta bort och verifiera vattenmärket då avsändaren vet nyckeln. (Marecki, Srivatsa &Varakantham, 2010)

Det finns en risk att mottagaren försöker förvanska informationsobjektet, exempelvis ändra delar av bildfilen, med målet att radera vattenmärket för att undvika upptäckt. Mottagaren kan även försöka att förvanska hela informationsobjektet och på så sätt radera hela vattenmärket. Men genom att göra detta reduceras värdet på informationen drastiskt till oanvändbar information. Detta kräver stark robusthet på det digitala vattenmärket så att försök för att radera vattenmärket gör en märkbar skillnad på datakvalitet innan vattenmärket helt är raderad. Figur 2.6 visar a) där datakvaliteten efter borttagning av vattenmärkning skett och b) hur bilden egentligen ser ut. Det vill säga, bild a) är omöjlig att använda efter borttagning av vattenmärkning (Cayre, Fontaine & Furon, 2005). Om mottagaren läcker informationen trots att vattenmärket är intakt kommer läckan med stor sannolikhet att upptäckas av avsändaren som följaktligen slutar att dela informationen med mottagaren. Däremot finns det alltid en risk att avsändaren inte upptäcker att mottagaren läcker informationen, således måste avsändaren vara uppmärksam på hur hanteringen av information sker med den avsändaren har delat den med. (Marecki, et al, 2010)

För såväl verksamhets- som militära applikationer har lösningar med snabb liksom säker delning av information ökat i efterfråga. För speciellt behov är lösningar som ser informationsdelning som en sekventiell process där trovärdighet av informationens mottagare konstant övervakas genom att använda mekanismer för att upptäcka informationsläckage. (Marecki, et al, 2010)

Figur 2.6 Skillnader i datakvalitet vid vattenmärkning (Cayre, F., Fontaine, C., Furon, T., 2005, s3985).

2.2.3 Säker informationsdelning – en tillämpning

Nya tillämpningar baserade på riskuppskattning och ekonomiska mekanismer har föreslagits för att möjliggöra informationsdelning i osäkra miljöer. Dessa tillämpningar är baserade på idén att avsändaren konstant uppdaterar en uppskattning av risk för informationsläckor när avsändaren förser informationen till mottagaren. Detta baseras på sekretessen av att informationen avslöjas och avsändarens uppskattning av trovärdighet för mottagaren. Avsändaren debiterar sedan mottagaren den estimerade risken. I sin tur kan mottagaren avgöra vilken information som är användbar och betala genom att använda sina ”riskkrediter” för att endast få tillgång till dessa delar av information. Detta med förbehåll att det endast finns en begränsad upplaga av riskkrediter och riskestimering. På så sätt uppmanas avsändaren att vara försiktig och att inte i onödan spendera dessa riskkrediter. Eftersom allt informationsflöde är debiterat mot förväntade förluster i enlighet med obehöriga läckor och mängden av tillgänglig risk är begränsad finns det ett argument för att informationsläckage i större grad är kontrollerat av organisationen. Däremot kan företag aldrig helt skydda sig mot detta då dåligt beteende är svårt att modellera. För att hantera oklara mottagare måste avsändaren estimera den information den har om mottagaren och på så sätt uppskatta sannolikheten att mottagaren kan läcka den information avsändaren delar med sig av. (Marecki, et al, 2010)

2.2.4 Rekommendationer från Verizon

Företaget Verizon gjorde en undersökning av cirka 800 fall där informationsläckage eller dataintrång inträffat och för deras slutsats rekommenderade de följande förslag på åtgärder för att förhindra att detta inträffar (Baker, Hutton, Hylender, Pamula, Porter & Spitler, 2011). Då Verizon undersökt cirka 800 fall anser vi att dessa rekommendationer är väldigt trovärdiga och har stor grund i för vilka åtgärder som bör vidtas.

Ändra grundinställningar för åtkomstkontroll: När administratörer för system eller nätverk implementerar ett nytt system, se till att användare ändrar sina lösenord. Om organisationer outsourcar detta till en tredje part, kontrollera så att även de ändrar lösenordet och förutsätt inte att personal eller partners genomgående följer policys och procedurer. Tillsammans med att ändra grundinställningar borde organisationer säkerställa att lösenorden är unika och inte delas mellan användare eller används på olika system. Detta har varit problematiskt för tredjepartsstyrda tillgångar. (Baker, et al, 2011)

Granskning av användarkonton: Enligt Verizons tidigare rapport för dataintrång och år av erfarenhet har lett till att de ser ett stort värde i att granska användarkonton regelbundet. Granskningen bör bestå av en formell process som säkerställer att aktiva konton har validitet, är nödvändiga, är ordentligt konfigurerade och är givna lämplig behörighet. (Baker, et al, 2011)

Begränsa och övervaka behöriga användare: Nyckelorden är: Tillit med verifiering. Använd kontroller före anställning för att eliminera problemet innan det inträffar. Ge inte användare mer behörighet än vad de behöver. Se till att anställda känner till policys och förväntningar och se till att de följer dem. Behörig användning bör loggas och generera meddelanden till överordnade. Oplanerad behörighet borde generera en alarmering som sedan ska undersökas. (Baker, et al, 2011)

Säkerställ fjärrstyrda åtkomsttjänster: I många instanser är fjärrstyrd åtkomsttjänst möjlig och är öppen mot Internet. Verizon rekommenderar att binda ner dessa tjänster så att endast specifika IP-adresser eller nätverk kan nå dem. Utöver detta är det viktigt att begränsa åtkomsten till känsliga system inom nätverket. Många organisationer tillåter vilken utrustning som helst att koppla upp sig på nätverket och genom fjärrstyrning ha tillgång till annan utrustning. Verizon menar att detta inte är ett bra sätt att hantera detta. Det är viktigt att binda ner fjärrstyrda åtkomsttjänster till specifika verksamhetsnätverk via en kontrollista för åtkomst. (Baker, et al, 2011)

Övervaka och filtrera utgående nätverkstrafik: För många dataintrång sker det att exempelvis data, kommunikation eller uppkopplingar stängs ner. Om det förhindras kan organisationer bryta kedjan och förhindra intrånget. Genom att övervaka, förstå och kontrollera utgående nätverkstrafik ökar chanserna för att en organisation kan mildra illvillig aktivitet. (Baker, et al, 2011)

Testning för applikationer och utvärdering av kod: Angripare har börjat attackera i applikationslagret vilket försvar för denna typen inte kan hantera. Verizon menar att det gäller att släcka elden först; även lättviktiga webbapplikationer för avsökning och testning hittar många av de problem som leder till stora intrång. Inkludera därtill utvärdering av arkitektur, behörighet och källkod. Inkorporera en säkerhets- och utvecklingslivscykel för utveckling av applikationer är att rekommendera. Bistå även utvecklare så att de uppskattar och skriver mer säker kod. (Baker, et al, 2011)

Möjliggör åskådarloggar för applikationer och nätverk och övervaka dessa: Allt för ofta leder belägg för händelser till att dataintrång var tillgängligt för den drabbade men denna information var varken uppmärksammad eller åtgärdad. Processer som förser känslig, effektiv och verkningsfull övervakning och respons är kritisk för att skydda data. Det gäller dock inte att enbart fokusera på att loggning för nätverk, operativsystem och brandväggar och sedan försumma fjärrstyrda åtkomsttjänster, webbapplikationer, databaser eller andra kritiska applikationer. Även dessa innehåller rik information för att upptäcka, förhindra och utreda dataintrång. (Baker, et al, 2011)

Definiera misstänkt och onormalt beteende: Utred vad som är kritiskt och identifiera vad normalt beteende innebär och implementera sedan mekanismer som upptäcker och alarmerar beteende som avviker från detta. (Baker, W., et al, 2011)

Öka medvetandet för social styrning: Utbilda anställda för olika metoder av social styrning och från var attacker kan ske. I flera av Verizons fall kan de härleda att användare klickar på länkar de inte ska eller öppnar bifogade filer mottagna från identifierade personer. Belöna användare när de rapporterar misstänkta e-mail eller hemsidor och skapa incitament som är nödvändig för vaksamhet. Utbilda anställda och kunder att leta efter tecken för manipulerande och bedrägeri. (Baker, et al, 2011)

Skapa en incidenthanteringsplan: Om och när ett dataintrång kan misstänkas ha skett måste organisationen vara redo att besvara detta. En effektiv incidenthanteringsplan hjälper att reducera skalan av intrång och försäkrar att bevisen samlas in på ett korrekt sätt. (Baker, et al, 2011)

Sysselsätta sig för incidenttestning: För att kunna sköta incidenthantering effektivt, måste organisationer praktisera och träna olika strategier för att besvara ett dataintrång. Detta kan vara, identifiering av hot, klassificering av hot, processdefinitioner, ordentlig bevishantering och scenarios som kan inträffa. (Baker, et al, 2011)

2.3 Konsekvenser av informationsläckage

Trots framsteg de senaste åren inom obligatorisk åtkomstkontroll i databassystem är dagens informationslager fortfarande sårbara för attacker som kan resultera i informationsläckage. Utan stöd för att hantera dessa attacker, så kan känslig information riskera offentliggörande på grund av utsläpp av mindre känslig men relaterad information. Förmågan att skydda sig emot dessa olämpliga läckor skulle vara fördelaktigt och är av stor betydelse för myndigheter, offentliga och privata institutioner. Det är av stor betydelse eftersom det numera är en skyldighet att göra delar av informationen tillgänglig och offentlig för utomstående. (Dawson, Licoln, De capitani di Vimercati & Samarti, 2002)

Ansvarsfulla chefer använder sig oftast av flera olika källor för att få information innan de engagerar sin verksamhet att genomföra stora investeringar och ta strategiska beslut. Förutom att samla information från den egna organisationen, kan chefer även låta utomstående som potentiella kunder, leverantörer, samarbetspartners, investerare osv. ta del av de planer chefer har för verksamheten och få feedback från dem. Att få feedback från utomstående kan dock vara kostsamt för verksamheten. Det är mer sannolikt att verksamhetens investeringsplaner avslöjas innan de kan implementeras. Dessa läckor kan ske på olika sätt. Det kan exempelvis vara ett konkurrerande företag som får tag på deras planer. Detta kan resultera i att det konkurrerande företaget kan matcha deras planer och konkurrenskraftighet. Det kan även vara en kund som läcker information om framtida produkter, vilket leder till att försäljningen av nuvarande produkter kan försämras eftersom kunder då väntar på de nya produkterna. En annan läcka kan vara olika föreningar eller myndigheter som tar del av denna plan att investera och implementera. Detta kan förhindra verksamhetens förmåga att implementera investeringen. Det kan också medföra att de får svårare att få medhåll och acceptans att implementera sin investering. (Dye, Sri & Sridhar, 2003)

Liksom alla andra säkerhetsincidenter kan förlorad data resultera i förödande konsekvenser. Hur allvarliga konsekvenserna blir beror på vilken typ av förlust det är. Finansiella dokument kan oftast återskapas. Bedrägeri drabbar inte alltid kunden eftersom det finns lagar som ser till att kunden inte drabbas ekonomiskt. Konsekvensen för organisationen kan vara mycket allvarliga och kostsamma, det kan innebära att pålitligheten försämras och att organisationer drabbas av ekonomiska förluster som inte täcks av den statliga försäkringen. Med tanke på att det finns allt fler digitaliserade journaler, och de risker som finns med informationsläckage, medför att det finns risk för både konsumenter och organisationen. Det finns risk att dessa journaler läcker ut och skadar den enskilde individen samt att det skadar organisationens rykte. (Liu, et al, 2010)

2.3.1 Konsekvenser av läckor från Wikileaks

Under en s.k. Question & Ask har professor i teknik, Joel Adams, och professor i statsvetenskap, Joel Westra, från Calvin College diskuterat etiken och legaliteten kring fenomenet Wikileaks och vilka konsekvenser dessa publiceringar har eller kommer att innebära. Wikileaks som har publicerat känslig information vilka bland annat har innefattat konfidentiella meddelanden mellan diplomater liksom amerikanska militära loggar för kriget i Irak och Afghanistan (Westra & Adams, 2010). Då vi inte har funnit en stor mängd trovärdiga artiklar kring fenomenet Wikileaks har vi endast begränsat oss till Westra och Adams då det de diskuterar är väldigt relevant och tydligt visar vilka konsekvenser som har och kan uppstå.

På frågan vad de anser om vad Wikileaks hittills läckt menar de att det som tidigare misstänkts har skett nu kan verifieras genom de läckta dokumenten, det vill säga händelser som regeringen tidigare öppet inte velat konfirmera finns nu öppet för allmänheten.

Exempelvis att amerikanska militära styrkor har varit delaktiga i hemliga aktioner i Pakistan och Jemen, att sunniaraber uppmanat USA att ta hårdare tag mot Iran liksom att den amerikanska regeringen varit medveten om korruption i länder som Afghanistan, Irak och Nigeria. Westra och Adams känner även en oro för detaljnivån i vissa dokument, exempelvis för platser som är centrala för amerikanska intressen som inkluderar hydroelektriska dammar, vaccinfabriker och undervattenskablar, en detaljnivå som de menar är en invit för terroristattacker. (Westra, et al, 2010)

Westra (2010) fortsätter med att konsekvenser förmodligen kommer att medföra misstro och ökade diplomatiska påfrestningar. Både för länder som har drabbats genom läckt sekretessbelagt material liksom länder som har behandlats grovt i de läckta dokumenten. Det kan även innebära att informationsdelning mellan länder kommer att minska och på så sätt mindre effektiv underrättelseverksamhet och hårdare förhandlande sker. I det långa loppet tror Westra att praktiken av diplomati måste förändras för att reflektera ett ökat transparant internationellt system. (Westra, et al, 2010)

Om länder inte längre i samma utsträckning delar med sig av underrättelseverksamheter kommer det att blir svårare att förhandla framgångsrikt i multilaterala forum. På så sätt kommer processen med en global administration bli svårare än vad det redan är, exempelvis för hur transnationell terrorism och miljömässig nedbrytning ska hanteras. Adams menar samtidigt att amerikanska politiker har gått hårt fram mot Wikileaks och kallat de för en terroristorganisation där en utredning måste inledas. Samtidigt som samma politiker tillrättavisar länder som Ryssland och Kina för att vara restriktiva för yttrandefrihet och pressfrihet. På så sätt kan omvärlden tolka amerikanska regeringen för att vara hycklare, vilket kan vara mer skadande än läckorna i sig. (Westra, et al, 2010)

Konsekvenser för Wikileaks har bland annat inneburit att motståndshackare har använt attackmetoder som *denial of service* för att förhindra att människor får tillgång till Wikileaks servrar. En attack som syftar till att överbelasta ett system (Nationalencyklopedin, 2011). Wikileaks som även använt servrar från Amazon.com har nekats fortsatt användande. Donationer som gått via PayPal, Mastercard och Visa har alla stoppat transaktioner som är menat att hjälpa Wikileaks. Som följd av det har anhängare till Wikileaks gjort motattacker mot just PayPal, Mastercard och Visa i form av *denial of service*-attacker. Samtidigt har inom vissa delar av den amerikanska militären som en förebyggande åtgärd mot framtida läckor förbjudit soldater att använda flyttbar media som usb-minnen, CD-skivor och DVD-skivor på datorer kopplade till militärens nätverk, om så sker står de inför krigsrätt. På ett juridiskt plan finns det dock ingen lag som Wikileaks har brutit mot, amerikanska ” The Espionage Act” och brott mot intellektuell egendom går inte direkt att applicera på fallet. (Westra, et al, 2010)

2.4 Undersökningsmodell

Som vi kan se utifrån litteraturgenomgången är informationsläckage ett problem som drabbar många organisationer. Informationsläckage förekommer i två huvudkategorier. Informationsläckage där informationen inte längre är under organisationens kontroll, vilket kan ske genom både en extern och en intern attack. Utifrån den genomgången av litteratur kan vi se att informationsläckage är något som organisationer har svårt att skydda sig emot. Detta gäller främst insiderattack. Detta beror på att de anställda har auktoriserad tillgång till informationen vilket medför att insiders är det svåraste att skydda sig emot. Detta något organisationer arbetar aktivt med att förebygga, både internt och externt hot. (Sektion 2.1.1, 2.1.3)

I litteraturgenomgången tas det upp olika åtgärder och metoder för att förebygga och hantera eventuella informationsläckage. Det finns många säkerhetsmekanismer och policys för att förebygga att informationen avslöjas. Dessa mekanismer kan vara brandväggar, kryptering och verifiering (Sektion 2.2). Att kombinera förebyggande och kontrollerande funktionalitet med tillgänglighet och effektivitet är en komplex uppgift gällande informationssystem (Sektion 2.2). Att använda policys för informationshantering kan vara ett hjälpmedel mot informationsläckage, i kombination med tidigare nämnda säkerhetsmekanismer. Detta kan exempelvis vara att skapa en incidenthanteringsplan, övervaka och filtrera utgående nätverkstrafik, granska användarkonton och kontrollera åtkomsten för dessa. (Sektion 2.2.4)

Förlorad data kan resultera i förödande konsekvenser. Hur allvarliga konsekvenserna blir beror på vilken typ av förlust det är. Konsekvenserna kan vara mycket allvarliga och kostsamma, det kan innebära att pålitligheten och trovärdigheten försämras samt att organisationen drabbas av ekonomiska förluster som inte täcks av den statliga försäkringen genom lagar. (Sektion 2.3)

Ett exempel i modern tid är Wikileaks, och de konsekvenser som deras publiceringar inneburit och kan komma att innebära. På kortsiktig tid kan det innebära misstro och ökade diplomatiska påfrestningar för regeringar och myndigheter. Deras publiceringar kan även innebära att informationsdelning mellan länder minskar och på så sätt mindre effektiv underrättelseverksamhet och hårdare förhandlande sker. I det långa loppet kan det även i praktiken innebära att diplomatin måste förändras för att reflektera ett ökat transparent system. (Sektion 2.3.1)

Vi har utifrån litteraturgenomgången skapat tre teman som följer hela uppsatsen. Dessa teman är hot, åtgärder och konsekvenser av informationsläckage. Utifrån dessa teman och litteratur har vi sedan identifierat områden vi vill undersöka vidare, för att kunna besvara forskningsfrågan. Dessa kategoriseras i sektion 3.2.5. För att förstå informationsläckage och hur det kan ske har vi utformat frågor för att undersöka detta. Detta ligger till grund för vilka åtgärder som kan tas när ett informationsläckage har skett, samt vilka handlingsplaner och policys som kan användas. Åtgärder ligger sedan till grund för att lindra eller förhindra de eventuella konsekvenser som kan uppstå genom informationsläckage. Konsekvenser är det mest intressanta att undersöka i vår studie, då det är det som påverkar organisationer i störst

utsträckning. Vår tankegång har sedan mynnat ut i de frågor till frågeformulär som finns i figur 2.7.

Litteraturgenomgång

Hot till informationsläckage	*Åtgärder för informationsläckage*	*Konsekvenser av informationsläckage*
Angreppssätt	Policys Tekniska åtgärder Handlingsplaner	Organisatoriska & ekonomiska kostnader

Frågor
Hur är förhållningen gentemot informationsläckage och är det ett problem?
Vilket hot är det största mot organisationen?
Hur ser handlingsplanen ut om information läcks utan tillåtelse utanför organisationen?
På vilket sätt arbetas det med att förbättra säkerheten för att förebygga att ett informationsläckage inträffar?
På vilket sätt påverkas organisationen av det förebyggande arbetet för informationsläckage för såväl positiva som negativa effekter?
Finns det tekniska säkerhetsmekanismer installerade eller konfigurerade för att förhindra oavsiktligt informationsläckage?
Scenariofråga 1: åtgärd vid scenario där ett tänkbart informationsläckage inträffat
Scenariofråga 2: åtgärd vid scenario där ett tänkbart informationsläckage inträffat
På vilket sätt kan informationsläckage påverka organisationer ur ett anseendemässigt perspektiv?
Hur skulle ett informationsläckage påverka arbetsrutiner?
Scenariofråga 1: Konsekvens vid scenario där ett tänkbart informationsläckage inträffat
Scenariofråga 2: Konsekvens vid scenario där ett tänkbart informationsläckage inträffat

Figur 2.7 Undersökningsmodell

3 Metod

I detta kapitel beskriver vi vårt tillvägagångssätt för studien och varför vi har handlat som vi gjort. Det är utifrån våra val av metoder som vi strukturerat vårt arbete.

3.1 Utgångspunkt för undersökning

Som utgångspunkt för undersökningen och arbetsmetod för studien har vi valt att göra en kvalitativ undersökning där vi först utgår från litteraturgenomgång som beskriver vad informationsläckage är, hur informationsläckage kan förebyggas och hanteras samt hur informationsläckage påverkar organisationer. Detta för att få en god koppling till de forskningsfrågor vi vill undersöka på informanterna. Genom att först utgå från litteraturgenomgång får vi även en uppfattning för hur verkligheten ser ut samt vilka scenarion som kan uppstå som vi sedan kan använda i vår kvalitativa undersökning (Jacobsen, 2002).

Undersökningen genomfördes med frågeformulär som innehöll frågor om hur informanten uppfattar informationsläckage utifrån olika aspekter liksom scenarion som kan uppstå som informanten ska förhålla sig till och svara utefter. Detta utförs som studier på Försvarsmakten och Lunds kommun där vi vill undersöka fenomenet informationsläckage och hur informanter uppfattar detta. Anledningen till att vi använder frågeformulär är för att frågeformulär ger koncisa svar för de frågor vi vill ha svar på som sedan kan tolkas, analyseras och diskuteras mot det teoretiska ramverket. Anledningen till att vi gör studier på två organisationer är att det syftar till att undersöka ett specifikt fenomen inom ett komplext område i sin realistiska miljö (Backman, 1998). Ändamålet med detta är att undersöka och belysa och på så vis få en bättre förståelse för den problematik som ligger till grund för uppsatsen.

3.2 Angreppssätt

Tillvägagångssättet för uppsatsen struktureras utefter tre teman eller områden i teori, empiriska studier och diskussion; hot – åtgärder – konsekvenser (Jacobsen, 2002). Anledningen till en struktur av denna karaktär är att först få en genomgående förståelse för

begreppet informationsläckage och vad som kan orsaka informationsläckage. Därefter undersöks hur handlingsplaner, policys och åtgärder för att förebygga informationsläckage kan se ut. Detta ligger sedan till grund för konsekvenser som kan uppstå och hur organisationer påverkas av informationsläckage. Detta görs för att underlätta en koppling mellan litteratur och empiri i en slutdiskussion. Vi får på så sätt även en genomgående struktur i alla delar av uppsatsen vilket underlättas för läsaren.

3.2.1 Empiri

Nästa del i studien utgörs av vår empiriska undersökning av informationsläckages påverkan på organisationer. Litteraturgenomgången kommer att beskriva en del av hur informationsläckage kan påverka organisationer och hur organisationer kan förebygga detta, men för att få en inblick för hur detta hanteras i verkligheten ska vi studera detta på organisationer där detta är en viktigt fråga; Försvarsmakten och Lunds Kommun. Ämnet informationsläckage och hanteringen kring det passar dessutom väldigt bra in på just Försvarsmakten då de under lång tid har erfarenhet inom ämnet och på så sätt kan ses som experter inom området och att det är ett specifikt fenomen vi ska undersöka inom ett komplext område i sin realistiska miljö.

Urvalet av informanter som ska besvara de frågeformulär vi tagit fram är både användare av informationssystem liksom chefer för användarna där båda typerna av informanter har någon form av insyn i informationssäkerhet, hur information hanteras och hur det kan påverka deras arbete och organisation. Då vi gör studier på två specifika organisationer är meningen heller inte att få en generell bild av hur informationsläckage påverkar organisationer, utan snarare att få en rik och detaljerad beskrivning av ett fenomen utifrån olika kontexter. Därför är det en intensiv utformning som inte går att generalisera i hög grad för hur informationsläckage hanteras och uppfattas på hela organisationen som undersöks eller exempelvis kommersiella organisationer (Jacobsen, 2002). Valet av informanter blir en typ av experter för vad vi vill ha ut av undersökningen då de direkt kan ha en uppfattning om ämnet. Detta med tanke på att en av organisationerna är Försvarsmakten där känslig eller sekretessbelagd information är en naturlig del av verksamheten. För att få olika uppfattningar från olika delar av organisationen valdes informanter som använder IT-system liksom chefer som är ansvariga om informationsläckor sker eller som i större eller mindre grad har erfarenheter och kunskaper inom området. Därför är informanterna relevanta för vår undersökning då de kan bidra med kunskap inom området liksom erfarenheter. På så sätt får vi resultat som är pålitlig, intressant och överrensstämmer med vår frågeställning.

Inledningsvis var tanken att undersöka myndigheter. Genom diskussion med handledare fick vi idén att rikta oss till Försvarsmakten och Lunds Kommun. Detta underlättades genom att vår handledare hade en kontaktperson inom Försvarsmakten. Vi har valt både Försvarsmakten och Lunds Kommun som organisationer för att det är intressant att ställa

dessa båda organisationer mot varandra. Synen på hur information hanteras och värderas samt hur organisationerna påverkas av ett eventuellt informationsläckage kan förmodas vara väldigt annorlunda mellan organisationerna. På så sätt får vi olika synsätt på hur information ska hanteras och hur informationsläckage påverkar organisationerna. Anledningen till att vi valde Försvarsmakten var att vi ansåg att de borde ha stor kunskap inom IT-säkerhet och informationsläckage, vilket kunde resultera i svar som kunde användas i diskussionen. Lunds Kommun valdes å andra sidan på grund av att de måste i större mån förhålla sig till en öppenhet gällande information, samtidigt som de måste ha en viss sekretess gällande viss information enligt offentlighetsprincipen.

Antalet svar som förväntades från de båda organisationerna var uppskattningsvis 20 stycken. Däremot skickades det inte ut 20 frågeformulär utan kontaktpersonerna på respektive organisation uppmanades att vidarebefordra frågeformulären till ett antal informanter via e-mail. Bortfallet kan således beräknas till uppskattningsvis 55 % då vi fick tillbaka nio svar. I tabell 3.1 ger vi en överblick av antalet informanter från respektive organisation.

Tabell 3.1 Överblick av antal informanter

	Lunds Kommun	*Försvarsmakten*	*Totalt*
Chefer	4	3	7
Användare	1	1	2
Totalt	5	4	9

3.2.2 Genomförande

Genomförandet av undersökningen skedde i form av frågeformulär som skickades till informanterna. Undersökningen var utformad med öppna frågor som var avsedd att ge öppna, utförliga och detaljrika svar från informanterna (Andersson, 2001). Undersökningen innehöll även scenariofrågor där informanten var tvungen att förhålla sig efter ett visst scenario och sedan beskriva hur de hade handlat efter det scenariot och hur det påverkade informanten. På så sätt var det menat att ge en förståelse och en rik beskrivning för hur informationsläckage kan påverka organisationer, liksom för hur arbetet med förebyggande hanteras (Jacobsen, 2002). Frågorna var därför menade att diskutera de frågor eller teman vi ämnade besvara med uppsatsen. Det gällde dock att vara försiktig så att vi inte hamnade i ett tillstånd där vi hade för mycket information än vad vi kunde hantera. Dels för att det kunde medföra irrelevant information för forskningsfrågorna och dels för att det skulle leda till att vi inte kunde sammanställa informationen och bearbeta den ordentligt. Frågeformulären skickades ut via e-mail för att informanterna på så sätt skulle kunna besvara frågeformulären när tid fanns och för att på så sätt få ett mer detaljrikt svar. Det gällde dock här att från vår sida vara uppmärksam och hantera informanterna på ett bra sätt så att de verkligen svarade eller så att de inte svarade för sent, för då skulle vi få ett bortfall som är alldeles för stort vilket skulle påverka vår uppsats negativt.

Vad gäller anonymitet för informanterna hanterades detta varsamt då det kunde vara känslig information vi fick tillgång till. Vi ämnade inte fråga efter bakgrund, personlig information eller vad informantens nuvarande roll eller titel var då den inte var nödvändig att veta för vår forskningsfråga. Således är informanten helt anonym i vår uppsats. Vad gäller bearbetningen sammanställdes svaren från frågeformulären och kategoriserades sedan för att diskuteras och analyseras mot litteraturen. Sedan kunde vi tolka frekvensen av svar från åsikter, värderingar eller beteende (Andersson, 2001).

3.2.3 Kategorisering av frågor för frågeformulär

I detta delkapitel ger tabell 3.2 en överblick över kategoriseringen av frågor för frågeformulären som informanterna har svarat på. Frågorna för frågeformulären är kategoriserade efter de teman vi tidigare arbetat efter; hot – åtgärder – konsekvenser.

Utifrån litteraturgenomgången har vi diskuterat fram frågor som är tänkbara för våra frågeformulär. De är baserade efter de tre teman vi har och för tänkbara hot som vi identifierat i litteraturgenomgången. Där var det viktigt för oss att undersöka hur organisationerna ser på informationsläckage och tacklar olika problem som kan uppstå. Formuleringarna av frågor diskuterades fram med samråd av handledare och kontaktperson vid försvarsmakten för att på så sätt få frågor som var relevanta och som även var tänkbara att svara på för informanterna. Vid varje fråga resonerade vi kring vilka svar vi ville ha från informanterna som senare kunde användas i diskussionen, detta har legat till stor grund för formuleringarna av frågorna. Våra scenariofrågor är framtagna utifrån vad vi ansåg vara tänkbara hot och incidenter som kan påverka organisationerna negativt. Dessa har även konfirmerats och bearbetats av vår kontaktperson från Försvarsmakten för att försöka spegla en verklighet som kan uppstå och som även är relevant. Då vi har informanter som både är användare och chefer har vissa frågor modifierats för att passa typen av informant. Detta var nödvändigt eftersom informanter av de olika typerna har olika insikt om ämnet och därför krävdes olika formuleringar av frågorna. Detta bidrog även till olika infallsvinklar då det var olika typer av informanter liksom organisationer.

Tabell 3.2 Översikt av frågor för frågeformulär och teman

Tema	*Frågor*
Hot till informationsläckage	Hur är förhållningen gentemot informationsläckage och är det ett problem?
	Vilket hot är det största hotet mot organisationen?
Åtgärder mot informationsläckage	Hur ser handlingsplanen ut om information läcks utan tillåtelse utanför organisationen?
	På vilket sätt arbetas det med att förbättra säkerheten för att förebygga att ett informationsläckage inträffar?
	På vilket sätt påverkas organisationen av det förebyggande arbetet för informationsläckage för såväl positiva som negativa effekter?
	Finns det tekniska säkerhetsmekanismer finns installerade eller konfigurerade för att förhindra oavsiktligt informationsläckage?
	Scenariofråga 1: Åtgärd vid scenario där ett tänkbart informationsläckage inträffar
	Scenariofråga 2: Åtgärd vid scenario där ett tänkbart informationsläckage inträffar
Konsekvenser av informationsläckage	På vilket sätt kan informationsläckage påverka organisationen ur ett anseendemässigt perspektiv?
	Hur skulle ett informationsläckage påverka arbetsrutiner?
	Scenariofråga 1: Konsekvens vid scenario där ett tänkbart informationsläckage inträffar
	Scenariofråga 2: Konsekvens vid scenario där ett tänkbart informationsläckage inträffar

3.2.4 Etik, reliabilitet och validitet

För de informanter vi tänkt undersöka är det viktigt att de frivilligt kan avgöra om de ska delta i undersökningen. Det är inte meningen att resultatet ska innebära negativa eller positiva konsekvenser för informanten. Det är inte meningen att påtryckningar ska finnas från något håll för att informanten ska delta. Det är även viktigt att informanten vet syftet med undersökningen och hur uppgifterna ska behandlas samtidigt som det inte ska innebära att informanten anpassar sina svar efter detta. För att få en anonymitet från informanten är det inte intressant för oss att ha med frågor som rör informantens privatliv eller bakgrund, det är heller inte intressant för vår forskningsfråga. Informanter behandlas med yttersta konfidentialitet i undersökningen genom att informanterna hålls anonyma under ett kodnamn. Det är även viktigt att kravet på riktig presentation av data existerar i undersökningen för att få en fullständig bild av de frågor vi ämnar undersöka. (Jacobsen, 2002)

För att få validitet i undersökningen krävs det att vi faktiskt undersöker det vi ämnar undersöka och att det vi undersöker är relevant. För kontrollera att resultaten från undersökningen håller en validitet jämför vi resultaten mot teori för om de överrensstämmer eller avviker. Om två oberoende undersökningar och olika ansatser mynnar ut i samma slutsatser innebär det att giltigheten stärks ytterligare. Vi måste även vara kritiska till de svar från informanter vi fått tillgång till liksom till de svar vi inte fick tillgång till och varför vi inte fick det. De frågeformulären vi har utformat har validerats mot den kontaktperson vi haft inom Försvarsmakten för att på så sätt få fram relevanta frågor. (Jacobsen, 2002)

Vad gäller reliabilitet är det viktigt att undersökningen är trovärdig och visar en tillförlitlighet. Genom att använda oss av frågeformulär undviker vi intervjuareffekt som kan inträffa för såväl negativa som positiva aspekter. Däremot är det viktigt att vi även tolkar och analyserar resultaten från undersökningen så att det går att lita på de slutsatser vi drar. Gällande litteraturgenomgången som ligger till grund för den empiriska undersökningen är det viktigt att teorin är trovärdig för sitt syfte och att vi har kontroll och undviker felkällor. (Jacobsen, 2002)

3.2.5 Analys och diskussion

För analys och diskussion kopplas svaren och litteraturen samman för att analyseras och diskuteras utefter forskningsfrågan och dess underfråga. Målet här är att tolka de resultat vi har erhållit som sedan ska ligga till grund för slutgiltig reflektion och diskussion. För att få en validitet tolkas resultaten mot litteraturen. Till en början strukturerar vi upp de svar vi får från frågeformulären efter om de är för; hot – åtgärd – konsekvens.

För att skilja mellan de olika informanterna benämns informanter från Lunds Kommun, användare eller chefer, som LA eller LC. Gällande Försvarsmakten benämns informanter, användare eller chefer, som FA eller FC. Därefter redovisas detta genom en sammanfattande löptext från insamlad data efter typ av område; hot – åtgärd – konsekvens, var påverkan av informationsläckage samt hantering av informationsläckage med hjälp av handlingsplaner, policys och hur informationsläckage förebyggs mynnar ut i huvudpunkter. Här är det även viktigt att vi inte drar saker ur sitt sammanhang.

Det är även viktigt vid bearbetningen att kontrollera att informanten har hög reliabilitet för att vi ska kunna analysera resultatet på det viset vi vill. Vid bearbetningen och analysen är det även viktigt att vi hela tiden återknyter till den grundläggande frågeställningen (Jacobsen, 2002). Till sist görs en avslutande slutsats och reflektion som ska besvara forskningsfrågan och dess underfrågor.

4 Empirisk undersökning

I det här kapitlet presenterar vi informanterna och de svar som undersökningarna har gett. Vi har valt att dela upp presentationen av svaren efter liknande struktur som i litteraturgenomgången, dvs. efter hot – åtgärd –konsekvens.

Undersökningarna genomfördes av praktiska skäl genom ett frågeformulär. Vi skickade ut dessa genom kontaktpersoner vi anskaffat oss på olika avdelningar inom Lunds kommun och genom en kontaktperson inom Försvarsmakten. Vi har valt att göra på detta sätt eftersom det är lättare att upprätthålla kontakten med en kontaktperson istället för flera. frågeformulären är utformade efter en semistrukturerad karaktär. frågeformulären är utformade efter vårt tema; hot – åtgärd – konsekvens. För att skilja mellan de olika informanterna benämns informanter från Lunds Kommun, användare eller chefer, som LA eller LC. Gällande Försvarsmakten benämns informanter, användare eller chefer, som FA eller FC.

4.1 Svar från frågeformulär

Här presenteras svaren från de informanter som deltagit i vår undersökning efter ämne och informant för att på ett tydligare sätt få en överblick av informanternas syn på de olika ämnesområdena. Vissa av tabellerna har här frågor som har sammanslagits mellan användare och chefer då resultatet speglar båda typerna av informanter. Efter varje tabell följer sedan en kort summering av frågan från frågeformuläret.

4.1.1 Hot till informationsläckage

Tabell 4.1 Hur är förhållningen gentemot informationsläckage och är det ett problem?

Informant	*Ståndpunkt*
LC1	Inga problem
LC2	Ja. Främst i relationen till läckage gentemot massmedia. Som chef inom offentlig sektor måste jag ha kunskap om den meddelarfrihet som finns och att det inte är förenligt med svensk lagstiftning att efterforska vem som har lämnat Information till massmedia.
LC3	Jag anser att i min roll är det viktigt med integritet. Politikerna måste kunna lite på att det som avhandlas under exempelvis en budgetprocess inte förs vidare förrän de vill.
LC4	Ja, det kan vara ett problem som finns i flera verksamheter. Informationssäkerhetsansvaret ligger på verksamhetscheferna. För infrastruktursystem ligger ansvaret gemensamt på Kommunkontoret, kommunikationsavdelningen.
LA1	Ja, det är ett problem. Informationssäkerhet och sekretess styr vår verksamhet så i de fallen kan problem uppstå om information läcker.
FC1	Ja jag anser att det ibland finns ett problem med informationsläckage. Det blir onödigt mycket jobb med att hantera ”rykten” och personalen blir orolig för påhittade konsekvenser av självsvängande rykten.
FC2	Ja, men egentligen bara gällande sekretessbelagd information.
FC3	Ja, det finns ett begränsat, med dock existerande, problem med läckage av ännu ej delgiven eller konfidentiell information, från medarbetare i organisationen till tidigare kolleger som nu finns i andra myndigheter eller i näringslivet. I många fall är det i oförstånd eller i syfte att visa ett positivt samarbetsklimat, men resultatet kan bli att andra parter får ett informationsöverläge inför kommande samtal.
FA1	Ja. Som användare måste jag vara medveten om vilken informationsklass materialet jag hanterar är placerat inom. Om det är öppet kan jag hantera det med normala rutiner, dvs öppen e-post, telefon eller liknande. Är materialet hemligt hanteras det med särskilda rutiner för detta. Informationsläckage är inget jag önskar att orsaka, men något jag måste leva med inom den typen av arbete jag har.

Frågan som informanterna fick svara på var om informationsläckage var något de var tvungna att förhålla sig efter och om det är ett problem. Informanterna är eniga att det är något de måste förhålla sig efter och att det är problem för båda myndigheterna. Informanterna från Lunds Kommun menar att det är främst ett problem gentemot massmedia och att det är viktigt att politikerna kan lita på att de inte läcker information som de hanterar innan den är tänkt att komma ut. Informanterna från Försvarsmakten anser att det främst är ett problem gällande säkerhetsklassat material och att det kan bli mycket onödigt jobb med alla rykten som uppstår. Notera att båda myndigheterna är i den offentliga sektorn och måste förhålla sig efter offentlighetsprincipen och meddelarfriheten, vilket innebär att de inte får efterforska vem som har sagt vad till exempelvis massmedia. (Tabell 4.1)

Tabell 4.2 Vilket hot är det största hotet mot organisationen?

Informant	*Ståndpunkt*
LC1	N/A
LC2	Vet ej.
LC3	I en politiskt styrd organisation är det politiker som ska fatta beslut och kommunicera den. Vi tjänstemän ska arbeta utifrån fattande beslut, oavsett vad man själv tycker. Om vi läcker information i beslutsprocessen eller har för många privata åsikter kan verkställigheten påverkas
LC4	Troligen internt pga. misstag, nyfikenhet.

	Det finns inte mycket affärshemligheter i kommunen som i privata företag.
LA1	Internt, tror jag. Nyfikenhet.
FC1	Internt avseende ryktesspridning vilket leder till effektnedgång. Externt avseende främst industrin.
FC2	N/A
FC3	Internt hot störst. Myndigheten (Försvarsmakten) har väl utvecklade rutiner för skydd mot yttre hot. Idag gäller t ex att fjärrinloggning i systemen (inkl mail) inte medges. Informationsläckage genom medvetna eller omedvetna handlingar från anställda är svårare att förhindra. Många medarbetare har tillgång till information av känslig natur, volymen av upphandlingar är omfattande och teknikfaktorn hög.
FA1	Internt. Personalen måste hantera allehanda information i olika säkerhetsklasser på ett korrekt sätt. Det finns uppenbara risker att hanteringen kan ske bristfälligt med konsekvensen att felaktig information läcker ur organisationen.

Informanterna fick svara på frågan vilket de ansåg var det största hotet mot organisationen gällande informationsläckage, vilket kan vara internt eller externt hot. Båda myndigheterna var eniga om att de trodde att internt hot var det största hotet. De ansåg att det är nyfikenhet och ryktesspridning som leder till det. Försvarsmakten menar även att de jobbar aktivt med att skydda sig för externt hot och därför ansåg de att internt hot vore det största hotet. Värt att notera är att de båda myndigheterna ansåg att internt hot var det som var störst hot.(Tabell 4.2)

4.1.2 Åtgärder för informationsläckage

Tabell 4.3 Hur ser handlingsplanen ut om information läcks utan tillåtelse utanför organisationen?

Informant	*Ståndpunkt*
LC1	Inga problem, inga handlingsplaner
LC2	Finns ingen entydig handlingsplan. Bedömningar får ske från fall till fall.
LC3	Vad jag vet har vi ingen sådan handlingsplan. En kommun lever ju i allra högsta grad efter offentlighetsprincipen och att så mycket som möjligt ska vara tillgängligt.
LC4	Ansvaret ligger hos linjechefer och beroende på vilken typ av information det handlar om hanteras det olika. Det mesta av vår information är offentlig dock.
LA1	Fel i verksamheten hanteras via linjechef.
FC1	Snarast skall en rapport konstrueras med tyngdpunkt avseende menbedömningen [1]av vad den förlorade informationen har för betydelse för oss och för en eventuell fiende
FC2	Menbedömning enligt gällande regelverk. I förekommande fall även polisanmälan.
FC3	Jag sitter inte i en roll som chef i säkerhetsbefattning och har därför inte kunskap om myndighetens handlingsplan i sammanhanget. På avdelningsnivå är det ju informationsplikt till central säkerhetsansvarig samt chefssamtal med individ (om det är känt vem som handlat fel) som gäller.
FA1	Jag informerar min chef om vad jag observerar.

På frågan om hur handlingsplanen ser ut om information läcks utan tillåtelse utanför organisationen finns det en del skillnader mellan de två olika myndigheterna. Informanterna från Lunds Kommun påpekar tydligt att de inte har en tydlig handlingsplan klar om ett informationsläckage inträffar, däremot sker bedömningar från fall till fall för hur de ska gå tillväga om informationsläckage inträffar. Informanterna från Försvarsmakten har här ett tydligare regelverk för hur de ska gå tillväga, en rapport ska konstrueras med avseende på

[1] Menbedömning: En bedömning av eventuell skada

menbedömning av informationsläckaget. Däremot är de två användarna inne på samma spår och menar att incidenten informeras till överordnad chef. (Tabell 4.3)

Tabell 4.4 På vilket sätt arbetas det med att förbättra säkerheten för att förebygga att ett informationsläckage inträffar?

Informant	*Ståndpunkt*
LC1	N/A
LC2	Information till medarbetare om när det är läge att informera och när det inte är läge.
LC3	Vet ej. För egen del går jag på sunt förnuft.
LC4	Information och medvetande. I de risk- och sårbarhetsanalyser som görs årligen har informationssäkerhet tagits upp som ett scenario för detta året. Det rör dock inte bara läckage.
LA1	Det går via min chef. Inloggning i system kan vara olika och tar tid, vilket kan göra att användare inte loggar ut.
FC1	Information och självkontroll. Vi genomför även årliga kontroller som leds av andra utanför arbetsplatsen.
FC2	Utbildning i IT- och informationssäkerhet.
FC3	Information till personalen, krav på årliga säkerhetsprov (man visar att man känner till regelverket). Till del görs också tekniska åtgärder i informationssystemet (nätverket av arbetsplatsdatorer). För mobiltelefoni finns regler för hur de får användas. Inom byggnaden finns rum där mobiltelefoner ej får medföras (inlåses i skåp utanför).
FA1	Jag försöker upplysa mina medarbetare om när det finns risk att klassad information kan röjas. Det tas upp i utbildningar och tas upp på olika genomgångar.

Gällande hur de båda myndigheterna arbetar med att förbättra säkerheten för att förebygga att ett informationsläckage inträffar är de överens på ett plan. Till stor del menar myndigheterna att det handlar om att informera sina medarbetare för hur information ska hanteras. Tydligt är dock att informanterna från Försvarsmakten är mer säkerhetsmedvetna. Försvarsmakten genomför årligen kontroller och det är krav på årliga säkerhetsprov för anställda, samt att informanterna genomgår utbildning i IT- och informationssäkerhet. Observera även att det inte enbart är chefer som informerar utan även användare informerar medarbetare för när det finns risk att klassad information kan röjas. (Tabell 4.4)

Tabell 4.5 På vilket sätt påverkas organisationen av det förebyggande arbetet för informationsläckage för såväl positiva som negativa effekter?

Informant	*Ståndpunkt*
LC1	N/A
LC2	Vet ej.
LC3	Vet ej.
LC4	Tyvärr är det ofta så att kraven på öppenhet och flexibilitet ofta är i konflikt med kraven på informationssäkerhet. Dvs. att man upplever att lösningar som ska ge mer säkerhet är ett hinder. Lösenord och lösenordsbyte är ett sådant exempel. Inte ifrågasatt men ändå besvärligt för användarna.
FC1	Det skapar dagliga rutiner.
FC2	Många moment/rutiner är omständligare än om ingen information var sekretessbelagd.
FC3	Medvetenhet om att organisationen hanterar känslig och viktig information kan i sig vara stärkande för självkänslan och samhörighetskänslan. Men begränsningar avseende hur de tekniska stödsystemen får utnyttjas leder i många fall till irritation, negativa upplevelser vid jämförelse med bekantas mera öppna organisationer och i värsta fall medvetna kryphålslösningar i strid med regelverket, för att lösa uppgiften att bli klar med en uppgift i tid.

För tabell 4.5 är informanterna från Lunds Kommun och Försvarsmakten delvis överens i stora drag för hur de och organisationen påverkas av det förebyggande arbetet för att förhindra att informationsläckage inträffar. De menar att det skapar dagliga rutiner. Samtidigt är tre av informanterna inne på att det förebyggande arbetet upplevs som ett hinder eller är omständligare. En informant menar att detta kan leda till irritation eller negativa upplevelser vid verkställandet av uppgiften. Tänkvärt är dock att som en informant beskriver, att hanterandet av känslig och viktig information kan vara stärkande för självkänslan och samhörighetskänslan. Flera av informanterna från Lunds Kommun har dock ingen insikt i frågan. (Tabell 4.5)

Tabell 4.6 Finns det tekniska säkerhetsmekanismer finns installerade eller konfigurerade för att förhindra oavsiktligt informationsläckage?

Informant	*Ståndpunkt*
LC1	N/A
LC2	Vet ej.
LC3	Inte så vitt jag vet.
LC4	Ansvaret för tillgång till informationssystem ligger på systemägare (ofta verksamhetschef) och ansvaret för att se till att informationssystemen uppfyller lagar och regler ligger i det ansvaret och hos systemförvaltaren. Det finns också tydliga riktlinjer till vad man inte ska använda e-post till. I kommunen finns det inte möjlighet att automatiskt vidarebefordra e-post till externa e-postanvändare. Ett exempel på att försöka undvika att det oavsiktligt går iväg information.
LA1	Vet ej.
FC1	Ja på de flesta av våra system finns det ett stöd som skall hjälpa oss att inte göra fel.
FC2	Separata IT-system för sekretessbelagd information finns. Vissa system har filter på meddelandenivå (här: meddelande = dataformat, ej löptext).
FC3	Till del har jag inte kunskap om detta. Annonserade kontroller av telefoni (fast och mobil) görs årligen för att analysera efterlevnad av bestämmelser. Separerade system för intranät och externt nät (Internet) gäller på arbetsplatsen. Vissa sökningar på servrar efter felaktigt lagrade dokument med sekretessklassning (som således inte får förekomma i det öppna systemet) genomförs.
FA1	Ja.

Gällande frågan om det finns tekniska säkerhetsmekanismer installerade eller konfigurerade för att oavsiktligt förhindra informationsläckage på informationssystemen svarar informanterna här varierat. Till viss del har informanterna från Lunds Kommun inte någon större insikt i frågan. En informant från Lunds Kommun menar dock att systemen måste uppfylla lagar och regler och att det exempelvis finns restriktioner för e-mail till externa e-mailanvändare. Försvarsmakten är tydligare och framhäver att det finns stöd i systemen för att förhindra att fel inträffar. Det finns även filter i vissa system där information inte förekommer i löptext utan i dataformat för att på så sätt hantera sekretessbelagd information. En informant från Försvarsmakten framhäver även att det genomförs sökningar på servrar efter felaktigt lagrade dokument med sekretessklassning som inte får förekomma i det öppna systemet. (Tabell 4.6)

Tabell 4.7 Scenariofråga 1: Åtgärd vid scenario där ett tänkbart informationsläckage inträffar

Informant	*Ståndpunkt*
LC1	Ingen åtgärd.
LC2	Snarast meddela personen i fråga att dokumentet har tagits om hand.
LC3	Vet ej.
LC4	Svårt att säga.
LA1	Att påtala misstaget till den som hanterat. Chefen ansvarar för att hantera situationen.
FC1	Digniteten på dokumentet kommer att avgöra vad som händer på alla plan. Från kanske bara ett samtal om vikten av att hålla rätt på sina papper till en fullt ut anmälan om brott.
FC2	Partnern kontaktas och ombeds att ta hand om kopian och skydda den på ett tillbörligt sätt. Då scenariot inte torde uppstå annat än hos en partner som är SUA-upphandlad[2], därav torde partnern vara pålitlig och angelägen om att bevara vårt förtroende.
FC3	Det anmäls till vår interna Säkerhetstjänst, som handlägger ärendet enligt sina regelverk. Framhållas bör dock att kopiering i vanliga kopiatorer av känsliga dokument generellt är förbjuden på vår arbetsplats, eftersom de flesta kopiatorerna idag har minne, för senarelagd utskrift. Därvid behöver man inte glömma kvar dokumentet i kopiatorn för att det skall kunna röjas. Därför har vi inom huset särskilda kopiatorer godkända för kopiering av sådant material. Detta skall alla medarbetare känna till, vilket leder tillbaka till utbildningsbehov och krav på rutiner. Att samma situation råder vid besök hos andra bör vara uppenbart för alla medarbetare.
FA1	Jag meddelar min chef vad som inträffat.

Vidare har vi använt oss av scenariofrågor för att på så sätt få en förståelse för hur informanter förhåller sig till ett tänkbart informationsläckage. Scenariot för de informanter som är chefer innefattar att en underordnad av misstag glömt en kopia av känslig typ i en kopiator hos en extern partner där obehöriga nu kan ta del av informationen. Då båda myndigheterna har här delvis samma åsikt för hur scenariot ska hanteras. Två av informanterna menar på att meddela partnern eller personen ifråga att dokumentet har tagits om hand är åtgärden. En annan informant påpekar att det anmäls till intern Säkerhetstjänst som handlägger ärendet. (Tabell 4.7)

Scenariot för användare såg ut som följande: En användare skickar ett dokument via e-mail som innehåller information om personal. Detta skickas av misstag till fler personer än vad

[2] SUA-upphandlad: Säkerhetsskyddad upphandling (Fortifikationsverket, 2011)

som var menat. Exempel på dokument som har skickats kan vara lönelistor. Informanterna säger att det skulle meddela chefen om vad som inträffat och att chefen får ta ansvar för ett sådant scenario. (Tabell 4.7)

Vid dessa scenariers är det tydligt att Försvarsmakten är mer medvetna för hur de ska handla för vilka åtgärder som kan tas. Lunds Kommun är mer begränsad i sina svar för dessa scenariers.

Tabell 4.8 Scenariofråga 2: Åtgärd vid scenario där ett tänkbart informationsläckage inträffar

Informant	*Ståndpunkt*
LC1	Inget problem
LC2	Frågan är inte relevant för offentlig sektor. Som chef inom offentlig sektor måste jag ha kunskap om den meddelarfrihet som finns och att det inte är förenligt med svensk lagstiftning att efterforska vem som har lämnat information till massmedia.
LC3	Nej det finns ingen handlingsplan.
LC4	N/A
LA1	Känslig information i vår verksamhet är framförallt personinformation som styrs av sekretesslagar. Respektive verksamhet kan ha olika instruktioner för hanteringen, generellt sätt ligger ansvaret på respektive verksamhetschef.
FC1	Det finns en mängd olika planer på hur en sådan händelse skulle hanteras på min arbetsplats. Beroende på digniteten på informationen som läckt skulle olika faser av den i förväg planering att träda i kraft.
FC2	Menbedömning enligt gällande regelverk. I förekommande fall även polisanmälan.
FC3	Information skall ges till Säkerhetsansvarig enhet inom arbetsplatsen (finns väl definierad). Därtill informeras Informationsavdelningen och dess pressansvarige. En plan för agerande upprättas, där Juridiska staben involveras i arbetet.
FA1	Jag meddelar min chef vad som inträffat.

Vidare på nästa scenariofråga innefattar denna samma scenario för såväl användare som chefer. Scenariot inbegriper att känslig kundinformation har läckt till massmedia som kan skada organisationens anseende och trovärdighet. Vid detta scenario finns det en tydlig gräns på hur de ser på sin information och hur öppna organisationerna är. Informanterna från Lunds Kommun är mer öppna och hänvisar till att de är en offentlig sektor och att de måste ha kunskap om meddelarfrihet. Försvarsmakten är här mer återhållsamma och menar på att betydelsegraden av informationen avgör vad som sker men att en menbedömning ska göras enligt gällande regelverk där polisanmälan kan bli som påföljd. Även för detta scenario hävdar användarna från de båda myndigheterna att informera överordnanden är vad som gäller. (Tabell 4.8)

4.1.3 Konsekvenser av informationsläckage

Tabell 4.9 På vilket sätt kan informationsläckage påverka organisationen ur ett anseendemässigt perspektiv?

Informant	*Ståndpunkt*
LC1	N/A
LC2	Vet ej.
LC3	I mycket hög utsträckning. Vem vill få eller köpa tjänster eller varor från ett företag där medarbetarna inte är lojala?
LC4	Bristande förtroende.
FC1	Det skulle skada vårt anseende mycket om det gick att bevisa att vi hade läckt säkerhetsklassad information till någon otillbörlig person eller makt.
FC2	Dåligt anseende eller förtroende från allmänheten.
FC3	Anklagelser mot myndigheten om jäv, slarv, fusk eller bristande lojalitet är förödande för en skattefinansierad verksamhet som redan i utgångsläget ifrågasätts av många medborgare. Det är av central betydelse att allmänheten har förtroende för att verksamheten bedrivs på ett ärligt och kontrollerat sätt.

Informanterna fick svara på frågan hur ett informationsläckage kan påverka organisationen ur ett anseendemässigt perspektiv. Informanterna var eniga och menar att det skulle påverka dem i hög utsträckning. Det skulle påverka dem genom att det skadat anseendet och att de inte är lojala och inte går att lita på. En informant från Lunds Kommun menar att vem vill köpa varor eller tjänster från ett företag där medarbetarna inte är lojala. Informanter från Försvarsmakten förtydligar att det är av central betydelse att det finns förtroende från allmänheten gällande skattefinansierade verksamheter. Ett läckage skulle innebära anklagelser om slarv, fusk eller bristande lojalitet.(Tabell 4.9)

Tabell 4.10 Hur skulle ett informationsläckage påverka arbetsrutiner?

Informant	*Ståndpunkt*
LC1	Inget skulle påverka
LC2	Översyn av rutiner och arbetssätt.
LC3	Jag skulle bli ännu mer återhållsam med att ge information innan jag fått protokoll osv.
LC4	Det skulle ge merarbete i form av att klara ut situationen.
LA1	Kan ske i vissa fall beroende på arbetsuppgifter. Framförallt kan det skapa merarbete och sänka förtroendet.
FC1	Vi skulle eventuellt behöva skapas fler eller nya rutiner för hur ett visst arbete skall utföras.
FC2	Det skulle inte påverka. Alternativt nytt regelverk, nya rutiner.
FC3	Det skulle kunna innebära ännu större slutenhet, att arbetsgrupper mm. måste avgränsas ytterligare samt försvåra nödvändig informationsdelning, eftersom det sannolikt skulle medföra krav på större begränsningar. Sannolikt skulle det medföra merarbete utan att effekten höjs, dvs. ge lägre produktivitet.
FA1	Det innebär oftast ett tillfälligt merarbete för att korrigera det som inträffat.

Informanterna fick frågan hur ett informationsläckage skulle påverka deras arbetsrutiner. Informanterna från båda myndigheterna är eniga om att det skulle påverka deras arbetsrutiner i den mån att det skulle bli nya arbetsrutiner och protokoll för hur information hanteras. Enligt en informant från Försvarsmakten skulle det även kunna innebära större slutenhet eftersom arbetsgrupper måste avgränsas ytterligare och försvåra informationsdelningen. Detta skulle sannolikt medföra merarbete utan att effekten höjs, alltså lägre produktivitet. Värt att

notera är att informanterna från de båda myndigheterna i stort var eniga om att det skulle påverka dem i den mån att nya arbetsrutiner och protokoll skulle införas. (Tabell 4.10)

Tabell 4.11 Scenariofråga 1: Konsekvens vid scenario där ett tänkbart informationsläckage inträffar

Informant	*Ståndpunkt*
LC1	Vi har inga hemligheter
LC2	N/A
LC3	Vet ej
LC4	Detta beror på vilken verksamhet och vilken information. Sådant inträffar tyvärr.
LA1	Chefen ansvarar för att hantera situationen.
FC1	Kostnaden är svårt att uttala sig om men jag tror att den största effekten hos oss skulle påverka vårt anseende hos andra och ur ett fortsatt samarbetsperspektiv.
FC2	Kostnaden blir arbetstimmar för hanteringen av menbedömningen.
FC3	Kostnaden är helt avhängig karaktären på innehållet i det kvarglömda dokumentet.
FA1	Jag meddelar min chef vad som inträffat.

Informanterna fick en scenariofråga de skulle förhålla sig till. Scenariot för informanter som är chefer innefattar att en underordnad av misstag glömt en kopia av känslig typ i en kopiator hos en extern partner där obehöriga nu kan ta del av informationen. Informanterna menar att det beror på vad det är för typ av information som avgör vad konsekvenser blir för detta. Kostnaden skulle förmodligen bli merarbete för hanteringen av menbedömningen samt försämrat anseende ur ett samarbetsperspektiv. (Tabell 4.11)

Scenariot för användare såg ut som följande: En användare skickar ett dokument via e-mail som innehåller information om personal. Detta skickas av misstag till fler personer än vad som var menat. Exempel på dokument som har skickats kan vara lönelistor. Informanterna säger att det skulle meddela chefen om vad som inträffat och att chefen får ta ansvar för ett sådant scenario. Värt att notera för båda scenarios är att informanterna menar att konsekvensen av ett sådant scenario är beroende på vilken typ av information som läckaget berör.(Tabell 4.11)

Tabell 4.12 Scenariofråga 2: Konsekvens vid scenario där ett tänkbart informationsläckage inträffar

Informant	*Ståndpunkt*
LC1	Inget problem
LC2	Frågan är inte relevant för offentlig sektor. Som chef inom offentlig sektor måste jag ha kunskap om den meddelarfrihet som finns och att det inte är förenligt med svensk lagstiftning att efterforska vem som har lämnat information till massmedia.
LC3	Det hade påverkat vårt förtroende i negativ riktning. Det är viktigt att vi uppfattas som neutrala och objektiva.
LC4	N/A
FC1	Beroende på digniteten på informationen som läckt skulle olika faser av den i förväg planering att träda i kraft.
FC2	Det skulle inte påverka. Alternativt nytt regelverk, nya rutiner träda i kraft. Dåligt anseende eller förtroende från allmänheten.
FC3	I en tid där negativ publicitet varit mera vanligt förekommande än positiv sådan, påverkar det naturligtvis medarbetarna i deras syn på organisationen som arbetsgivare. Det blir tyngre att arbeta och i värsta fall blir alla skuldbelagda för att läckaget kunnat ske. Om det uppdagas vem som läckt blir det naturligtvis besvärande relationssituationer gentemot vederbörande, samt eventuellt ett rättsligt efterspel som påverkar även omgivningen.

Informanterna fick svara på ytterligare ett scenario. Scenariot inbegriper att känslig kundinformation har läckt till massmedia som kan skada organisationens anseende och trovärdighet. Informanterna från Lunds Kommun menar att detta scenario inte riktigt är relevant eftersom de är inom den offentliga sektorn, fast att det ändå skulle påverka dem. De menar att förtroendet hade påverkats i negativ riktning även fast de är i den offentliga sektorn. Informanterna från Försvarsmakten menar att det beror på digniteten på informationen som läcker ut. De menar även att nya regelverk och rutiner skulle träda i kraft. Värt att notera är att en av informanterna menar att det även skulle bli tyngre att arbeta och att alla på organisationen i värsta fall skulle bli skuldbelagda för att läckaget kunnat ske. Det skulle även kunna resultera i rättsligt efterspel.(Tabell 4.12)

5 Analys och Diskussion

I detta kapitel analyserar vi den empiri vi har samlat och kopplat den till den teori vi har i litteraturgenomgången. Detta kapitel struktureras upp efter temat som går genom hela uppsatsen, hot – åtgärder – konsekvenser.

5.1 Hot till informationsläckage

Informationsläckage är när intern information avslöjas och publiceras utanför organisationen. Informationsläckage har blivit ett större problem sedan konkurrensen i vårt samhälle har ökat. Det mesta pekar på att informationsläckage är ett problem, men alla organisationer anser inte att det är ett större problem. Informationsläckage var något de båda myndigheterna ansåg att det var tvungna att förhålla sig efter. Informanterna från Lunds Kommun ansåg att problemet var främst gentemot massmedia där informationen kan publiceras. Det är även något de måste förhålla sig gentemot eftersom att det är viktigt att politikerna kan lita på att de inte läcker informationen de hanterar, speciellt innan det är tänkt att informationen ska komma ut. Försvarsmakten anser att informationsläckage främst är ett problem gällande säkerhetsklassad information, och menar även att ett informationsläckage kan leda till onödigt mycket jobb att hantera rykten som kan uppstå (Tabell 4.1).

Det som framgår från de båda myndigheterna är att de anser att informationsläckage är ett problem och något de måste förhålla sig till. Skillnaden mellan myndigheterna är att Lunds Kommun menar att de jobbar inom den offentliga sektorn och måste även förhålla sig till meddelarfrihet och offentlighetsprincipen och därav är problemet inte lika relevant för dem. Försvarsmakten anser att det absolut är ett problem de måste förhålla sig till, även om de också måste förhålla sig till offentlighetsprincipen. Framförallt gällande säkerhetsklassad information som det blir jobb med att hantera och hantera de rykten som uppstår. (Tabell 4.1)

Vidare då myndigheterna ansåg att informationsläckage var ett problem de måste förhålla sig till är det relevant att undersöka vilka typer av hot de anser finnas. Det finns olika typer av hot gällande informationsläckage. Hot brukar delas in i internt och externt hot. Internt brukar manifestera sig genom en s.k. insiderattack. En insiderattack är det svåraste för en organisation att skydda sig emot eftersom de har auktoriserad tillgång till informationen (Sektion 2.1.3). Detta kan förekomma inom den egna organisationen där personal har tillgång till känslig information, men även via partners som vid exempelvis outsourcing. Eftersom outsourcing innebär att andra organisationer har tillgång till information ökar även risken för

informationsläckage. En nackdel är att risken finns att kontrollen minskar över informationsflödet vilket kan leda till ökat informationsläckage. (Sektion 2.1.4) Detta är något verksamheter försöker förebygga genom kontrakt och klausuler för de anställda. De båda myndigheterna är även av uppfattningen att det hot som är störst mot deras är organisation är internt hot (Tabell 4.2). Detta kan även styrkas genom litteraturgenomgången. I de myter som finns om informationsläckage är en av myterna att de flesta läckage sker genom en insiderattack. Denna myt hänger kvar sedan 80-talet då de vanligaste attackerna var en insiderattack men faktum är enligt litteraturgenomgången att externt attacker är ett större hot (Sektion 2.1.1, 2.1.5).

Vi förutsatte att båda myndigheterna skulle förhålla sig till informationsläckage eftersom att det borde påverka dem. Som resultatet från informanter tyder på var informationsläckage något som båda myndigheterna måste förhålla sig efter. Dock så är Försvarsmakten mer medveten om olika risker som finns och vi tolkar det som att Försvarsmakten har en bättre förståelse för informationsläckage. (Tabell 4.2) Vår uppfattning är att det beror på att de jobbar mer aktivt med informationsläckage ur olika aspekter som exempelvis hur organisationen ska skydda sig emot ett informationsläckage.

5.2 Åtgärder för informationsläckage

Idag har känslig information blivit mer viktigt för finansiella avdelningar, medicinska organisationer, säkerhetssektorer och verksamheter världen över. Om viktig information läcker ur organisationen kan detta innebära förödande konsekvenser. För att hantera informationsläckage krävs åtgärder för såväl innan som efter incidenten inträffat i form av förebyggande arbete, policys och handlingsplaner. (Sektion 2.2)

5.2.1 Policys

Vi ser det relevant att undersöka hur det förebyggande arbetet hanteras på de myndigheter vi undersökte, då det ligger till grund för att lindra eller förhindra informationsläckage. Med stöd från litteraturgenomgången kan vi se att det förebyggande arbetet kan ske på många olika sätt för att hantera det komplexa problemet informationsläckage utifrån olika aspekter. Det kan handla om brandväggar, kryptering eller verifiering för att säkra att informationen används av behöriga användare. Detta kan vara mekanismer för åtkomstkontroller som endast tillåter behöriga användare att använda känslig information genom åtkomstkontrollspolicys. Organisationer måste arbeta kontinuerligt och aktivt för att förhindra att informationsläckage uppstår. Att kombinera förebyggande och kontrollerande funktionalitet med tillgänglighet och effektivitet är en komplex uppgift gällande informationssystem. (Sektion 2.2)

När de båda myndigheterna svarade för hur de hanterar det förebyggande arbetet för att förhindra informationsläckage är de överens på ett plan för hur detta ska gå till. Till stor del menar båda att det handlar om att informera sina medarbetare för hur information ska hanteras tillsammans med självkontroll (Tabell 4.4). Detta kan kopplas till litteraturgenomgången där vi ser att en rekommenderad åtgärd genom policys är social styrning för anställda. Där ska anställda hjälpa varandra för beteende som kan orsaka informationsläckage liksom att de uppmuntras rapportera misstänkta hemsidor eller bifogade filer i e-mail som kan vara skadliga. På så sätt upptäcks misstänkt hot som tekniska säkerhetsmekanismer inte alltid spårar upp (Sektion 2.2.4). Värt att notera från Försvarsmakten är att det inte enbart är chefer som informerar medarbetare utan även användare informerar när det finns risk att säkerhetsklassad information kan röjas (Tabell 4.4).

En skillnad vi kan se för förebyggande arbete mellan de båda myndigheterna är att Försvarsmakten är mer säkerhetsmedvetna. Informanterna förklarar här att det årligen görs kontroller och säkerhetsprov för anställda, samt att informanterna genomgår utbildningar i IT- och informationssäkerhet (Tabell 4.4). Tydligt är också att informanterna måste förhålla sig till rutiner och att behovet för utbildning är stort (Tabell 4.7). Som vi kan se i litteraturen är detta en nödvändighet. Det är viktigt att anställda känner till säkerhetspolicys och rutiner och att de följer dem. Precis som att det är viktigt att övervaka anställda och se till att anställda inte har mer behörighet än vad de behöver. Därav bör behörig användning loggas och generera meddelanden till överordnade. Oplanerad behörighet borde generera en alarmering som sedan ska undersökas. (Sektion 2.2.4)

”[…] Framhållas bör dock att kopiering i vanliga kopiatorer av känsliga dokument generellt är förbjuden på vår arbetsplats, eftersom de flesta kopiatorerna idag har minne, för senarelagd utskrift. Därvid behöver man inte glömma kvar dokumentet i kopiatorn för att det skall kunna röjas. Därför har vi inom huset särskilda kopiatorer godkända för kopiering av sådant material. Detta skall alla medarbetare känna till, vilket leder tillbaka till utbildningsbehov och krav på rutiner.” (Bilaga 11, fråga 10)

5.2.2 Tekniska åtgärder

Utöver att använda sig av policys eller utbildning för att göra anställda medvetna för vilka risker och hot som kan uppstå och för hur man skyddar sig mot informationsläckage bör tekniska åtgärder implementeras. Även detta är en nödvändighet för att hantera information säkert. Det är inget problem som går att hantera med hjälp av enbart en lösning. Därför bör verksamheter använda sig av metoder som passar den specifika organisationen bäst. Att förebygga ett informationsläckage är en taktisk uppgift och är grundat på mycket analys. Det är exempelvis viktigt att ändra grundinställningar för åtkomstkontroll och att övervaka behöriga användare med nyckelorden tillit med verifiering. Organisationer måste säkerställa fjärrstyrda åtkomsttjänster, som att nätverk är öppna mot Internet liksom att det är viktigt att

övervaka och filtrera utgående nätverkstrafik. (Sektion 2.2.4, 2.2.1) För detta märks skillnaden mellan de olika myndigheterna tydligt (Tabell 4.6).

Till viss del har informanterna från Lunds Kommun ingen större insikt i frågan. Vilket kan tyckas märkligt då detta bör vara tydligt. Vi kan dock se att det finns restriktioner för hur e-mail ska hanteras och distribueras till externa e-mailanvändare utanför Lunds Kommun. Försvarsmakten är här tydlig för vilka tekniska åtgärder som finns implementerade. Som vi kan koppla från litteraturen har Försvarsmakten flera olika åtgärder för att förhindra informationsläckage, vilket är nödvändigt. Vad vi kan uppfatta är en stor del av detta de stöd som finns i systemen som ska förhindra att fel uppstår. Ytterligare finns det även filter i vissa system där information inte förekommer i löptext utan i dataformat för att på sätt hantera sekretessbelagd information. En informant från Försvarsmakten framhäver även att det genomförs sökningar på servrar efter felaktigt lagrade dokument med sekretessklassning som inte får förekomma i det öppna systemet. (Tabell 4.6) Detta är precis vad litteraturen rekommenderar. Övervakning och kontroll är något som litteraturen förespråkar för att förebygga informationsläckage (Sektion 2.2.4).

Samtidigt som det förebyggande arbetet är en nödvändighet för att skydda sig mot informationsläckage bör det inte påverka verksamhetens aktiviteter på sådant sätt att det stör den anställde. Det förebyggande arbetet och skyddsarbetet ska fungera så att det går obemärkt förbi av personal och inte hindra dem från att utföra deras dagliga arbete (Sektion 2.2.1). Men att det påverkar den anställde och dess rutiner i större eller mindre grad är inte så konstigt. Informanterna är delvis överens mellan de båda myndigheterna för hur de och organisationen påverkas av det förebyggande arbetet för att förhindra informationsläckage. Det skapar dagliga rutiner för hur information ska hanteras. Vad som är intressant och som kan återkopplas är att en del av informanterna upplever det förebyggande arbetet som ett hinder eller att rutiner blir omständligare. (Tabell 4.5) Detta tolkar vi som att de båda myndigheterna måste förbättra, då det kan leda till att policys eller rutiner försummas. Tänkvärt är dock att som en informant beskriver, att hanterandet av känslig och viktig information kan vara stärkande för självkänslan och samhörighetskänslan (Tabell 4.5).

”[…] Begränsningar avseende hur de tekniska stödsystemen får utnyttjas leder i många fall till irritation, negativa upplevelser vid jämförelse med bekantas mera öppna organisationer och i värsta fall medvetna kryphålslösningar i strid med regelverket, för att lösa uppgiften att bli klar med en uppgift i tid.” (Bilaga 11, fråga 8)

5.2.3 Handlingsplaner

Om ett informationsläckage nu inträffar trots de förebyggande åtgärder som finns är det viktigt att skapa en incidenthanteringsplan. Om och när ett dataintrång kan misstänkas ha skett måste organisationen vara redo att besvara detta. En effektiv incidenthanteringsplan hjälper att reducera skalan av intrång och försäkrar att bevisen samlas in på ett korrekt sätt.

Sedan kan organisationer även sysselsätta sig för incidenttestning. För att kunna sköta incidenthantering effektivt, måste organisationer praktisera och träna olika strategier för att besvara ett dataintrång. Detta kan vara, identifiering av hot, klassificering av hot, processdefinitioner, ordentlig bevishantering och scenarios som kan inträffa. (Sektion 2.2.4)

När vi nu även har undersökt hur de båda myndigheterna ser på och hanterar handlingsplaner kan vi konstatera att de hanterar detta på olika sätt. Där Försvarsmakten har mer tydligt regelverk för hur de ska gå tillväga är Lunds Kommun mer oförberedda och hanterar incidenter när de har inträffat. Informanterna från Försvarsmakten hävdar att en rapport ska konstrueras med avseende på menbedömning av informationsläckaget. (Tabell 4.3) Försvarsmakten arbetar således mer efter hur litteraturen rekommenderar. Detta anser vi är viktigt att göra för att på sätt lindra den skada som kan uppstå vid informationsläckage samt effektivt hantera situationen. Vi kan även konstatera att de informanter som är användare inte har en större roll i handlingsplanen, utan det handlar om att informera överordnad chef (Tabell 4.3).

Vidare för de scenarier vi använder i undersökningen kan vi även här se att Försvarsmakten har tydligare reglemente för hur de ska gå tillväga. Vi ser även en tydligare öppenhet från Lunds Kommun, liksom en oförbereddhet för hur de ska hantera de scenarion vi ponerar uppstå. Båda myndigheterna är dock delvis överens för hur det första scenariot initialt ska hanteras; genom att meddela partnern eller personen ifråga att dokumentet har tagits om hand. Försvarsmakten vidareutvecklar dock sina svar och menar att det anmäls till intern Säkerhetstjänst. Ytterligare en informant från Försvarsmakten hävdar dock att scenariot inte borde uppstå då partnern ifråga för scenariot borde vara SUA-upphandlad (Tabell 4.7). Att Lunds Kommun inte utvecklar sina svar här speglar tillbaka på tabell 4.3 där de klart uttrycker att de inte har en klar handlingsplan när ett informationsläckage inträffar utan att varje fall behandlas när de inträffar.

Till sist för temat åtgärder påvisas den öppenhet vi tidigare nämnde för Lunds Kommun i jämförelse med Försvarsmakten än mer tydligt för det sista scenariot. En informant förklarar tydligt att scenariot inte är relevant då Lunds Kommun är inom den offentliga sektorn och således måste förhålla sig till meddelarfrihet. (Tabell 4.8) De måste alltså förhålla sig efter offentlighetsprincipen som exempelvis enligt Tryckfrihetsförordning (1949:105) 11§ beskriver att en handling är allmän om den förvaras på en myndighet och har inkommit till myndigheten eller upprättats där (Sektion 2.1).

Visserligen måste även Försvarsmakten förhålla sig till offentlighetsprincipen, men information får dock inte vara öppet som kan beröra rikets säkerhet. (Sektion 2.1) Således är Försvarsmakten mer restriktiva i sina svar. Informanterna påpekar att det finns en mängd olika planer som kan träda i kraft men att digniteten på informationen avgör vad som sker (Tabell 4.8). Men som kan hänvisas till litteraturen är en incidenthanteringsplan en nödvändighet för att reducera skalan av intrånget (Sektion 2.2.4). Försvarsmakten förklarar att en rapport ska konstrueras med avseende på menbedömning där även Juridiska staben kan involveras med en anmälan som påföljd (Tabell 4.8). För båda scenariofrågorna kan vi se att

användarna inte alls är särskilt delaktiga i handlingsplanen eller vet hur scenariot ska hanteras utan användarna från såväl Lunds Kommun som Försvarsmakten hänvisar till att meddela överordnad chef för vad som inträffat (Tabell 4.7, 4.8).

5.3 Konsekvenser av informationsläckage

Trots framsteg de senaste åren inom obligatorisk åtkomstkontroll i databassystem är dagens informationslager fortfarande sårbara för attacker som kan resultera i informationsläckage. Utan stöd för att hantera dessa attacker, så kan känslig information riskera offentliggörande på grund av utsläpp av mindre känslig men relaterad information. Förmågan att skydda sig emot dessa olämpliga läckor skulle vara fördelaktigt och är av stor betydelse för myndigheter, offentliga och privata institutioner. Det är av stor betydelse eftersom det numera är en skyldighet att göra delar av informationen tillgänglig och offentlig för utomstående. (Sektion 2.3)

Information är något som är av stort värde för organisationer samtidigt som det är något av det svåraste att skydda. För organisationer har hotet alltid funnits att information kan avslöjas och spridas (Sektion 1.1). Information som för tidigt läckta årsredovisningar, publikationer eller arbetsdokument som inte bör läckas eller som endast är menat för ”stängda dörrar”, dvs. information som är känslig då den kan skada personer eller organisationer om den läcks utanför organisationen. Informanterna är eniga om att ett informationsläckage skulle påverka dem. Det skulle främst påverka och skada dem genom att deras anseende och trovärdighet skulle kompromissas (Tabell 4.6). Detta kan kopplas mot de konsekvenser som USA:s Försvarsmakt fick erfara då Wikileaks publicerade tusentals sekretessbelagda dokument för amerikanska militära loggar för kriget i Irak och Afghanistan. Det var förödande och försämrade deras anseende och förtroende avsevärt och de fick hård kritik från omvärlden. Detta kan även innebära att vad som tidigare misstänkts har skett kan verifieras genom läckta dokument (Sektion 2.3.1).

”[…] Vem vill få eller köpa tjänster/varor från ett företag där medarbetarna inte är lojala?” (Bilaga 7, fråga 6)

Eftersom de båda myndigheterna är inom den offentliga sektorn innebär det att de är skattefinansierade. Förtroende är av central betydelse för organisationerna och anklagelse om slarv, fusk eller bristande lojalitet är dåligt för deras anseende och förödande (Tabell 4.6).

Ett informationsläckage kan påverka organisationer på fler sätt än att anseendet och förtroendet försämras. Det kan även påverka de anställdas arbetsrutiner. Merparten av informanterna från Lunds kommun är av åsikten att ett informationsläckage skulle påverka deras arbetsrutiner, på så sätt att arbetssätt och rutiner skulle ses över. Försvarsmaktens informanter menar också att det skulle innebära fler eller nya rutiner för hur arbetet ska

utföras. Informationsläckaget skulle även leda till att personalen skulle vara mer återhållsamma med att lämna ut information tills de har fått protokoll. Återhållsamheten och de nya rutinerna skulle leda till att organisationen arbetar mer ineffektivt. Detta blir en konsekvens av informationsläckaget eftersom att det leder till fler eller ändrade rutiner som i sin tur leder till ökat merarbete utan att effektiviteten höjs, det vill säga lägre produktivitet (Tabell 4.7). Detta är givetvis något som är oönskat för en organisation, ökad andel merarbete utan höjd effekt vilket Försvarsmakten menar att kostnaden hade blivit.

För att vidare undersöka hur de förhåller sig till informationsläckage och hur det kan påverka dem gav vi informanterna från de båda myndigheterna scenariofrågor. Utifrån de svar som presenteras i empirin går det att tolka att konsekvenserna för ett sådant scenario är beroende på vad det är för typ av information som läcks utanför organisationen. Vi vill även undersöka vad kostnaden för ett sådant scenario skulle bli. Det nämns ingen kostnad ur ett ekonomiskt perspektiv förutom det merarbetet för att hantera menbedömningen för informationsläckaget. De andra kostnader och konsekvenser som går att tolka ur informanternas svar är försämrat anseende ur ett samarbetsperspektiv (Tabell 4.8). Detta är givetvis något som inte är bra för någon organisation, och eftersom att myndigheter kan ha många samarbetspartners är detta något som bör undvikas.

När vi undersökte hur användare skulle förhålla sig till att de skulle ha orsakat ett läckage genom slarv visade sig att de inte visste hur de skulle hantera situationen. Det var chefen som skulle informeras om det inträffade och låta chefen göra en menbedömning (Tabell 4.9). Det kan tolkas som att användarna inte har vetskap och kunskap för hur en sådan situation hanteras. Det går även att tolka det som att det saknas kunskap om hur informationsläckage kan uppstå och vad konsekvenserna kan bli av det.

Vi undersökte även hur det skulle påverka dem om känslig kundinformation kom ut.
Det som går att tolka från informanterna svar från Lunds Kommun på detta scenario är att de inte är helt eniga i fråga. En del menar att det inte riktigt skulle påverka dem eftersom att de är inom den offentliga sektorn samtidigt som andra menar att det skulle påverka dem. Informanterna från Lunds Kommun är således inte helt eniga om de skulle påverkas eller inte. De som är av uppfattningen att de skulle påverkas menar att anseende är något som främst hade påverkats. Försvarsmakten menar att det beror på digniteten av informationen som läcker ut och därför är svårt att svara på. Ett sådant scenario skulle även innebära att nya regelverk och rutiner skulle träda i kraft. Det skulle även kunna bli tyngre att arbeta och att de skulle kunna bli skuldbelagda för att informationsläckaget kunnat ske. Det skulle även kunna resultera i rättsliga efterspel om det kommer fram vem som varit orsak till läckaget (Tabell 4.9). Detta är konsekvenser som drabbar personal individuellt och givetvis något som varje person vill undvika. Att bli skuldbelagd för ett informationsläckage är något som gärna undviks. Det går även att tolka ur deras resonemang att de kanske inte är fullt medvetna om att även fast de är inom den offentliga sektorn så kan även de drabbas av informationsläckage. Vi är helt övertygande om att fastän de följer offentlighetsprincipen har de även information som inte får vara helt öppna i vissa sammanhang eller får publiceras utanför deras organisation.

6 Slutsats

Syftet med denna studie var att besvara vår forskningsfråga: *Hur påverkas organisationer av informationsläckage?* Med följande underfråga: *Vad finns det för handlingsplaner och policys vid informationsläckor och hur förebyggs detta?*

För att besvara vår forskningsfråga har vi ställt upp ett ramverk och en struktur genom hela uppsatsen som först har inneburit att skapa en förståelse för informationsläckage. För att sedan gå djupare och analysera hur informationsläckage kan förebyggas, liksom hur organisationer påverkas. Utifrån vår analys kan vi konstatera att konsekvenserna för ett informationsläckage hade främst påverkat myndigheternas anseende, trovärdighet och förtroende. Gällande vår underfråga är det tydligt att myndigheterna har handlingsplaner och använder förebyggande åtgärder för att hantera informationsläckage. Handlingsplanerna är inte specifika utan anpassas från fall till fall, beroende på digniteten på informationen som har läckt. Policys som finns är att man informerar sina medarbetare om hur informationen ska hanteras tillsammans med självkontroll.

Vår slutsats är att informationsläckage är något alla organisationer måste förhålla sig efter då det kan ge konsekvenser för hela organisationen såväl som den enskilde anställde. Tydligt är att de båda myndigheterna jobbar aktivt med att förhålla sig efter och förebygga att ett informationsläckage kan inträffa. Det är även påtagligt att Försvarsmakten har en större medvetenhet och kunskap gällande detta. Vilket vi anser vara en nödvändighet i hanterandet av informationssäkerhet.

Ett informationsläckage kan även påverka samarbetsperspektivet som kan leda till att andra organisationer eller samarbetspartners inte vill fortsätta samarbetet. Informationsläckaget kan innebära att nya arbetsrutiner, regelverk och moment tillkommer som blir omständligare. Detta eftersom det måste finnas restriktioner för hur information får hanteras. Informationsläckage kan till och med leda till att en slutenhet uppstår inom organisationen som med följd av detta ledar till en minskad informationsdelning. För att hantera ett informationsläckage uppstår ofta ett merarbete vilket kan leda till att organisationen blir ineffektiv och att lägre produktivitet uppstår.

Vi anser vi att det måste finnas en ökad medvetenhet och förståelse för informationsläckage. Organisationer som hanterar sekretessbelagd information eller information av känslig natur, måste arbeta aktivt med att förebygga informationsläckage. Organisationer måste således använda flera olika typer av åtgärder för att förhindra informationsläckage. Detta inkluderar policys för hur organisationer hanterar information samt handlingsplaner för att bemöta ett

eventuellt informationsläckage. Detta eftersom informationsläckage kan ha förödande konsekvenser för en organisation, såväl ekonomiska som organisatoriska.

Bilaga 1 – Följebrev Chefer

Du mottar detta brev då du arbetar för en myndighet eller liknande och är chef och har insikt inom organisationen.

Syftet med dessa frågor är att undersöka hur informationsläckage påverkar organisationer och dess användare, samt hur användaren kan vara med att förebygga att informationsläckage inträffar.

Undersökningen är en del av vår kandidatuppsats vid institutionen för Informatik vid Lunds universitet. Vår förhoppning är att utreda hur organisationen arbetar med att förebygga informationsläckage samt hur organisationen hanterar ett eventuellt informationsläckage och påverkas av detta.

Förväntat utfall med denna uppsats är större klarhet i hur handlingsplaner ser ut och hur pass förberedd organisationen är. Dessutom vill vi ha insikt i hur ett informationsläckage påverkar en organisation.

Samtliga svar behandlas högst konfidentiellt och används endast ur ett undersökningsperspektiv.

Beroende på utfall av undersökningen kan det hända att vi återkommer med följdfrågor för att förtydliga vissa svar. Vi kommer givetvis att återkoppla för att låta er ta del av slutprodukten.

Vi tackar på förhand för din medverkan!

Henrik Johnsson och Tobias Håkansson

Bilaga 2 – Frågeformulär Chefer

1: Anser du att informationsläckage är ett problem som du måste förhålla dig efter? Förklara ditt svar.

För att få förståelse för hur informationsläckage kan ske har vi nedan några exempel:

- För tidigt läckta årsredovisningar
- Läckta publikationer
- Läckta arbetsdokument
- Läckta e-mail
- Läckta mötesprotokoll
- Läckt information för enskild persons kännedom om ett visst förhållande

Svar:

2: Hur ser handlingsplanen ut om information läcks utan tillåtelse utanför er organisation? Informationen är känslig, exempelvis material som innehåller information om nya prototyper, planer eller mötesprotokoll.

Svar:

3: Har ni olika handlingsplaner/checklistor för olika typer av informationsläckage?

Svar:

4: På vilket sätt arbetar ni med att förbättra säkerheten för att förebygga informationsläckage?

Svar:

5: Vilket hot gällande informationsläckage anser du är det största hotet mot din organisation, internt eller externt hot? Förklara.

Svar:

6: På vilket sätt kan informationsläckage påverka organisationen ur ett anseendemässigt perspektiv?

Svar:

7: Hur skulle ett informationsläckage påverka dina arbetsrutiner?

Svar:

8: På vilket sätt påverkas organisationen av det förebyggande arbetet för informationsläckage för såväl positiva som negativa effekter?

Svar:

9: Finns det tekniska säkerhetsmekanismer installerade/konfigurerade för att förhindra oavsiktligt informationsläckage, t ex via e-mail eller annat kommunikationsmedium?

Svar:

Scenariofrågor :

10: En användare har varit på besök hos en extern partner. Han har där använt kopiatorn och av misstag glömt en kopia av ett dokument i kopiatorn. Dokumentet som blev kvarglömt är av känslig typ och obehöriga kan nu ta del av denna information samt publicera den vilket kan vara oangenämt.

- *Hur hanteras ett sådant scenario?*
- *Vad blir kostnaden ifall ett sådant scenario inträffar, ur ett ekonomiskt och ett organisatoriskt perspektiv?*

Svar:

11: Ett läckage har skett där exempelvis känslig kundinformation har läckt ut från er avdelning. Dessa hemligheter har läckts till pressen och kan skada organisationens anseende och trovärdighet.

- *Finns det en färdig handlingsplan för hur man hanterar en sådan situation? Hur ser en sådan handlingsplan ut?*
- *Hur påverkar ett sådant scenario organisationen?*

Svar:

Bilaga 3 – Följebrev Användare

Du mottar detta brev då du arbetar för en myndighet eller liknande och är en användare av informationssystem eller andra kommunikationsmedium.

Syftet med dessa frågor är att undersöka hur informationsläckage påverkar organisationer och dess användare, samt hur användaren kan vara med att förebygga att informationsläckage inträffar.

Undersökningen är en del av vår kandidatuppsats vid institutionen för Informatik vid Lunds universitet. Vår förhoppning är att utreda hur organisationen arbetar med att förebygga informationsläckage samt hur organisationen hanterar ett eventuellt informationsläckage och påverkas av detta.

Förväntat utfall med denna uppsats är större klarhet i hur handlingsplaner ser ut och hur pass förberedd organisationen är. Dessutom vill vi ha insikt i hur ett informationsläckage påverkar en organisation. Samtliga svar behandlas högst konfidentiellt och används endast ur ett undersökningsperspektiv.

Beroende på utfall av undersökningen kan det hända att vi återkommer med följdfrågor för att förtydliga vissa svar. Vi kommer givetvis att återkoppla för att låta er ta del av slutprodukten.

Vi tackar på förhand för din medverkan!

Henrik Johnsson och Tobias Håkansson

Bilaga 4 – Frågeformulär Användare

1: Anser du att informationsläckage är ett problem som du måste förhålla dig efter? Förklara ditt svar.

För att få förståelse för hur informationsläckage kan ske har vi nedan några exempel:

- För tidigt läckta årsredovisningar
- Läckta publikationer
- Läckta arbetsdokument
- Läckta e-mail
- Läckta mötesprotokoll
- Läckt information för enskild persons kännedom om ett visst förhållande

Svar:

2: Hur ser din roll ut i handlingsplanen för hanterandet av ett informationsläckage?

Svar:

3: På vilket sätt ingår det i dina arbetsuppgifter att hantera och kontrollera förebyggandet av informationsläckage?

Svar:

4: På vilket sätt kan du påverka arbetet med förebyggande åtgärder mot informationsläckage?

Svar:

5: Vilket är det största hotet gällande informationsläckage mot din organisation, internt eller externt hot? Förklara.

Svar:

6: Anser du att det finns ett förebyggande arbete mot informationsläckage som påverkar dina arbetsrutiner? Förklara.

Svar:

7: Hur skulle ett informationsläckage påverka dina arbetsrutiner?

Svar:

8: Hur känner du kring att du skulle kunna orsaka ett informationsläckage genom oförsiktighet eller ovetskap?

Svar:

9: Finns det tekniska säkerhetsmekanismer installerade/konfigurerade för att förhindra oavsiktligt informationsläckage, t ex via e-mail eller annat kommunikationsmedium?

Svar:

Scenariofrågor:

10: En användare skickar ett dokument via e-mail som innehåller information om personal. Detta skickas av misstag till fler personer än vad som var menat. Exempel på dokument som har skickats kan vara lönelistor.

- *Hur ser en handlingsplan ut för att bemöta detta misstag?*
- *Vad blir konsekvenserna av ett sådant scenario?*

Svar:

11: Ett läckage har skett där exempelvis känslig kundinformation har läckt ut från er avdelning. Dessa hemligheter har läckts till pressen och kan skada organisationens anseende och trovärdighet.

Finns det policys för hur man hanterar informationsläckage och hur påverkar det arbetsrutinerna?

Om ja; *Hur kontrolleras det att användaren förhåller sig till policys?*

Om nej: *Vad anser du om policys för informationshantering för att förhindra informationsläckage inom er organisation?*

Svar:

Bilaga 5 – Informant LC1

H= Hot, Å = Åtgärd, K = Konsekvens

Fråga	**1:** Anser du att informationsläckage är ett problem som du måste förhålla dig efter? Förklara ditt svar. För att få förståelse för hur informationsläckage kan ske har vi nedan några exempel: • För tidigt läckta årsredovisningar • Läckta publikationer • Läckta arbetsdokument • Läckta e-mail • Läckta mötesprotokoll • Läckt information för enskild persons kännedom om ett visst förhållande	
Svar	**Inga problem**	**H**
Fråga	**2:** Hur ser handlingsplanen ut om information läcks utan tillåtelse utanför er organisation? Informationen är känslig, exempelvis material som innehåller information om nya prototyper, planer eller mötesprotokoll.	
Svar	**Inga problem, inga handlingsplaner**	**Å**
Fråga	**3:** Har ni olika handlingsplaner/checklistor för olika typer av informationsläckage?	
Svar		
Fråga	**4:** På vilket sätt arbetar ni med att förbättra säkerheten för att förebygga informationsläckage?	
Svar		
Fråga	**5:** Vilket hot gällande informationsläckage anser du är det största hotet mot din organisation, internt eller externt hot? Förklara.	
Svar		
Fråga	**6:** På vilket sätt kan informationsläckage påverka organisationen ur ett anseendemässigt perspektiv?	
Svar		
Fråga	**7:** Hur skulle ett informationsläckage påverka dina arbetsrutiner?	
Svar	**Inget**	**K**
Fråga	**8:** På vilket sätt påverkas organisationen av det förebyggande arbetet för informationsläckage för såväl positiva som negativa effekter?	
Svar		

Fråga	**9:** Finns det tekniska säkerhetsmekanismer installerade/konfigurerade för att förhindra oavsiktligt informationsläckage, t ex via e-mail eller annat kommunikationsmedium?	
Svar		
Fråga	**10:** En användare har varit på besök hos en extern partner. Han har där använt kopiatorn och av misstag glömt en kopia av ett dokument i kopiatorn. Dokumentet som blev kvarglömt är av känslig typ och obehöriga kan nu ta del av denna information samt publicera den vilket kan vara oangenämt. • *Hur hanteras ett sådant scenario?* • *Vad blir kostnaden ifall ett sådant scenario inträffar, ur ett ekonomiskt och ett organisatoriskt perspektiv?*	
Svar	**Ingen åtgärd, vi har inga hemligheter**	**Å, K**
Fråga	**11:** Ett läckage har skett där exempelvis känslig kundinformation har läckt ut från er avdelning. Dessa hemligheter har läckts till pressen och kan skada organisationens anseende och trovärdighet. • *Finns det en färdig handlingsplan för hur man hanterar en sådan situation? Hur ser en sådan handlingsplan ut?* • *Hur påverkar ett sådant scenario organisationen?*	
Svar	**Inget problem**	**Å, K**

Bilaga 6 – Informant LC2

H= Hot, Å = Åtgärd, K = Konsekvens

Fråga	**1:** Anser du att informationsläckage är ett problem som du måste förhålla dig efter? Förklara ditt svar. För att få förståelse för hur informationsläckage kan ske har vi nedan några exempel: • För tidigt läckta årsredovisningar • Läckta publikationer • Läckta arbetsdokument • Läckta e-mail • Läckta mötesprotokoll • Läckt information för enskild persons kännedom om ett visst förhållande	
Svar	**Ja. Främst i relationen till läckage gentemot massmedia. Som chef inom offentlig sektor måste jag ha kunskap om den meddelarfrihet som finns och att det inte är förenligt med svensk lagstiftning att efterforska vem som har Lämnat Information till massmedia.**	**H**
Fråga	**2:** Hur ser handlingsplanen ut om information läcks utan tillåtelse utanför er organisation? Informationen är känslig, exempelvis material som innehåller information om nya prototyper, planer eller mötesprotokoll.	
Svar	**Finns ingen entydig handlingsplan. Bedömningar får ske från fall till fall.**	**Å**
Fråga	**3:** Har ni olika handlingsplaner/checklistor för olika typer av informationsläckage?	
Svar	**Nej**	**Å**
Fråga	**4:** På vilket sätt arbetar ni med att förbättra säkerheten för att förebygga informationsläckage?	
Svar	**Information till medarbetare om när det är läge att informera och när det inte är läge.**	**Å**
Fråga	**5:** Vilket hot gällande informationsläckage anser du är det största hotet mot din organisation, internt eller externt hot? Förklara.	
Svar	**Vet ej.**	**H**
Fråga	**6:** På vilket sätt kan informationsläckage påverka organisationen ur ett anseendemässigt perspektiv?	
Svar	**Vet ej.**	**K**
Fråga	**7:** Hur skulle ett informationsläckage påverka dina arbetsrutiner?	
Svar	**Översyn av rutiner och arbetssätt.**	**K**

Fråga	**8:** På vilket sätt påverkas organisationen av det förebyggande arbetet för informationsläckage för såväl positiva som negativa effekter?	
Svar	**Vet ej.**	**K**
Fråga	**9:** Finns det tekniska säkerhetsmekanismer installerade/konfigurerade för att förhindra oavsiktligt informationsläckage, t ex via e-mail eller annat kommunikationsmedium?	
Svar	**Vet ej.**	**Å**
Fråga	**10:** En användare har varit på besök hos en extern partner. Han har där använt kopiatorn och av misstag glömt en kopia av ett dokument i kopiatorn. Dokumentet som blev kvarglömt är av känslig typ och obehöriga kan nu ta del av denna information samt publicera den vilket kan vara oangenämt. • *Hur hanteras ett sådant scenario?* • *Vad blir kostnaden ifall ett sådant scenario inträffar, ur ett ekonomiskt och ett organisatoriskt perspektiv?*	
Svar	**Snarast meddela personen i fråga att dokumentet har tagits om hand.**	**Å**
Fråga	**11:** Ett läckage har skett där exempelvis känslig kundinformation har läckt ut från er avdelning. Dessa hemligheter har läckts till pressen och kan skada organisationens anseende och trovärdighet. • *Finns det en färdig handlingsplan för hur man hanterar en sådan situation? Hur ser en sådan handlingsplan ut?* • *Hur påverkar ett sådant scenario organisationen?*	
Svar	**Frågan är inte relevant för offentlig sektor. Se svar på fråga nr 1.**	**Å, K**

Bilaga 7 – Informant LC3

H= Hot, Å = Åtgärd, K = Konsekvens

Fråga	**1:** Anser du att informationsläckage är ett problem som du måste förhålla dig efter? Förklara ditt svar. För att få förståelse för hur informationsläckage kan ske har vi nedan några exempel: • För tidigt läckta årsredovisningar • Läckta publikationer • Läckta arbetsdokument • Läckta e-mail • Läckta mötesprotokoll • Läckt information för enskild persons kännedom om ett visst förhållande	**H**
Svar	**Jag anser att i rollen som budgetchef är det viktigt med integritet. Politikerna måste kunna lite på att det som avhandlas under exempelvis en budgetprocess inte förs vidare förrän de vill.**	
Fråga	**2:** Hur ser handlingsplanen ut om information läcks utan tillåtelse utanför er organisation? Informationen är känslig, exempelvis material som innehåller information om nya prototyper, planer eller mötesprotokoll.	**Å**
Svar	**Vad jag vet har vi inge sådan handlingsplan. En kommun lever ju i allra högsta grad efter offentlighetsprincipen och att så mycket som möjligt ska vara tillgängligt.**	
Fråga	**3:** Har ni olika handlingsplaner/checklistor för olika typer av informationsläckage?	**Å**
Svar	Som sagt, nej inte såvitt jag vet.	
Fråga	**4:** På vilket sätt arbetar ni med att förbättra säkerheten för att förebygga informationsläckage?	**Å**
Svar	**Vet ej. För egen del går jag på sunt förnuft.**	
Fråga	**5:** Vilket hot gällande informationsläckage anser du är det största hotet mot din organisation, internt eller externt hot? Förklara.	**H**
Svar	**I en politiskt styrd organisation är det politiker som ska fatta beslut och kommunicera dem. Vi tjänstemän ska arbeta utifrån fattade beslut, oavsett vad man själv tycker. Om vi läcker information i beslutsprocessen eller har får många privata åsikter kan verkställigheten påverkas.**	
Fråga	**6:** På vilket sätt kan informationsläckage påverka organisationen ur ett anseendemässigt perspektiv?	**K**

Svar	**I mycket hög utsträckning. Vem vill få eller köpa tjänster/varor från ett företag där medarbetarna inte är lojala?**	
Fråga	**7:** Hur skulle ett informationsläckage påverka dina arbetsrutiner?	**K**
Svar	**Jag skulle bli ännu mer återhållsam med att ge information innan jag fått protokoll osv.**	
Fråga	**8:** På vilket sätt påverkas organisationen av det förebyggande arbetet för informationsläckage för såväl positiva som negativa effekter?	**K**
Svar	**Vet ej.**	
Fråga	**9:** Finns det tekniska säkerhetsmekanismer installerade/konfigurerade för att förhindra oavsiktligt informationsläckage, t ex via e-mail eller annat kommunikationsmedium?	**Å**
Svar	Inte så vitt jag vet.	
Fråga	**10:** En användare har varit på besök hos en extern partner. Han har där använt kopiatorn och av misstag glömt en kopia av ett dokument i kopiatorn. Dokumentet som blev kvarglömt är av känslig typ och obehöriga kan nu ta del av denna information samt publicera den vilket kan vara oangenämt. • *Hur hanteras ett sådant scenario?* • *Vad blir kostnaden ifall ett sådant scenario inträffar, ur ett ekonomiskt och ett organisatoriskt perspektiv?*	**Å, K**
Svar	**Vet ej.**	
Fråga	**11:** Ett läckage har skett där exempelvis känslig kundinformation har läckt ut från er avdelning. Dessa hemligheter har läckts till pressen och kan skada organisationens anseende och trovärdighet. • *Finns det en färdig handlingsplan för hur man hanterar en sådan situation? Hur ser en sådan handlingsplan ut?* • *Hur påverkar ett sådant scenario organisationen?*	**Å, K**
Svar	**Nej det finns ingen handlingsplan.** **Det hade påverkat vårt förtroende i negativ riktning. Det är viktigt att vi uppfattas som neutrala och objektiva.**	

Bilaga 8 – Informant LC4

H= Hot, Å = Åtgärd, K = Konsekvens

Fråga	**1:** Anser du att informationsläckage är ett problem som du måste förhålla dig efter? Förklara ditt svar. För att få förståelse för hur informationsläckage kan ske har vi nedan några exempel: • För tidigt läckta årsredovisningar • Läckta publikationer • Läckta arbetsdokument • Läckta e-mail • Läckta mötesprotokoll • Läckt information för enskild persons kännedom om ett visst förhållande	
Svar	**Ja, det kan vara ett problem som finns i flera verksamheter. Informationssäkerhetsansvaret ligger på verksamhetscheferna. För infrastruktursystem ligger ansvaret gemensamt på Kommunkontoret, kommunikationsavdelningen.**	**H**
Fråga	**2:** Hur ser handlingsplanen ut om information läcks utan tillåtelse utanför er organisation? Informationen är känslig, exempelvis material som innehåller information om nya prototyper, planer eller mötesprotokoll.	
Svar	**Ansvaret ligger hos linjechefer och beroende på vilken typ av information det handlar om hanteras det olika. Det mesta av vår information är offentlig dock.**	**Å**
Fråga	**3:** Har ni olika handlingsplaner/checklistor för olika typer av informationsläckage?	
Svar	**Inte specifikt för läckage. Det finns informationssäkerhetsplaner för resp system. Det finns policies kring hantering av information och epost tex. Det kan i vissa verksamheter finnas spec rutiner om man tagit fram det men inte några generella. Vid misstanke om läckage eller missbruk kan verksamheten vända sig till kommunikationsavdelningen för stöd.**	**Å**
Fråga	**4:** På vilket sätt arbetar ni med att förbättra säkerheten för att förebygga informationsläckage?	
Svar	**Information och medvetande.I de risk och sårbarhetsanalyser som görs årligen har informationssäkerhet tagits upp som ett scenario för detta året. Det rör dock inte bara läckage.**	**Å**
Fråga	**5:** Vilket hot gällande informationsläckage anser du är det största hotet mot din organisation, internt eller externt hot? Förklara.	
Svar	**Troligen internt pga misstag, nyfikenhet. Det finns inte mycket affärshemligheter i kommunen som i privata företag.**	**H,K**

Fråga	**6:** På vilket sätt kan informationsläckage påverka organisationen ur ett anseendemässigt perspektiv?	
Svar	**Bristande förtroende.**	**K**
Fråga	**7:** Hur skulle ett informationsläckage påverka dina arbetsrutiner?	
Svar	**Det skulle ge merarbete i form av att klara ut situationen.**	**K**
Fråga	**8:** På vilket sätt påverkas organisationen av det förebyggande arbetet för informationsläckage för såväl positiva som negativa effekter?	
Svar	**Tyvärr är det ofta så att kraven på öppenhet och flexibilitet ofta är i konflikt med kraven på informationssäkerhet. Dvs att man upplever att lösningar som ska ge mer säkerhet är ett hinder.** **Lösenord och lösenordsbyte är ett sådant exempel. Inte ifrågasatt men ändå besvärligt för användarna.**	**K**
Fråga	**9:** Finns det tekniska säkerhetsmekanismer installerade/konfigurerade för att förhindra oavsiktligt informationsläckage, t ex via e-mail eller annat kommunikationsmedium?	
Svar	**Ansvaret för tillgång till informationssystem ligger på systemägare (ofta verksamhetschef) och ansvaret för att se till att informationssystemen uppfyller lagar och regler ligger i det ansvaret och hos systemförvaltaren.** **Det finns också tydliga riktlinjer till vad man inte ska använda epost till.** **I kommunen finns det inte möjlighet att automatiskt vidarebefordra epost till externa epostanvändare. Ett exempel på att försöka undvika att det oavsiktligt går iväg information.**	**Å**
Fråga	**10:** En användare har varit på besök hos en extern partner. Han har där använt kopiatorn och av misstag glömt en kopia av ett dokument i kopiatorn. Dokumentet som blev kvarglömt är av känslig typ och obehöriga kan nu ta del av denna information samt publicera den vilket kan vara oangenämt. • *Hur hanteras ett sådant scenario?* • *Vad blir kostnaden ifall ett sådant scenario inträffar, ur ett ekonomiskt och ett organisatoriskt perspektiv?*	
Svar	**Svårt att säga.** **Som jag tidigare sagt beror detta på vilken verksamhet och vilken information. Sådant inträffar tyvärr.**	**Å,K**
Fråga	**11:** Ett läckage har skett där exempelvis känslig kundinformation har läckt ut från er avdelning. Dessa hemligheter har läckts till pressen och kan skada organisationens anseende och trovärdighet. • *Finns det en färdig handlingsplan för hur man hanterar en sådan situation? Hur ser en sådan handlingsplan ut?*	

	Hur påverkar ett sådant scenario organisationen?	
Svar	**N/A**	**Å,K**

Bilaga 9 – Informant LA1

H= Hot, Å = Åtgärd, K = Konsekvens

Fråga	**1:** Anser du att informationsläckage är ett problem som du måste förhålla dig efter? Förklara ditt svar. För att få förståelse för hur informationsläckage kan ske har vi nedan några exempel: • För tidigt läckta årsredovisningar • Läckta publikationer • Läckta arbetsdokument • Läckta e-mail • Läckta mötesprotokoll • Läckt information för enskild persons kännedom om ett visst förhållande	
Svar	**Ja, det är ett problem.** **Informationssäkerhet och sekretess styr vår verksamhet så i de fallen kan problem uppstå om information läcker.**	**H**
Fråga	2: Hur ser din roll ut i handlingsplanen för hanterandet av ett informationsläckage?	
Svar	**Fel i verksamheten hanteras via linjechef.**	**Å**
Fråga	**3:** På vilket sätt ingår det i dina arbetsuppgifter att hantera och kontrollera förebyggandet av informationsläckage?	
Svar	**Att påtala risker.** **Inte lämna datorer eller utrymme med information tillgängliga för obehöriga.**	**Å**
Fråga	**4:** På vilket sätt kan du påverka arbetet med förebyggande åtgärder mot informationsläckage?	
Svar	**Via min chef.**	**Å**
Fråga	**5:** Vilket är det största hotet gällande informationsläckage mot din organisation, internt eller externt hot? Förklara.	
Svar	**Internt, tror jag. Nyfikenhet.**	**H**
Fråga	**6:** Anser du att det finns ett förebyggande arbete mot informationsläckage som påverkar dina arbetsrutiner? Förklara.	
Svar	**Inloggning i system kan vara olika och tar tid, vilket kan göra att användare inte loggar ut.**	**Å**
Fråga	**7:** Hur skulle ett informationsläckage påverka dina arbetsrutiner?	
Svar	**Kan ske i vissa fall beroende på arbetsuppgifter. Framförallt kan det skapa merarbete och sänka förtroendet.**	**K**
Fråga	**8:** Hur känner du kring att du skulle kunna orsaka ett informationsläckage genom oförsiktighet eller ovetskap?	
Svar	**Otrygghet kanske.**	**H**
Fråga	**9:** Finns det tekniska säkerhetsmekanismer installerade/konfigurerade för att förhindra oavsiktligt informationsläckage, t ex via e-mail eller annat kommunikationsmedium?	

Svar	**Vet ej.**	**Å**
Fråga	**10:** En användare skickar ett dokument via e-mail som innehåller information om personal. Detta skickas av misstag till fler personer än vad som var menat. Exempel på dokument som har skickats kan vara lönelistor. • *Hur ser en handlingsplan ut för att bemöta detta misstag?* • *Vad blir konsekvenserna av ett sådant scenario?*	
Svar	**Att påtala misstaget till den som hanterat.** **Att chefen ansvarar för att hantera situationen.**	**Å**
Fråga	**11:** Ett läckage har skett där exempelvis känslig kundinformation har läckt ut från er avdelning. Dessa hemligheter har läckts till pressen och kan skada organisationens anseende och trovärdighet. *Finns det policys för hur man hanterar informationsläckage och hur påverkar det arbetsrutinerna?* Om ja; *Hur kontrolleras det att användaren förhåller sig till policys?* Om nej: *Vad anser du om policys för informationshantering för att förhindra informationsläckage inom er organisation?*	
Svar	**Känslig information i vår verksamhet är framförallt personinformation som styrs av sekretesslagar.** **Resp verksamhet kan ha olika instruktioner för hanteringen, generellt sätt ligger ansvaret på resp verksamhetschef.**	**Å**

Bilaga 10 – Informant FC1

H= Hot, Å = Åtgärd, K = Konsekvens

Fråga	**1:** Anser du att informationsläckage är ett problem som du måste förhålla dig efter? Förklara ditt svar. För att få förståelse för hur informationsläckage kan ske har vi nedan några exempel: • För tidigt läckta årsredovisningar • Läckta publikationer • Läckta arbetsdokument • Läckta e-mail • Läckta mötesprotokoll • Läckt information för enskild persons kännedom om ett visst förhållande	
Svar	**Ja jag anser att det ibland finns ett problem med infoläckage. Det blir onödigt mycket jobb med att hantera ”rykten” och personalen blir orolig för påhittade konsekvenser av självsvängande rykten.**	**H**
Fråga	**2:** Hur ser handlingsplanen ut om information läcks utan tillåtelse utanför er organisation? Informationen är känslig, exempelvis material som innehåller information om nya prototyper, planer eller mötesprotokoll.	
Svar	**Snarast skall en rapport konstrueras med tyngdpunkt avseende menbedömningen av vad den förlorade informationen har för betydelse för oss och för en eventuell ” fi”.**	**Å**
Fråga	**3:** Har ni olika handlingsplaner/checklistor för olika typer av informationsläckage?	
Svar	**Ja beroende på hur säklassad informationen är agerar vi på olika sett.**	**Å**
Fråga	**4:** På vilket sätt arbetar ni med att förbättra säkerheten för att förebygga informationsläckage?	
Svar	**Information och självkontroll. Vi genomför även årliga kontroller som leds av andra utanför arbetsplatsen.**	**Å**
Fråga	**5:** Vilket hot gällande informationsläckage anser du är det största hotet mot din organisation, internt eller externt hot? Förklara.	
Svar	**Internt avseende ryktesspridning vilket leder till effektnedgång; se tidigare svar. Externt avseende främst industrin.**	**H,K**

Fråga	**6:** På vilket sätt kan informationsläckage påverka organisationen ur ett anseendemässigt perspektiv?	
Svar	**Det skulle skada vårt anseende mycket om det gick att bevisa att vi hade läckt säk-klassad info till någon otillbörlig person eller makt.**	**K**
Fråga	**7:** Hur skulle ett informationsläckage påverka dina arbetsrutiner?	
Svar	**Se tidigare svar samt att vi eventuellt skulle behöva skapa fler eller nya rutiner för hur ett visst arbete skall utföras.**	**K**
Fråga	**8:** På vilket sätt påverkas organisationen av det förebyggande arbetet för informationsläckage för såväl positiva som negativa effekter?	
Svar	**Skapar dagliga rutiner.**	**K**
Fråga	**9:** Finns det tekniska säkerhetsmekanismer installerade/konfigurerade för att förhindra oavsiktligt informationsläckage, t ex via e-mail eller annat kommunikationsmedium?	
Svar	**Ja på de flesta av våra system finns det ett stöd som skall hjälpa oss att inte göra fel.**	**Å**
Fråga	**10:** En användare har varit på besök hos en extern partner. Han har där använt kopiatorn och av misstag glömt en kopia av ett dokument i kopiatorn. Dokumentet som blev kvarglömt är av känslig typ och obehöriga kan nu ta del av denna information samt publicera den vilket kan vara oangenämt. • *Hur hanteras ett sådant scenario?* • *Vad blir kostnaden ifall ett sådant scenario inträffar, ur ett ekonomiskt och ett organisatoriskt perspektiv?*	
Svar	**Digniteten på dokumentet kommer att avgöra vad som händer på alla plan. Från kanske bara ett samtal om vikten av att hålla rätt på sina papper till en fullt ut anmälan om brott.** **Kostnaden är svårt att uttala sig om men jag tror att den största effekten hos oss skulle det bli med vårt anseende hos andra och ur ett fortsatt samarbetes perspektiv.**	**Å,K**
Fråga	**11:** Ett läckage har skett där exempelvis känslig kundinformation har läckt ut från er avdelning. Dessa hemligheter har läckts till pressen och kan skada organisationens anseende och trovärdighet. • *Finns det en färdig handlingsplan för hur man hanterar en sådan situation? Hur ser en sådan handlingsplan ut?*	

	• *Hur påverkar ett sådant scenario organisationen?*	
Svar	**Det finns en mängd olika planer på hur en sådan händelse skulle hanteras på min arbetsplats. Beroende på digniteten på informationen som läckt skulle olika faser av den i förväg planering att träda i kraft.**	**Å,K**

Bilaga 11 – Informant FC2

H= Hot, Å = Åtgärd, K = Konsekvens

Fråga	**1:** Anser du att informationsläckage är ett problem som du måste förhålla dig efter? Förklara ditt svar. För att få förståelse för hur informationsläckage kan ske har vi nedan några exempel: • För tidigt läckta årsredovisningar • Läckta publikationer • Läckta arbetsdokument • Läckta e-mail • Läckta mötesprotokoll • Läckt information för enskild persons kännedom om ett visst förhållande	
Svar	**Ja, men egentligen bara gällande sekretessbelagd information.**	**H**
Fråga	**2:** Hur ser handlingsplanen ut om information läcks utan tillåtelse utanför er organisation? Informationen är känslig, exempelvis material som innehåller information om nya prototyper, planer eller mötesprotokoll.	
Svar	**Menbedömning enligt gällande regelverk. I förekommande fall även polisanmälan (t.ex. USB-stickan på KB).**	**Å**
Fråga	**3:** Har ni olika handlingsplaner/checklistor för olika typer av informationsläckage?	
Svar	**Nej**	**Å**
Fråga	**4:** På vilket sätt arbetar ni med att förbättra säkerheten för att förebygga informationsläckage?	
Svar	**Utbildning i IT- och informationssäkerhet.**	**Å**
Fråga	**5:** Vilket hot gällande informationsläckage anser du är det största hotet mot din organisation, internt eller externt hot? Förklara.	
Svar	**-**	**H,K**
Fråga	**6:** På vilket sätt kan informationsläckage påverka organisationen ur ett anseendemässigt perspektiv?	
Svar	**Dåligt anseende/förtroende från allmänheten.**	**K**
Fråga	**7:** Hur skulle ett informationsläckage påverka dina arbetsrutiner?	
Svar	**Inte. Alternativt nytt regelverk, nya rutiner.**	**K**

Fråga	**8:** På vilket sätt påverkas organisationen av det förebyggande arbetet för informationsläckage för såväl positiva som negativa effekter?	
Svar	**Många moment/rutiner är omständligare än om ingen information var sekretessbelagd.**	**K**
Fråga	**9:** Finns det tekniska säkerhetsmekanismer installerade/konfigurerade för att förhindra oavsiktligt informationsläckage, t ex via e-mail eller annat kommunikationsmedium?	
Svar	**Separata IT-system för sekretessbelagd information finns. Vissa system har filter på meddelandenivå (här: meddelande = dataformat, ej löptext).**	**Å**
Fråga	**10:** En användare har varit på besök hos en extern partner. Han har där använt kopiatorn och av misstag glömt en kopia av ett dokument i kopiatorn. Dokumentet som blev kvarglömt är av känslig typ och obehöriga kan nu ta del av denna information samt publicera den vilket kan vara oangenämt. • *Hur hanteras ett sådant scenario?* • *Vad blir kostnaden ifall ett sådant scenario inträffar, ur ett ekonomiskt och ett organisatoriskt perspektiv?*	
Svar	**Partnern kontaktas och ombeds att ta hand om kopian och skydda den på ett tillbörligt sätt. Då scenariot inte torde uppstå annat än hos en partner som är SUA-upphandlad torde partnern vara pålitlig och angelägen om att bevara vårt förtroende. Kostnaden blir arbetstimmar för hanteringen av menbedömningen.**	**Å,K**
Fråga	**11:** Ett läckage har skett där exempelvis känslig kundinformation har läckt ut från er avdelning. Dessa hemligheter har läckts till pressen och kan skada organisationens anseende och trovärdighet. • *Finns det en färdig handlingsplan för hur man hanterar en sådan situation? Hur ser en sådan handlingsplan ut?* • *Hur påverkar ett sådant scenario organisationen?*	
Svar	**Se svaren på frågorna 2, 6 och 7. Jft även med ärendet med den kvarglömda USB-stickan i en dator på Kungliga Biblioteket.**	**Å,K**

Bilaga 12 – Informant FC3

H= Hot, Å = Åtgärd, K = Konsekvens

Fråga	**1:** Anser du att informationsläckage är ett problem som du måste förhålla dig efter? Förklara ditt svar. För att få förståelse för hur informationsläckage kan ske har vi nedan några exempel: • För tidigt läckta årsredovisningar • Läckta publikationer • Läckta arbetsdokument • Läckta e-mail • Läckta mötesprotokoll • Läckt information för enskild persons kännedom om ett visst förhållande	
Svar	**Ja, det finns ett begränsat, med dock existerande, problem med läckage av ännu ej delgiven eller konfidentiell information, från medarbetare i organisationen till tidigare kolleger som nu finns i andra myndigheter eller i näringslivet. I många fall är det i oförstånd eller i syfte att visa ett positivt samarbetsklimat, men resultatet kan bli att andra parter får ett informationsöverläge inför kommande samtal.**	**H**
Fråga	**2:** Hur ser handlingsplanen ut om information läcks utan tillåtelse utanför er organisation? Informationen är känslig, exempelvis material som innehåller information om nya prototyper, planer eller mötesprotokoll.	
Svar	**Jag sitter inte i en roll som chef i säkerhetsbefattning och har därför inte kunskap om myndighetens handlingsplan i sammanhanget. På avdelningsnivå är det ju informationsplikt till central säkerhetsansvarig samt chefssamtal med individ (om det är känt vem som handlat fel) som gäller.**	**Å**
Fråga	**3:** Har ni olika handlingsplaner/checklistor för olika typer av informationsläckage?	
Svar	**Se svaret för fråga 2.**	**Å**
Fråga	**4:** På vilket sätt arbetar ni med att förbättra säkerheten för att förebygga informationsläckage?	
Svar	**Information till personalen, krav på årliga säkerhetsprov (man visar att man känner till regelverket). Till del görs också tekniska åtgärder i informationssystemet (nätverket av arbetsplatsdatorer). För mobiltelefoni finns regler för hur de får användas. Inom byggnaden finns rum där mobiltelefoner ej får medföras (inlåses i skåp utanför).**	**Å**
Fråga	**5:** Vilket hot gällande informationsläckage anser du är det största hotet mot din organisation, internt eller externt hot? Förklara.	
Svar	**Internt hot störst. Myndigheten (Försvarsmakten) har väl utvecklade rutiner för skydd mot yttre hot. Idag gäller t ex att fjärrinloggning i systemen (inkl mail) inte medges. Informationsläckage genom medvetna eller omedvetna handlingar från anställda är svårare att förhindra. Många medarbetare har tillgång till information av känslig natur, volymen av upphandlingar är omfattande och teknikfaktorn hög.**	**H,K**
Fråga	**6:** På vilket sätt kan informationsläckage påverka organisationen ur ett anseendemässigt perspektiv?	
Svar	**Anklagelser mot myndigheten om jäv, slarv, fusk eller bristande lojalitet är förödande för en skattefinansierad verksamhet som redan i utgångsläget ifrågasätts av många medborgare. Det är av central betydelse att allmänheten har förtroende för att verksamheten bedrivs på ett ärligt och kontrollerat sätt.**	**K**

Fråga	**7:** Hur skulle ett informationsläckage påverka dina arbetsrutiner?	
Svar	**Det skulle kunna innebära ännu större slutenhet, att arbetsgrupper m m måste avgränsas ytterligare samt försvåra nödvändig informationsdelning, eftersom det sannolikt skulle medföra krav på större begränsningar. Sannolikt skulle det medföra merarbete utan att effekten höjs, dvs ge lägre produktivitet.**	**K**
Fråga	**8:** På vilket sätt påverkas organisationen av det förebyggande arbetet för informationsläckage för såväl positiva som negativa effekter?	
Svar	**Medvetenhet om att organisationen hanterar känslig och viktig information kan i sig vara stärkande för självkänslan och samhörighetskänslan. Men begränsningar avseende hur de tekniska stödsystemen får utnyttjas leder i många fall till irritation, negativa upplevelser vid jämförelse med bekantas mera öppna organisationer och i värsta fall medvetna kryphålslösningar i strid med regelverket, för att lösa uppgiften att bli klar med en uppgift i tid.**	**K**
Fråga	**9:** Finns det tekniska säkerhetsmekanismer installerade/konfigurerade för att förhindra oavsiktligt informationsläckage, t ex via e-mail eller annat kommunikationsmedium?	
Svar	**Till del har jag inte kunskap om detta. Annonserade kontroller av telefoni (fast och mobil) görs årligen för att analysera efterlevnad av bestämmelser. Separerade system för intranät och externt nät (Internet) gäller på arbetsplatsen. Vissa sökningar på servrar efter felaktigt lagrade dokument med sekretessklassning (som således inte får förekomma i det öppna systemet) genomförs.**	**Å**
Fråga	**10:** En användare har varit på besök hos en extern partner. Han har där använt kopiatorn och av misstag glömt en kopia av ett dokument i kopiatorn. Dokumentet som blev kvarglömt är av känslig typ och obehöriga kan nu ta del av denna information samt publicera den vilket kan vara oangenämt. • *Hur hanteras ett sådant scenario?* • *Vad blir kostnaden ifall ett sådant scenario inträffar, ur ett ekonomiskt och ett organisatoriskt perspektiv?*	
Svar	**Det anmäls till vår interna Säkerhetstjänst, som handlägger ärendet enligt sina regelverk. Kostnaden är helt avhängig karaktären på innehållet i det kvarglömda dokumentet.** **Framhållas bör dock att kopiering i vanliga kopiatorer av känsliga dokument generellt är förbjuden på vår arbetsplats, eftersom de flesta kopiatorerna idag har minne, för senarelagd utskrift. Därvid behöver man inte glömma kvar dokumentet i kopiatorn för att det skall kunna röjas. Därför har vi inom huset särskilda kopiatorer godkända för kopiering av sådant material. Detta skall alla medarbetare känna till, vilket leder tillbaka till utbildningsbehov och krav på rutiner. Att samma situation råder vid besök hos andra bör vara uppenbart för alla medarbetare.**	**Å,K**
Fråga	**11:** Ett läckage har skett där exempelvis känslig kundinformation har läckt ut från er avdelning. Dessa hemligheter har läckts till pressen och kan skada organisationens anseende och trovärdighet. • *Finns det en färdig handlingsplan för hur man hanterar en sådan situation? Hur ser en sådan handlingsplan ut?* • *Hur påverkar ett sådant scenario organisationen?*	

Svar	**Information skall ges till Säkerhetsansvarig enhet inom arbetsplatsen (finns väl definierad). Därtill informeras Informationsavdelningen och dess pressansvarige. En plan för agerande upprättas, där Juridiska staben involveras i arbetet.** **I en tid där negativ publicitet varit mera vanligt förekommande än positiv sådan, påverkar det naturligtvis medarbetarna i deras syn på organisationen som arbetsgivare. Det blir tyngre att arbeta och i värsta fall blir alla skuldbelagda för att läckaget kunnat ske.** **Om det uppdagas vem som läckt blir det naturligtvis besvärande relationssituationer gentemot vederbörande, samt eventuellt ett rättsligt efterspel som påverkar även omgivningen.**	**Å,K**

Bilaga 13 – Informant FA1

H= Hot, Å = Åtgärd, K = Konsekvens

Fråga	**1:** Anser du att informationsläckage är ett problem som du måste förhålla dig efter? Förklara ditt svar. För att få förståelse för hur informationsläckage kan ske har vi nedan några exempel: • För tidigt läckta årsredovisningar • Läckta publikationer • Läckta arbetsdokument • Läckta e-mail • Läckta mötesprotokoll • Läckt information för enskild persons kännedom om ett visst förhållande	
Svar	**Ja. Som användare måste jag vara medveten om vilken informationsklass materialet jag hanterar är placerat inom. Om det är öppet kan jag hantera det med normala rutiner, dvs öppen e-post, telefon eller liknande. Är materialet hemligt hanteras det med särskilda rutiner för detta.**	**H**
Fråga	2: Hur ser din roll ut i handlingsplanen för hanterandet av ett informationsläckage?	
Svar	**Jag informerar min chef om vad jag observerar.**	**Å**
Fråga	**3:** På vilket sätt ingår det i dina arbetsuppgifter att hantera och kontrollera förebyggandet av informationsläckage?	
Svar	**Jag skall känna till vilken säkerhetsklassning materialet jag hanterar har och handla därefter. Jag skall även förebygga att mina medarbetare inte hanterar klassat material på ett felaktigt sätt.**	**Å**
Fråga	**4:** På vilket sätt kan du påverka arbetet med förebyggande åtgärder mot informationsläckage?	
Svar	**Jag försöker upplysa mina medarbetare om när det finns risk att klassad information kan röjas.**	**Å**
Fråga	**5:** Vilket är det största hotet gällande informationsläckage mot din organisation, internt eller externt hot? Förklara.	
Svar	**Internt. Personalen måste hantera allehanda information i olika säkerhetsklasser på ett korrekt sätt. Det finns uppenbara risker att hanteringen kan ske bristfälligt med konsekvensen att felaktig information läcker ur organisationen.**	**H**

Fråga	**6:** Anser du att det finns ett förebyggande arbete mot informationsläckage som påverkar dina arbetsrutiner? Förklara.	
Svar	**Ja, det tas upp i utbildningar och tas upp på olika genomgångar.**	**Å**
Fråga	**7:** Hur skulle ett informationsläckage påverka dina arbetsrutiner?	
Svar	**Det innebär oftast ett tillfälligt merarbete för att korrigera det som inträffat.**	**K**
Fråga	**8:** Hur känner du kring att du skulle kunna orsaka ett informationsläckage genom oförsiktighet eller ovetskap?	
Svar	**Det är inget jag önskar orsaka men något man måste kunna leva med i den typen av arbete jag har.**	**H**
Fråga	**9:** Finns det tekniska säkerhetsmekanismer installerade/konfigurerade för att förhindra oavsiktligt informationsläckage, t ex via e-mail eller annat kommunikationsmedium?	
Svar	**Ja.**	**Å**
Fråga	**10:** En användare skickar ett dokument via e-mail som innehåller information om personal. Detta skickas av misstag till fler personer än vad som var menat. Exempel på dokument som har skickats kan vara lönelistor. • *Hur ser en handlingsplan ut för att bemöta detta misstag?* • *Vad blir konsekvenserna av ett sådant scenario?*	
Svar	**Jag meddelar min chef vad som inträffat.**	**Å**
Fråga	**11:** Ett läckage har skett där exempelvis känslig kundinformation har läckt ut från er avdelning. Dessa hemligheter har läckts till pressen och kan skada organisationens anseende och trovärdighet. *Finns det policys för hur man hanterar informationsläckage och hur påverkar det arbetsrutinerna?* Om ja; *Hur kontrolleras det att användaren förhåller sig till policys?* Om nej: *Vad anser du om policys för informationshantering för att förhindra informationsläckage inom er organisation?*	

Svar	**Samma svar som på fråga 10. Jag meddelar min chef vad som inträffat.**	**Å**

Referenser

Abbadi, I.M., Alawneh, M., (2008), *Preventing Insider Information Leakage for Enterprises*, 2008 Second International Conference on Emerging Security Information, Systems and Technologies. IEEE

Andersson, B., (2001), *Som man frågar får man svar*, Tema nova

Backman, J., (1998), *Rapporter och uppsatser*, Studentlitteratur Lund

Baker, W., Hutton, A.C., Hylender, D., Pamula, J., Porter, C., Spitler, M., (2011) *2011 Data Breach Investigations Report*, Verizon

Bishop, S., Okhravi, H., Rahimi, S., Lee, Y.-C., (2010), *Covert channel resistant information leakage protection using a multi-agent architecture*, IET Information Security IEEE

Byers, S., (2004): *Information leakage caused by hidden data in published documents,* Security & Privacy Magazine. IEEE

Cayre, F., Fontaine, C., Furon, T., (2005) *Watermarking Security: Theory and Practice*, IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL. 53, NO. 10, OCTOBER 2005

Dawson, S., De Capitani di Vimercati, S., Lincoln, P., Samarati, P., (2002) *Maximizing Sharing of Protected Information*, Journal of Computer and System Sciences; May 2002, Vol. 64

Dye, R.A., Sri S. Sridhar, S.S., (2003*)Investment Implications of Information Acquisition and Leakage*, Management Science; Vol. 49

Einwechter, N. (2002) *Preventing and detecting insider attacks using IDS*.
Tillgänglig: http://online.securityfocus.com/infocus/1558
Senast hämtad: 2011-04-20

Fortifikationsverket, (2011)
Tillgänglig: http://www.fortv.se/sv/Aktuellt/Aktuella-upphandlingar1/SUA/
Senast hämtad: 2011-05-20

Garsten, C., Grey, C., (1998), *Trust and post-bureaucracy*, paper presented at the 14th EGOS Colloquium, Maastricht, 9-11 July

Gellman, B., Harrell, E., (2010): *3 Julian Assange*, Time; 12/27/2010, Vol. 176 Issue 26. EBSCOhost

Hoecht, A., Trott, P., (2006) *Outsourcing, information leakage and the risk of losing technology-based competencies*, European Business Review

Inkpen, A.C., Dinar, A. (1998), *Knowledge management processes and international joint ventures*, Organization Science, Vol. 9 No. 4

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

Karhula, P., (2011): *What is the effect of WikiLeaks for Freedom of Information?*, IFLA

Lawton, G., (2008), *New Technology Prevents Data Leakage*, Computer, IEEE

Liu S., Kuhn R., (2010) *Data Loss Prevention*, IEEE Computer Society

Liu, S., Zhang, Z., Cui, Y., Wu, L., (2008): *A new information leakage defendable model*, 2008 9th International Conference on Computer-Aided Industrial Design an Conceptual Design. IEEE

Marecki, J., Srivatsa, M., Varakantham, P., (2010): *A Decision Theoretic Approach to Data Leakage Prevention,* 2010 IEEE Second International Conference on Social Computing. IEEE

Melek, A., Mackinnon, M., (2006), *2006 Global Security Survey*, Research report, Deloitte, 2006

Nationalencyklopedin, (2011): *denial of service*
Tillgänglig: http://www.ne.se/lang/whistle-blowing
Senast hämtad: 2011-04-11

Nationalencyklopedin, (2011): *nätfiske*
Tillgänglig: http://www.ne.se/lang/whistle-blowing
Senast hämtad: 2011-05-04

Nationalencyklopedin, (2011): *whistle-blowing*
Tillgänglig: http://www.ne.se/lang/whistle-blowing
Senast hämtad: 2011-04-11

Norman, P., (2004), *Knowledge acquisition, knowledge loss and satisfaction in high technology alliances*, Journal of Business Research, Vol. 57 No. 6

Oxley, J., Sampson, R., (2004), *The scope and governance of international R&D alliances*, Strategic Management Journal, Vol. 25 Nos 8/9

Pereira, M.T., (2005): *Leakage of classified information by e-mail: a case study,* Security and Privacy for Emerging Areas in Communication Networks, 2005. Workshop of the 1st International Conference. IEEE

Regeringskansliet, (2011)
Tillgänglig: http://www.sweden.gov.se/sb/d/504/a/3029
Senast hämtad: 2011-05-11

Richardson, R., Peters, S., (2007), *CSI Computer Crime and Security Survey 2007*, New York: Computer Security Institute

Schultz, E.E. (2002) *A framework for understanding and predicting insider attacks*, Computers & Security Volume 21, Issue 6

Schultz, E.E., Shumway, R. (2001), *Incident response: A strategic guide for system and network security breaches*, Indianapolis: New Riders.

SFS, (1990), Lag om skydd för företagshemligheter, (1990:409)

SFS, (1949), Tryckfrihetsförordningen, (1949:105)

Tuglular, T., Spafford, E.H., (1997), *A framework for characterization of insider computer misuse*, Unpublished paper, Purdue University, 1997.

Wang, S., Li, X., (2008): *A security model to protect sensitive information flows based on trusted computing technologies*, 2008 International Conference on Machine Learning and Cybernetics. IEEE

Westra J., Adams J., (2010), *Q&A: Wikileaks - News and Stories*, Calvin College 2010

Wikileaks, (2011)
Tillgänglig: http://www.wikileaks.fi/About.html
Senast hämtad: 2011-05-31

Yin, F., Wang, Y., Wang, L., Yu, R., (2010), *A Trustworthiness-Based Distribution Model for Data Leakage Prevention,* Springer, Berlin

Zucker, L., Darby, M., Yusheng, P., (1996), *Collaboration structures and information dilemmas in biotechnology: organizational boundaries of trust production*", Sage, London