VT 2011

Åtgärdsplaner vid informationssystemhaveri

Kandidatuppsats 15 högskolepoäng, SYSK01/INFK03 i informatik

Framlagd:	Juni, 2011.	
Författare:	David Wahlström	890205-1955
	Lars Lindvall	890909-3513
Handledare:	Hans Lundin	
Examinatorer:	Agneta Olerup	
	Markus Lahtinen	

Titel:	Åtgärdsplaner vid informationssystemhaveri
Författare:	David Wahlström Lars Lindvall
Utgivare:	Institutionen för Informatik
Handledare:	Hans Lundin
Examinatorer:	Agneta Olerup Markus Lahtinen
Publiceringsår:	2011
Uppsatstyp:	Kandidatuppsats
Språk:	Svenska
Nyckelord:	IT, ledning, åtgärdsplan, risker, katastroftyper, riskhantering, sårbarhetsbedömning, riskprioritering, säkerhetsutbildning, kontroll.

Abstrakt: IT-System får idag en allt större och betydande del i organisationer, därmed ökar även beroendet av att informationssystemen ska fungera. Utan sina informationssystem kan verksamheter helt stanna upp eller försenas kraftigt. Riskerna som kan leda till systemhaveri är många och en god beredskap samt åtgärdsplanering krävs för att effektivt hantera dem. Med en god planering kan de negativa konsekvenserna av ett systemhaveri reduceras. Syftet med uppsatsen är att klargöra hur organisationer idag nyttjar åtgärdsplaner för att säkerställa organisationens fortsatta existens i samband med ett systemhaveri, samt hur de anställda engageras i planeringen. I denna studie genomfördes en undersökning över hur tre organisationer på olika nivåer; regional, nationell samt internationell nivå, hanterar sin risk- och åtgärdsplanering. Av resultaten framgick att samtliga var medvetna om de risker som de ställs inför, men val av riskprioritering och tillvägagångssätt skilde dem åt. Resurser är en betydande faktor i utvecklandet av en åtgärdsplanering, som påverkar till vilken grad risken kan hanteras. Vidare prioriterar organisationerna hanteringen av riskerna olika, detta till följd av faktorer såsom organisationstyp samt var i världen organisation är förlagd.

Innehåll

Figurförteckning

Tabellförteckning

1 Inledning

1.1 Bakgrund

Användning av informationssystem (IS) blir idag allt vanligare och återfinns inom nästan alla organisationer. I takt med att kunskapsnivån kring IT-system ökar, ökar även de krav som organisationer ställer på informationssystemen. Informationssystemen blir därför allt mer integrerade i organisationers verksamhet och får därmed en allt viktigare roll i organisationen. Detta eftersom ett datoriserat informationssystem har många positiva egenskaper som kan underlätta en organisations arbete. (Woodhouse, 2008)

Den ständiga utvecklingen och förbättringen av mjukvara bidrar till nödvändig förändring och uppdatering av system i organisationen. Denna utveckling bidrar också ofta till en ökad systemkomplexitet, vilket i sig leder till höga krav på underhåll samt höga utvecklingskostnader. (Breivold et al., 2008)

Ett datoriserat informationssystem kan, som ovan nämnts, på många sätt effektivisera en organisations arbete. Ofta läggs fokus i IS-sammanhang på just de positiva effekter som följer användningen av ett informationssystem, samtidigt bör det beroende som uppstår också beaktas. I IS-sammanhang finns alltid risken för haveri och ett problem som kan uppkomma då relaterar ofta till det beroende som kan ha uppstått i organisationen (Woodhouse, 2008). För att hantera oväntade händelser såsom en katastrof som orsakat ett systemhaveri hos organisationen, krävs det någon form av åtgärdsplan eller strategi för att arbetet effektivt ska kunna fortsätta till haveriet är löst (Snedaker, 2007). Det är även intressant att veta om de anställda på organisationen vet vad de ska göra eller vem som ska ta besluten för det fortsatta arbetet. Ytterligare en aspekt är hur länge organisationen kan klara sig utan sitt IT-system, ett tillfälligt problem som är löst på en timme gentemot ett problem som varar i flera dagar. Genom att prioritera sin riskhantering med en välutarbetad plan kan en organisation minska risken för en stor förlust och på så vis förhindra en potentiell konkurs under ett haveri. (Snedaker, 2007)

Jordbävningen och tsunamin som inträffade i Japan tidigare i år är ett tydligt exempel på en katastrofsituation för ett företag där mycket förstördes och IS havererade som följd av jordbävningen eller av tsunamin. I Japan finns flera stora IT-företag som direkt är drabbade av katastrofen, detta är något som vidare påverkar hela branschen. Flera företag har fått stänga ner sin produktion eller försöker hålla verksamheten uppe trots stora problem. Ett av de större

problemen som företag i japan ställdes inför var problem med elförsörjning. (Åsblom, 2011) Det skapar därför problem att fullständigt förlita sig på sitt IS då dessa företag vill kunna fortsätta med sin verksamhet. Fram tills problemen är lösta krävs därför en tidigare utarbetad åtgärdsplan för hur dessa situationer ska hanteras.

Cummings et al. (2005) beskriver detta problem i en studie. Studien visar resultatet att av de företag som till följd av ett systemhaveri ställts inför en stor dataförlust utan en stabil åtgärdsplan återupptog 43 % aldrig sin verksamhet, 51 % tvingades stänga inom två år, endast 6 % av företagen klarade sig undan konkurs. Trots stor sannolikhet att en organisation går i konkurs efter ett systemhaveri orsakat av en katastrof saknar nästan 90 % av mindre företag en åtgärdsplan.

1.2 Problem

Om en organisation har ett stort beroende av sina informationssystem och därför är beroende av dess funktioner samt data för att hantera sitt vardagliga arbete, skulle stora problem kunna uppstå om IT-systemet plötsligt inte skulle fungera. Det finns alltid risk för systemhaveri, och det bör ingen bortse ifrån. Intressant är då hur en organisation planerar för just en sådan situation.

För att tydliggöra det stora behovet av en åtgärdsplan kan exempelvis ett sjukhus arbete sättas i relation till ett systemhaveri. Det kan gälla vilken organisation som helst men på ett sjukhus kan övervakningssystemet handla om liv och död och är därför ett bättre exempel ur en säkerhetsaspekt. På ett sjukhus används IT-system för övervakning av patienter, om då ett av dessa övervakningssystem skulle haverera och därför inte längre fungerade skulle detta medföra stora konsekvenser och problem för organisationen. Organisationer kan inte blunda för situationer som inte ska kunna hända eller som har låg sannolikhet att inträffa, däremot bör de vara beredda att hantera ett sådant riskscenario. Om de tidigare därför skulle ha utvecklat en tydlig åtgärdsplan för hur dessa situationer ska hanteras skulle arbetet på sjukhuset kunna hanteras på ett effektivt sätt fram tills dess att systemet skulle fungera igen. Däremot om organisationen skulle vara helt utan plan skulle under samma scenario kulle organisationens arbete därför fördröjas eller helt stanna upp. (Rittinghouse et al., 2006)

En vidare aspekt kring området är huruvida de anställda på organisationen känner till att det existerar en åtgärdsplan för hur arbetet ska skötas och hur det är tänkt att de ska agera under sådana specifika förhållanden. Om organisationens anställda inte skulle ha vetenskap om åtgärdsplanens existens eller hur det är menat att agera i en sådan situation, fyller planen heller ingen roll. Därför måste de anställdas på något sätt hållas informerade om att en plan finns så att de kan agera utefter denna om det skulle behövas, därmed även uppdateras så att de minns vad som ingår i den eller känner till förändringar om planen har reviderats. (Snedaker, 2007)

Problemet som vi ser är hur en organisation kan planera för att arbetet ska kunna fortsätta trots ett haveri, med minsta möjliga förlust. Vilket leder oss till vår forskningsfråga:

Hur använder sig organisationer idag av åtgärdsplaner vid informationssystemhaveri och hur engageras anställda i planeringen?

1.3 Syfte

Vi vill med den här uppsatsen klargöra hur olika organisationer idag nyttjar åtgärdsplaner för att säkerställa organisationens fortsatta existens i samband med ett systemhaveri, samt hur organisationens anställda är delaktiga och informerade om planeringen inför sådana situationer.

1.4 Avgränsningar

Vi har i vårt arbete valt att fokusera på systemhaveri som varar i mer än en dag, studien kommer inte gå in på korta eller tillfälliga haverier i form av exempelvis ett kort elavbrott. Åtgärdsplaner för att hantera dessa riskscenariers utformning skiljer sig beroende på risken som ska hanteras, vi kommer därför inte att fokusera på samtliga potentiella katastrofer utan endast specifikt utvalda scenarier. Vidare har vi valt att i studien undersöka ämnet ur ett organisatoriskt perspektiv, vi avser därför inte att undersöka ämnet ur en teknisk aspekt.

2 Litteraturgenomgång

I följande kapitel kommer vi att presentera de teorier som vi anser är relevanta för uppsatsen och som ska hjälpa oss att besvara forskningsfrågan. Denna presentation kommer att bistå oss genom att ge insikt i problemområdet och senare vara en bidragandefaktor till att syftet med uppsatsen uppnås. Det finns ett otal artiklar samt studier som behandlar hur organisationer bör strukturera sin verksamhet samt dess system, för att täcka säkerhetsrisker. Forskningen behandlar däremot mer sällan hur chefer och anställda bör arbeta för att motverka dessa risker. Även hur de reaktivt bör agera då någon komplikation skulle uppstå i verksamheten.

2.1 Katastroftyper att överväga

Det finns många olika typer av katastrofer som kan orsaka ett systemhaveri. I systemsammanhang brukar katastrofer delas in i tre generella kategorier: mänskligt orsakade katastrofer, naturkatastrofer samt oavsiktliga eller tekniska katastrofer. De mänskligt orsakade katastroferna, avsiktliga såväl som oavsiktliga, inbegriper bland annat terrorism och internetattacker. Naturkatastrofer innefattar väderproblem i både varma och kalla klimat, samt geologiska katastrofer såsom jordbävningar och tsunamis. Till de oavsiktliga eller tekniska katastroferna räknas bland annat fel i infrastuktur och transportolyckor. (Snedaker, 2007)

Vad som bör tilläggas är att alla katastrofer inte berör samtliga organisationer, utan skiljer sig från organisation till organisation. När en organisation menar att utarbeta en åtgärdsplan bör ett flertal faktorer så som placering i världen och organisationstyp beaktas. (Snedaker, 2007)

2.2 Planeringskostnad kontra haverikostnad

Snedaker (2007) påvisar att en åtgärdsplan kan kosta mycket att utveckla. Det krävs mycket tid, resurser och det kan påverka de ekonomiska resurserna i organisationen. Det krävs sedan att planen underhålls och uppdateras för att den ska fungera om det händer något, det i sig är också en kostnadsfråga för organisationen. Trots att det uppkommer en stor kostnad, bör denna sättas i relation till den kostnad som kan uppstå vid ett haveri. Konsekvenserna av ett systemhaveri kan bli omfattande och just därför är det viktigt att dessa kostnader analyseras. Vidare kommer en sådan situation att påverka bland annat organisationens finansiella tillgångar, investerarnas inställning samt verksamhetens position på marknaden. Ett långvarigt haveri kan vidare göra hela organisationens existens osäker. Med en åtgärdsplan kan

haverikostnaden reduceras, därmed kan kostnaden för en åtgärdsplan vara värd priset för att säkra organisationens existens. Detta stämmer överens med vad Rittinghouse et al. (2006) beskriver. Författarna tydliggör detta argument genom att påvisa att planeringen är värd kostnaden bara genom att förvissa sig om organisationens säkerhet inom såväl data som fortsatta arbete.

2.3 Riskhantering

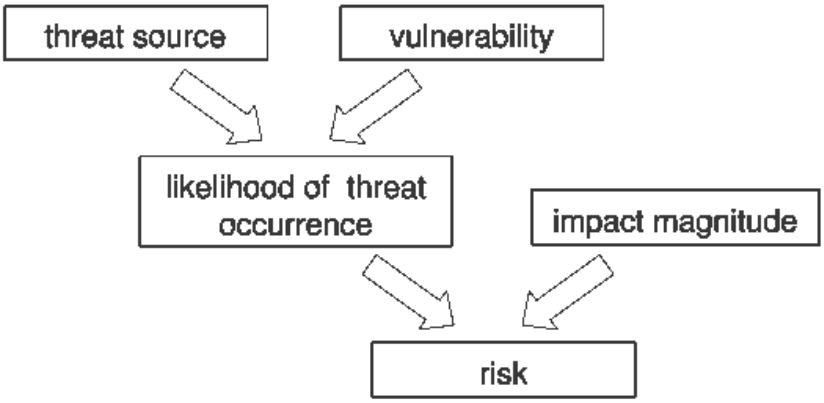
Riskhantering är tillvägagångssättet då en organisation hanterar de risker som de ställs inför och som tidigare nämnts är riskerna idag många. Därmed är riskhantering ett betydande och omfattande arbete. Målet med riskhantering är just att försöka hantera ovisshet. Det inte alltid möjligt att helt eliminera en risk däremot finns möjlighet att reducera den.(Snedaker, 2007) Riskhantering inbegriper tre huvudsakliga moment: riskbedömning, riskhantering och riskvärdering (Rittinghouse et al., 2006).

Day (1998) beskriver riskhantering i relation till projektledning, och framhäver dess likheter. Riskhantering är en teknik för att planera, organisera, implementera och kontrollera, vilket på många sätt liknar projektledning. Projektledaren måste kontinuerligt planera för de risker som kan uppstå. Om inte riskerna behandlas direkt utan istället skjuts upp framtill att problem uppstår kan konsekvenserna bli omfattande.

Riskhanteringsprocessen syftar på tillvägagångssätt som organisationer använder för att hantera risker. Riskhanteringen skiljer sig något mellan olika organisationer och dess olika faser kan ha olika benämningar, men detta moment har oberoende av organisation alltid samma mål.

Två viktiga aspekter att använda sig av under en riskestimering är riskens *omfattning* och *frekvens*, varmed menas att en organisation måste bedöma omfattningen av en risk, exempelvis jordbävning, i relation till den frekvens som dessa förekommer (Snedaker, 2007).

Jøsang et al. (2007) beskriver riskbedömning med hjälp av Figur 2.1 nedan. Modellen visar hur en organisation först måste identifiera källan till hotet och sin sårbarhet, för att sedan undersöka och bedöma hur stor chans det är att ett särskilt hot ska inträffa. Denna bedömning i relation till omfattningen om det skulle inträffa i organisationen utgör den risk som verksamheten kan behöva planera för .



Figur 2.1 Riskbedömning (Jøsang et al., 2007)

Riskhanteringsprocessen är därmed en riskbedömning, som vanligtvis brukar delas upp i fyra steg: *hotbedömning*, *sårbarhetsbedömning*, *konsekvensbedömning* och *riskreducerande strategiutveckling*. Hotbedömningssteget går ut på att identifiera och bedöma alla de potentiella hot som organisationen ställs inför och vad som är källan till hotet. Ett strömavbrott är ett exempel på ett hot som alla organisationer har, hotet är då strömavbrott medan källan till hotet är det som har orsakat strömavbrottet. För att sedan göra en noggrann analys av dessa hot. Därefter kan riskbedömningen fortsätta genom att gå vidare till sårbarhetsbedömningssteget. Det här steget syftar till att undersöka organisationens sårbarhet och allmänna mottaglighet för de hot som har identifierats i tidigare steg. Viktigt är även här att sätta det i relation till hur ofta eller hur stor sannolikhet det är att det hotet inträffar. Konsekvensbedömningssteget är som namnet säger ett steg där riskens omfattning och den påverkan som ett särskilt hot har på organisationen om det skulle inträffa analyseras.

Påverkan och omfattningen varierar på flertalet faktorer såsom bland annat lokalisering och data som organisationen hanterar. Det sista steget i processen är riskreducerande strategiutveckling, som syftar till att utveckla en strategi för att hantera de hot som efter tidigare steg prioriteras. Generellt finns det fyra typer av strategier i ett sådant sammanhang; reducera, överföra, undvika eller acceptera riskerna. I strategiutveckling blir därför kostnad en stor faktor, då det ofta är dyrare att helt undvika ett hot jämfört med att reducera risken. (Snedaker, 2007)

2.4 Riskbedömning

”Risk is a function of the likelihood of a given threat-source’s exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.” (Stoneburner et al., 2002, s. 6)

Risker förknippas med ett stort antal system, allt ifrån affärsmässiga risker såsom fysiska system för leverans av varor till en kund, såväl som systemrisker i datoriserade system för att leverera information till en slutkälla. System är ofta skapade för modifiering, men misslyckas genom förstörelse, stöld eller brist på datorutrustning såsom hårdvara, mjukvara, data och/eller tjänster. Det omfattar även IT-brottslighet och katastrofscenarier. En ytterligare risktyp är projektrisk, såsom ett utvecklingsprojekts möjliga misslyckande. (Keil, 1995)

För att kunna bedöma en total risk måste den drabbade organisationen ha en god uppfattning om riskens sannolikhet samt riskens potentiella omfattning. Det finns ett stort antal risker men då vi diskuterar IT-säkerhet är en användbar uppdelning risken för en katastrof och risken för IT-brottslighet. Det mest allvarliga riskscenariot en organisation kan konfronteras med är då vital verksamhetsdata skulle bli otillgänglig genom systemhaveri och enkla transaktioner inte skulle kunna utföras. (Peach, 1991)

Verksamheter skulle även kunna konfronteras med olika typer av olyckor eller katastrofer såsom orkaner, jordbävningar, eldsvåda eller sabotage. Risken för verksamhetsmässig prestandaförlust i form av systemkrascher bör tas i beaktande till samma grad som obehörigt och/eller olaga intrång i verksamhetens system. (Hoffer & Straub, 1989)

”Dåliga användare” som utnyttjar systemets sårbarheter finns bland missnöjda användare och tidigare anställda. Att detta fortfarande sker är ett bevis på att säkerhetspersonal bör vara vaksamma. Det har rapporterats fall av manipulering av valutatransaktioner i verksamheter som Volkswagen, vilka skulle kostat företaget 260 miljoner dollar, men även dess bank i Schweiz 54 miljoner dollar. Lyckligtvis upptäcktes bedrägeriet precis i tid. (Neumann, 1994)

Då stölder, destruktivitet och spionage i IT-system är problem som bör tas allvarligt så har hoten via Internet blivit allt mer riktade och attackerna allt mer frekventa. Sedan år 1985 har säkerhetshoten ökat drastiskt, informationssystems nya krav på säkerhet samt IT-utvecklingen har dessvärre än idag inte avblåst dessa hot (Arnum, 1995; Latimer, M., 2011)

Många verksamheter ser Internet som en mycket stor fördel inom elektronisk handel, det finns dock ett fåtal verksamheter som satsar på webben utan att inse den fulla potentialen i en stark IT-säkerhet. Riskerna ökar liksom verksamhetens exponering för virus som passerar över internet utan att känna några nationsgränser. Även utomstående (varav många är crackers[1] eller hackers[2]) har historiskt perspektiv varit en relativt liten andel av IT-brottsligheten (Gips, 1995; Hoffer & Staub, 1989; King, 1995), deras fortsatta attacker och motståndskraft mot avskräckande motåtgärder gör dessa hot särskilt farliga. (Straub et al., 1992; Straub & Widom, 1984).

Dessa individer attackerar system direkt såväl som genom smygande attacker. Enligt en

[1] Crackers: Individer som utforskar samt kringgår säkerhetssystem med syfte att orsaka skada. (Sjoholm, 1997a)
[2] Hackers: Individer som utforskar samt kringgår säkerhetssystem i lärandesyfte. (Sjoholm, 1997b)

fransk studie så attackeras system under 20,000 tillfällen framgångsrikt varje år (Forcht, 1992). Så mycket som 70 % av Amerikas organisationer upplever samma typer av allvarliga attacker (Panettieri, 1995). De flesta IT chefer hävdar även att systemriskerna eskalerat under de senaste åren och att deras organisationer lidit ekonomiska förluster genom dessa datorangrepp (Panettieri, 1995).

Enligt ett flertal studier tas inte detta problem på så stort allvar i ledningen; verksamheter förblir oskyddade eller dåligt skyddade (Brown, 1993; Hoffer & Staub, 1989; Loch et al., 1992).

2.5 Bristande säkerhetsfokus

Informationssystem ignoreras alltför ofta ur ett säkerhetsperspektiv, detta ligger till grund för den dåliga säkerheten samt den stora skada som dessa hål medför hos verksamheten. Straub (1998) menar att detta problem beror på att ett stort antal IT-chefer inte tar systemrisker på tillräckligt stort allvar, något som sker även idag.

Under åren har studie efter studie påvisat faktiska och potentiella systembrister (beskrivs i delkapitel 2.1) (Hoffer & Staub 1989; Loch et al. 1992; Parker 1976, 1981, 1983) såväl som studier som innefattar den amerikanska regeringen (Colton et al. 1982a, 1982b; Kusserow, 1983; the American Bar Association (ABA 1984), the American institute of Certified Public Accountants (AICPA 1984), Ernst & Young (Burger, 1993; Panettieri 1995), såväl som the Local Government Audit Inspectorate (1981). Uppskattningar av årliga förluster varierar men ligger mestadels mellan 500 miljoner dollar – 5 miljarder dollar per år bara i USA. (Flanagan och McMenamin, 1992). Schwartz (1990) menar även att systemförluster blivit allt mer allvarliga. Idag listas IT-säkerhet i ett flertal verksamheter som en mycket viktigt fråga (Ball och Harris, 1982; Brancheau och Wetherbe, 1987; Dickson et al. 1984; Hartlog och Herbert 1986; Niederman et al. 1991), men endast under ett tillfälle har IT-säkerhet rankats bland de 10 mest prioriterade verksamhetsområdena. Ännu mer talande är ”katastrofåterställning”, såsom säkerhetskopiering och liknande, samt ”Säkerhet och kontroll” vilka inte kunde ses bland de 20 högst rankade områdena (Brancheau et al. 1996).

Dessa typer av brister har genom IT-utvecklingen till viss grad reducerats men kan än idag upptäckas då kryphål upptäcks allt eftersom IT-brottsligheten ständigt utvecklas och attacker blir allt mer sofistikerade. (Latimer, M., 2011)

2.6 Ledningens roll

Verksamheters informationssystem är idag otillräckligt skyddade mot ett flertal typer av skada

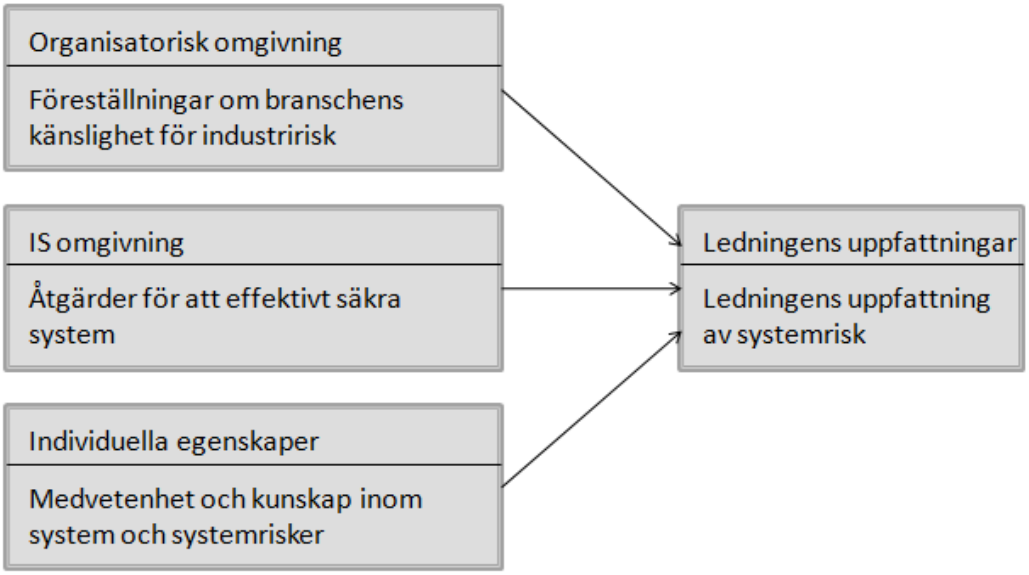
och förluster kända som systemrisker. Förluster utifrån IT-brottslighet och katastrofer är idag oroväckande stora och fortfarande mycket stora potentiella hot för verksamheter vilka kan ta flera år att återställa. Därför är det viktigt att IT-experter arbetar för att motverka och reducera risker, eftersom dessa först kan bli hanterbara och reducerade i verksamheten då verksamhetens ledande roller väl fått kännedom över hela problemet, såväl som kännedom kring alla möjliga åtgärder för att hantera problemet i fråga. Därför är det viktigt att arbeta med säkerhet genom teoribaserat säkerhetsprogram som innehåller en säkerhetsrisksplaneringsmodell, utbilda personal i säkerhetsmedvetande, samt tillhandahålla ett motåtgärdsprogram. (Straub, 1998)

Det finns idag väletablerade teorier och modeller kring hur en organisations ledning bör arbeta för att reducera systemrisker. Ett alternativ är avskräckning (Straub, 1990), detta kommer att beskrivas närmare i delkapitel 2.7, som tillhandahåller vedertagna principer för att hantera direkta och indirekta lägre systemrisker.

2.6.1 Riskmedvetenhet

Allt för ofta ertappas organisationer med säkerhetsbrister på ofta redan tidigt kända brister. Det är därför mycket viktigt att IT-ansvariga utvecklar en riskövervägande tankegång, där underskattning av risker inte får förekomma. Goodhue och Straub, (1991) menar att ett antal studier behandlar dessa frågor konceptuellt genom ett teoretiskt samt ett empiriskt perspektiv. (Goodhue & Straub, 1991)

Nedan presenteras en av dessa teoretiska studier, denna studie hävdar att ledningens oro för verksamhetens säkerhet grundas i följande: (1) Inneboende risk i branschen, (2) omfattningen av det arbete som redan vidtagits för att kontrollera dessa risker, och (3) individuellt fokus såsom medvetenhet om tidigare IT-brott, systemens bakgrund och liknande illustrerat i Figur 2.2 . (Dixon et al., 1992)



Figur 2.2 Faktorer som påverkar den IT ansvariges arbete (modell baserad på (Dixon et al., 1992)).

Enligt Figur 2.2, är det uppenbart att chefers uppfattning av de tre elementen i modellen ovan spelar en stor roll vilka även påverkar anställdas allmänna uppfattning om risker. En IT-chef bör ha ett fast grepp om de nivåerna av systemrisk organisationen är utsatt för, vilka även återspeglas i *Organisatorisk omgivning* specificerad i modellen.

De andra elementen i modellen är *IS omgivning* och *Individuella egenskaper,* vilka erbjuder IT-ansvariga goda möjligheter till lärande och förbättring. IT-ansvariga måste ha goda kunskaper i den lokala förekomsten av IT-brottslighet såväl som organisationens känslighet för skador, detta visas i *Individuella egenskaper* specificerad i modellen.

Skulle ett verksamhetssystem anfallas ett antal gånger under en månad och under en av attackerna penetreras med skadlig kod, skulle detta medföra bland annat prestandaförluster. Det spelar därför en mycket stor roll att organisationens IT ansvarig har god kännedom kring problemområdet, samt hur detta ska hanteras, t.ex. genom säkerhetskopior, systemåterställning och liknande. Detta kommer att diskuteras vidare i stycke 2.7, eftersom effektiva åtgärder för att hantera systemrisker är avgörande för en god riskanalys.

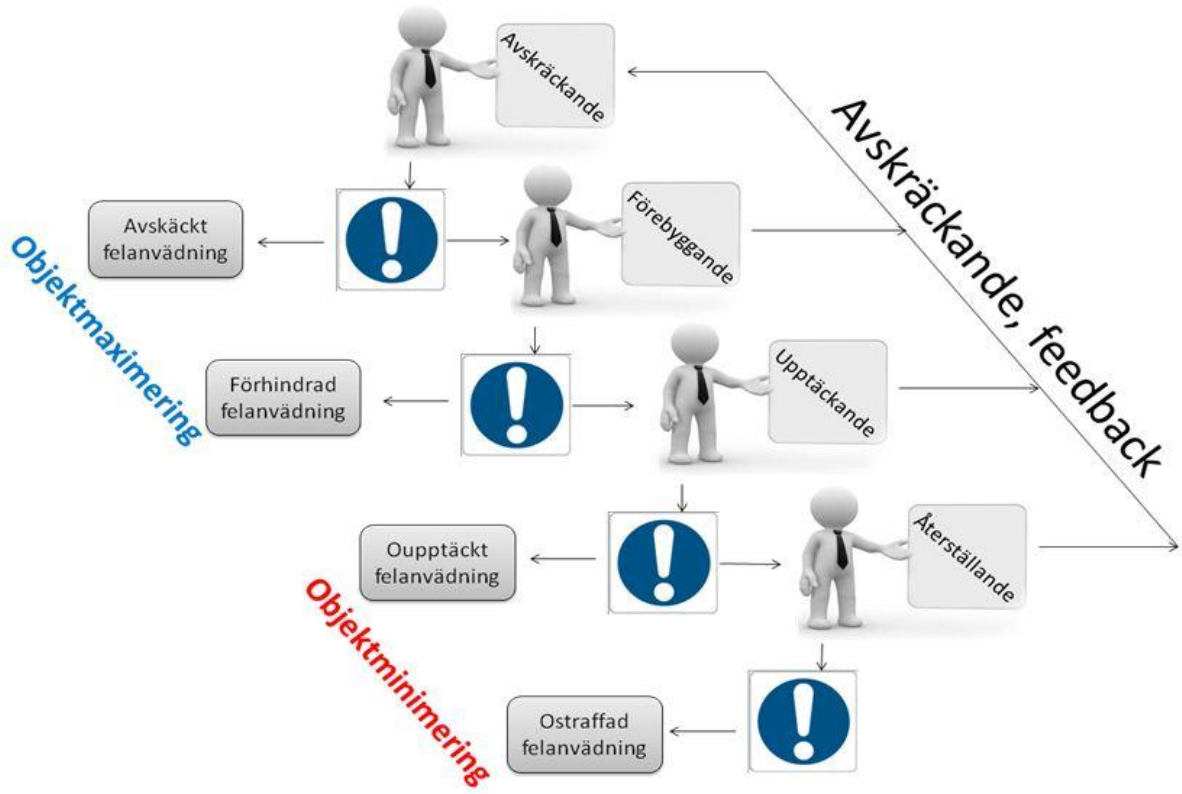
Det andra elementet i ovanstående modell; *IS omgivning,* speglar en IT-ansvarigs grundläggande förståelse för tekniska och administrativa kontroller för hantering av risker. Detta element återspeglar även åtgärder som kan vidtas genom grundläggande säkerhetsprinciper. Skulle organisationens kundbas kopplas på elektronisk väg till verksamheten, krävs exempelvis en färdig säkerhetslösning i form av säker uppkoppling och liknande. Denna uppkoppling skulle kunna säkras genom mjukvarulösningar, till exempel lösenord. (Dixon et al., 1992)

Dessutom är dessa element områden där kunskapsbehovet är som viktigast för att åtgärda riskfaktorer. Kunskaperna inom *risker* har visat sig vara fragmentariska och ofullständiga i ett otal studier (Loch et al., 1992; Straub, 1986a; 1986b). Organisationens individuella kunskap bör därför tidig tas i fokus då denne kan leda till handlingar för reducering av risk, handlingar såsom effektiv planering och gott genomförande. Då kunskapen ökar kommer även allt fler risker upptäckas och därefter behandlas med största prioritet i ett tidigt skede. Vilka områden för förändring senare kommer skapa förutsättningar för ett framgångsrikt system.

2.7 Effektiva åtgärder för att hantera systemrisker

Det finns ett flertal åtgärdsstrategier (Forcht, 1994; Martin, 1973; Parker, 1981) vid hantering av systemrisker, dessa åtgärder faller under fyra identifierade områden: (1) *avskräckande,* (2) *förebyggande,* (3) *upptäckande,* och (4) *återställning.* Begreppen är ofta åtkommande i litteraturen, dessa säkerhetsmässiga försvarsprinciper är även beskrivna i Figur 2.3. Blumstein (1978) samt Pearson och Weiner (1985) menar att den effektivaste åtgärden är avskräckningsteorin vilken idag är väletablerad inom området för kriminologi. Med

avskräckning menar litteraturen att brott förhindras genom starka straff såsom höga bötessummer och liknande. Polisen arbetar enligt avskräckningsteorin genom att göra polisinsatser synliga för allmänheten. På liknande vis kan organisationer sänka IT-brottsligheten genom att övertyga potentiella brottslingar att säkerheten är hög, risken att bli upptäckt är mycket hög samt att höga straff väntar de som trots detta försöker.



Figur 2.3 Säkerhetsåtgärdscykeln

Försvarsbarriärerna beskrivna i Figur 2.3 beskrivs som framgångsrikt implementerade i IS omgivning (Hoffer & Straub, 1989; Straub, 1990; Straub & Nance, 1990; Straub et al., 1992; 1993). Enligt denna modell avskräcks potentiella IT-brottslingar att begå brott och brytande av företagets policy. Avskräckandeteorin är dock helt passiv då individer inte skulle reagera på åtgärderna och är därför helt beroende på individers medgivande av policy. I huvudsak betonar säkerhetsmedvetande två centrala inslag i avskräckande teorin: Säkerhet för bestraffning, och Sanktion-/Straffgrad. (Blumstein, 1978)

Säkerhetsutbildningar av systemanvändare samt av organisationens ledning kommer på sikt ge god säkerhetsberedskap. Enligt Brodie (2008) kan sådana utbildningar även ses som avskräckande åtgärder. Dessa kurser förmedlar kunskap om risker i den miljö som systemanvändarna arbetar i, de lyfter även fram åtgärder som vidtagits av företaget. Med dessa åtgärder menas bland annat policys samt sanktioner som gjorts vid brott mot organisationens policy. Kurser tar även upp risker användare kan ha i åtanke då de använder systemet, såsom systemets sårbarheter samt brådskande områden under en potentiell attack.

Dessa typer av utbildningar är mycket viktiga då de övertygar potentiella IT-brottslingar att företaget tar dessa risker på mycket stort allvar. Detta visar även att organisationen är seriösa med sin systemsäkring och på ett kontinuerligt vis arbetar för skydd mot externa samt interna hot, som kan hota verksamhetens säkerhetspolicy. (Brodie, 2008)

Skulle potentiella IT-brottslingar välja att ignorera de avskräckande åtgärderna som gjorts, är nästa steg att förebygga attacker. Detta uträttas genom att installera lås på datorsalar och åtkomstkontroller, såsom lösenord. Genom att aktivt arbeta i förebyggande syfte med motåtgärder skapas en god upprätthållning av ordning och avvärjning av icke-legitima användare. (Gopal & Sanders, 1992; 1997)

Skulle en IT-brottsling ta sig igenom de två första försvarslinjerna i Figur 2.3, behöver verksamheten förmåga att upptäcka felanvändning. Proaktiva säkerhetsrapporter, såsom misstänksam aktivitet, systemgranskningar och virusrapportering. Reaktivt arbete innefattas av detektivarbete då ett brott dokumenterats. Det främsta mål för säkerhet är att samla bevis för missbruk och därefter identifiera förövaren/förövarna. (Stoneburner et al., 2004)

Slutligen borde ett effektivt säkerhetsprogram innefattas av ett sista steg, *återställande* vilket beskrivs i Figur 2.3. Återställande innebär reparation av den skadliga inverkan ett missbruk medfört samt gärningsmannens/ -männens bestraffning. Interna åtgärder i detta skede inkluderas av varningar, tillrättavisningar samt uppsägning. Rättsliga åtgärder omfattar böter såväl som civilmål.

Utfallet av dessa mål och rättsliga åtgärder används ofta senare som avskräckandeåtgärder för att i framtiden motverka IT-brottslighet. Andra åtgärder såsom systemåterställning och säkerhetskopiering är tekniska lösningar för återhämtning vilka inte enskilt leder till avskräckande för framtida missbruk i sig. Utan mer är ur ett bredare perspektiv då organisationens försvar snabbt byggs upp igen efter en attack och bidrar till en senare avskräckande verkan. Detta innebär att IT-brottslingar snabbt ska förstå att deras attack inte gjorde så stor inverkan på organisationen och att dessa ska förstå vad som kan vänta nästa gång. Avskräckandeloopen handlar om att förstärka avskräckande genom att göra angripare medvetna enligt ovanstående om konsekvenserna vid felaktig användning.

IT såväl som vanliga chefer är direkt involverade i identifieringen av de individer som bryter mot verksamhetens säkerhetsprinciper (Hoffer & Straub, 1989; Straub & Nance, 1990) samt att tillämpa lämpliga åtgärder för att avskräcka, förebygga, upptäcka samt reparera skador efter attack enligt Figur 2.3.

2.8 Information Security Management

Som tidigare nämnts har beroendet av IT ökat kraftigt inom organisationer idag. Woodhouse (2008) beskriver hur IT, under de senaste två senaste decennierna har blivit en allt mer

integrerad del i en organisation. Information har blivit en viktig tillgång för att förbli konkurrenskraftig på marknaden och därför hanteringen av information minst lika viktig. Systemen har därför fått en större och väsentligare roll i dagens organisationer.
För att underlätta detta arbete finns Information System Management (ISM) riktlinjer till hands. Dessa är riktlinjer som ska tillhandahålla de bästa ISM tillämpningarna för organisationer. Flera ISM riktlinjer har utvecklats, däribland COBIT (se 2.8.1) och GAISP[3]. (Siponen & Willison, 2009)

2.8.1 Control Objectives for Information and related Technology

Control Objectives for Information and related Technology (COBIT) är en samling *best practices*[4], metoden utvecklades av en organisation vid namn Information Systems Audit and Control Association (ISACA) år 1996. (Morimoto, 2009)

Morimoto (2009) påvisar att eftersom organisationer idag hanterar och kräver mycket information för att kunna bedriva verksamhet, läggs stor vikt därför på organisationens informationsteknik (IT). Det krävs att organisationen har god kontroll över den informationsteknik och de system som används. COBIT är ett ramverk för att underlätta att skapa just en sådan kontroll i organisationen. Bortsett ifrån best practices, som ovan nämnts, innehåller ramverket vidare även olika typer av mått, processer samt indikatorer menade att maximera de positiva effekterna av att använda sig av IT i en organisation. COBIT är ett ramverk som kan appliceras i flera situationer, och omfattar vidare även säkerhet till de risker som kan uppstå när en organisation använder IT (Morimoto, 2009). Detta stämmer bra överens med hur Ridley et al (2004) beskriver COBIT, men vidare tillägger de att COBIT som ramverk har sitt fokus på att säkerställa att anpassningen av IT sker på ett bra sätt i relation till organisationens mål.

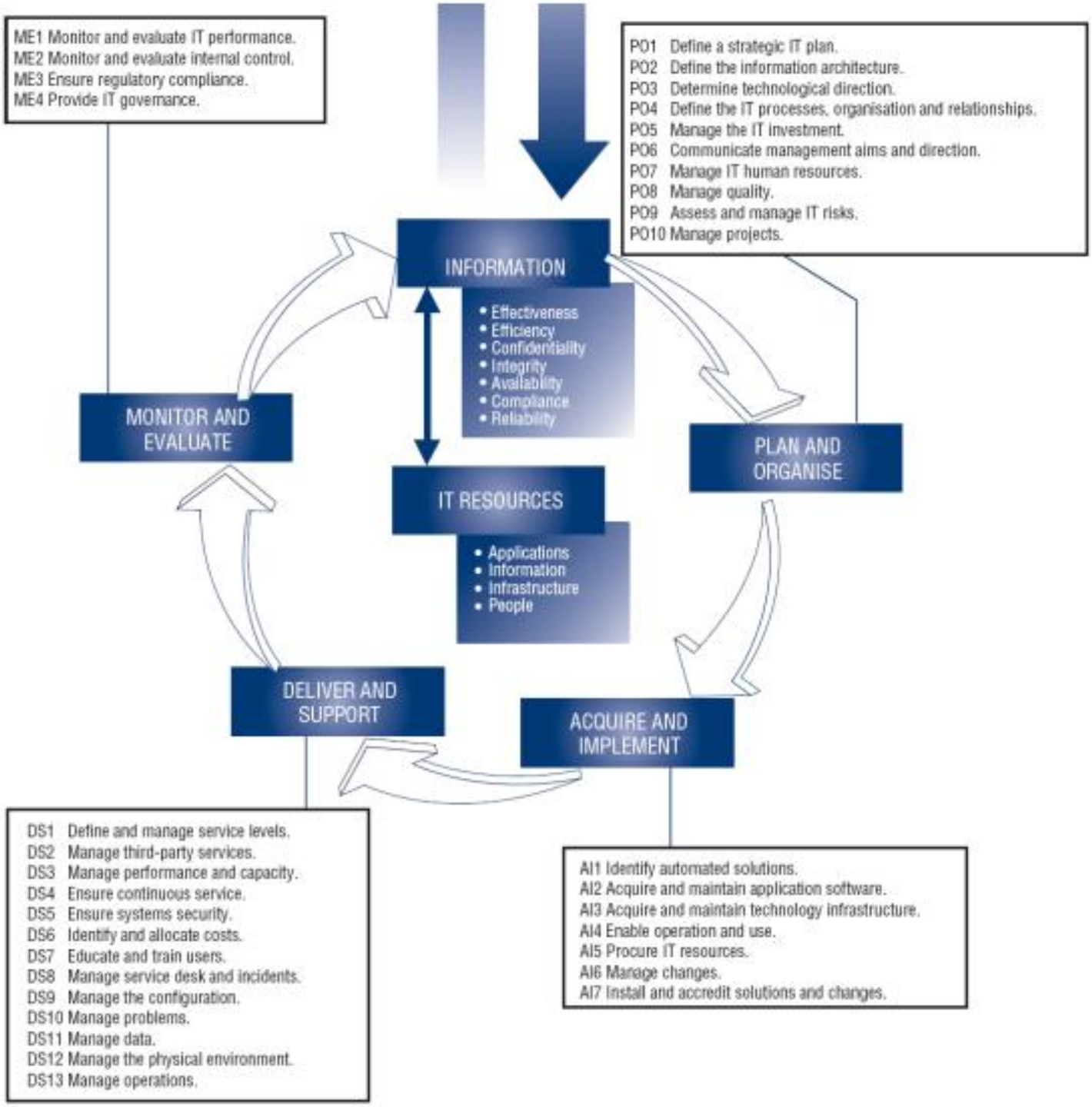
COBIT Ramverket (Figur 2.4) består av 34 kontrollmål eller processer, som vanligtvis delas in i fyra huvudgrupper (Radovanović et al., 2010):

- *Plan and Organize (PO),* som innehåller processer för att planera och designa organisationen så att de mål verksamheten har kan uppnås. Det är också i detta moment som riskbedömningen sker.
- *Aquire and implement (AI),* innehåller moment som syftar till att identifiera och ordna IT-lösningar. Vidare även att hantera dessa lösningar i framtiden.
- *Deliver and support (DS),* är det processer som gäller själva leveransen av IT-service till en organisation. Hit hör även sådant som gäller problem och andra oönskade händelser, vilket i sig även innebär säkerhetsaspekter som påverkar IT.

[3] *Generally Accepted Information Security Principles,* är principer för säkerhet av information (Siponen & Willison, 2009)
[4] *Best practices* är metoder, processer och tekniker som effektivare kan leverera ett specifikt resultat än andra metoder. Dessa metoder ska också bidra till att färre svårigheter eller oförutsedda komplikationer. (BusinessDictionary, 2011)

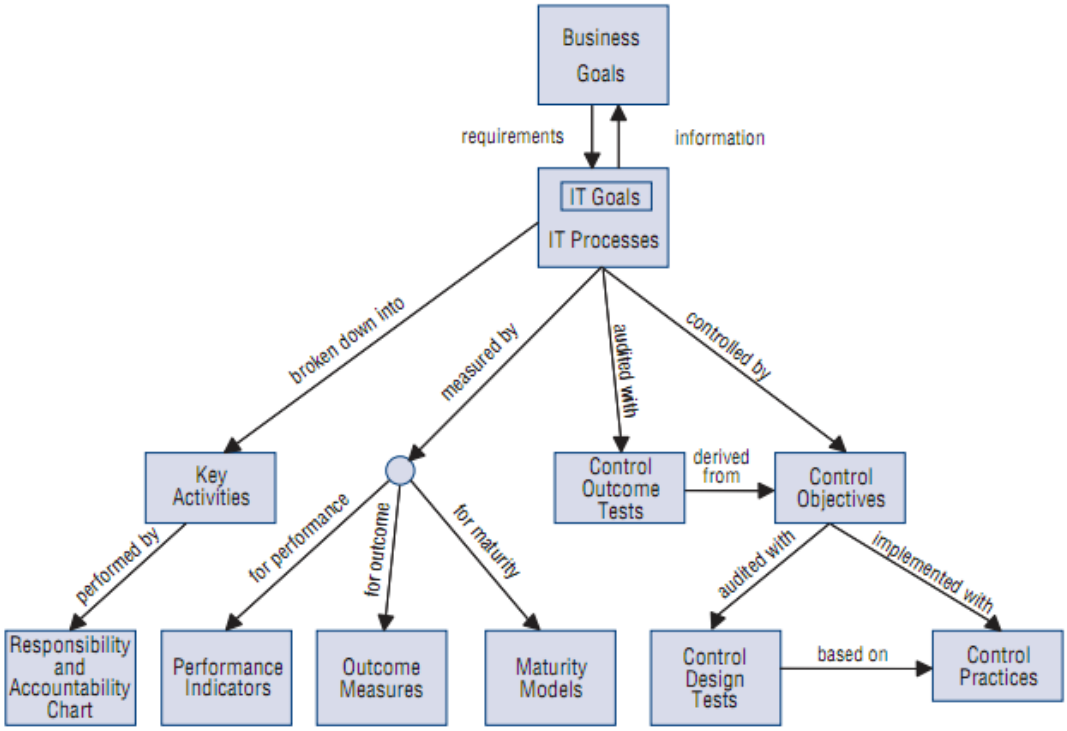
- *Monitor and Evaluate (ME),* här ingår de processer som gäller att utvärdera och övervaka det som organisationen numera använder.

Modellen(Figur 2.4) beskriver hur förloppet ska gå till när en organisation ska etablera kontroll i sin organisation. Där information kommer in eller samlas in och när tillräcklig information finns tillgänglig, övergår arbetet till planera och organisera för de nya kontrollerna. I nästa steg ingår att börja implementera dessa kontroller. Efter implementering är kontrollerna redo att börja användas, vilket är nästa steg i ramverket. Under det steget är det också viktigt att hantera alla eventuella problem som kan uppstå och stödja de kontroller som har utvecklats. Därefter övergår arbetet till övervaka och utvärdera de nya kontrollerna. Figuren visar även här informationskriterierna eller de krav som finns på den information som ska bidra till att en organisation ska uppnå sina mål. Ytterligare demonstrerar modellen kopplingen mellan information och de IT-resurser som en organisation har till sitt förfogande. (Radovanović et al., 2010)



Figur 2.4 COBIT framework (IT Governance Institute, 2011)

COBIT behandlar ett flertal olika processer i en organisation, i Figur 2.5. nedan finns en detaljerad bild av dessa samt hur de påverkar varandra (Radovanović et al., 2010).



Figur 2.5 Förhållande mellan COBIT komponenter (IT Governance Institute, 2011)

Vad modellen demonstrerar är hur organisationens mål relaterar till de IT processer som finns och därmed IT-målen. Vi kan här se hur dessa IT-mål och processer kan hanteras på ett lämpligt och effektivt sätt. Att målen kan brytas ner i nyckelaktiviteter genom att använda sig av särskilda diagram. Vidare förevisar modellen hur dessa processer kan mätas på olika sätt, hur de kan kontrolleras samt vad dessa kontroller baseras på.

2.9 Guide to the Assessment of IT Risk

Guide to the Assessment of IT Risk (GAIT) är en samling av riktlinjer som skapades år 2007 av en organisation vid namn The Institute of Internal Auditors (IIA). IIA utvecklade sedan denna guide ytterligare till GAIT for Business and IT Risk (GAIT-R), som utvidgar omfattningen av GAIT ytterligare genom att också inkluderar operativ effektivitet i förhållande till lagar och regler. GAIT-R underlättar att identifiera och bedöma alla kontrollerna som krävs för att hantera företagets mål, med hjälp av dess samling av principer och riskbaserade struktur. (The Institute of Internal Auditors, 2009)

GAIT-R är baserad på 4 principer (The Institute of Internal Auditors, 2009):

- Princip 1: Fel på tekniken behöver endast hanteras och granskas om det utsätter organisationen för risk.

- Princip 2: Nyckelkontroller bör identifieras med hjälp av en genomgående bedömning av affärsrisker och risktolerans.
- Princip 3: Företagsrisker motverkas med hjälp av ett antal nyckelkontroller, både automatiserade och manuella.
- Princip 4: Generella IT-kontroller ska fungera som en garanti för de automatiserade nyckelkontrollerna.

GAIT-R metodologin använder sig av 8 steg för att på bästa sätt ska kunna identifiera den omfattning som en situation har (The Institute of Internal Auditors, 2009):

- Steg 1: Identifiera de processer där kontroller ska tillämpas.
- Steg 2: Identifiera nyckelkontrollerna som krävs för att organisationens mål ska uppnås.
- Steg 3: Identifiera kritiska IT funktionaliteter bland organisationens kontroller.
- Steg 4: Identifiera den datormiljö där data ska skickas, lagras eller processeras, där ITGC's[5] måste testas.
- Steg 5: Identifiera ITGC processrisker samt relaterade kontrollmål.
- Steg 6: Identifiera de viktigaste ITGC's för att testa de identifierade riskerna och kontrollmålen.
- Steg 7: Utför en resonlig översyn over alla viktiga kontrollerna.
- Steg 8: Fastställ omfattning av översynen och bygg en lämplig design och effektivitetstestningsprogram

2.10 Underhåll

När är en organisation har utvecklat en åtgärdsplan som ska användas om ett haveri skulle inträffa måste denna plan kontinuerligt underhållas, detta för att planen ska fungera när den behövs. Annars finns risken att anställda glömmer bort en del kritiska delar i planen, vidare är underhåll viktigt om organisationen anställer nya medarbetare. Organisationer idag förändras ständigt, därmed krävs det att planen granskas, revideras och att anställda informeras om dess existens. Snedaker (2007) framhäver hur organisationen måste överväga hur förändringar kan påverka deras utarbetade åtgärdsplan. Hon nämner de fyra typer av förändring som måste övervägas; förändring av informationsteknologi, Förändringar i verksamheten, kooperativ förändring och till sist förändring i lagar och regler. (Snedaker, 2007)

Det är väldigt svårt att helt lyckas med en felfri plan första gången som en plan utarbetas, och det är därför först då den testas som de potentiella problem och fel som den besitter kommer till ytan. Därför är underhåll som även inbegriper testning en väsentlig del i en organisations arbete och åtgärdsplan. Revideringen av åtgärdsplanen sker genom att organisationen går

[5] *IT Generals Controls (ITGC)* är kontroller som tillämpas på alla systemkomponenter, processer m.m. Målet med ITGC är att säkerställa utveckling och implementering av applikationer. (The Institute of Internal Auditors, 2009)

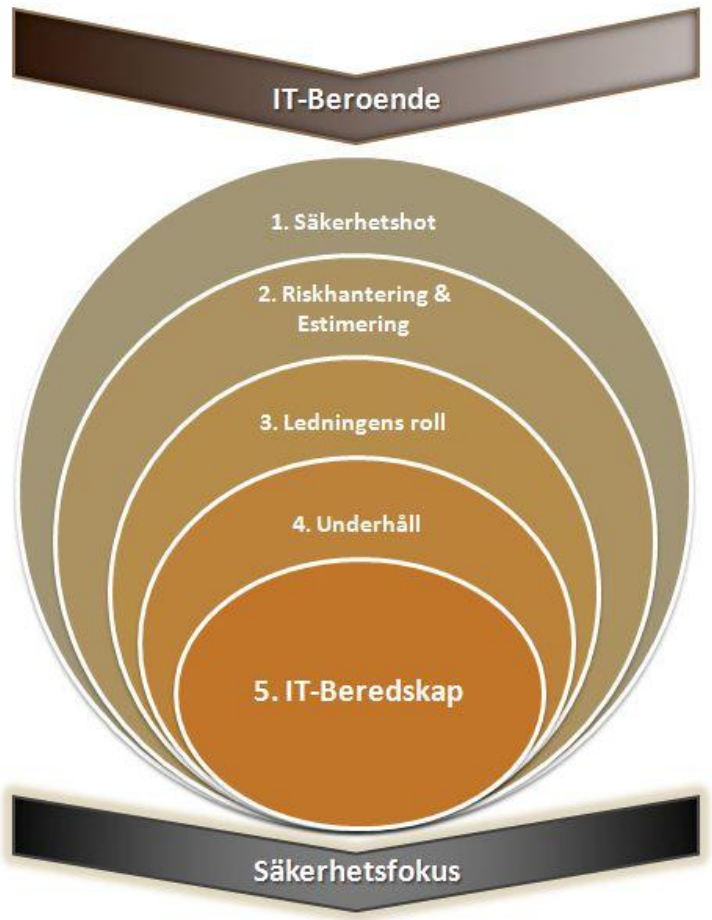
tillbaka i utvecklingsprocessen och gör om de tidigare stegen i processen, beskrivet i sektion 2.3. (Snedaker, 2007)

Rittinghouse et al. (2006) betonar att åtgärdsplanens procedurer måste uppdateras, revideras och anställda måste informeras minst en gång om året. Under denna uppdatering bör exempelvis telefonlistor aktualiseras så organisationer kan nå varandra och andra viktiga kontakter om ett haveri skulle inträffa. Därmed bör organisationen även schemalägga ett antal träningstillfällen där de anställda får öva sig i att hantera haverisituationer. Genom att testa och öva ökar förståelse samt medvetenhet hos de anställda, en åtgärdsplanen kan då få en ökad positiv effekt. Revideringen bör som sagt ske minst en gång om året då planen förlorar det mesta av sitt värde inom sex till tolv månader från det att den realiseras, detta eftersom ständig förändring i organisationen gör att den blir föråldrad och dåligt anpassad till verksamheten. (Rittinghouse et al., 2006)

2.11 Undersökningsmodell

Det ramverk vi använder oss av för att beskriva vår teoretiska ansats illustreras i Figur 2.6 från dagens ökade IT-beroende till deras tilltagande krav på säkerhet. Denna illustration beskriver de områden som berörts för att skapa en stödjande bas för vår fortsatta studie. Avsikten med att framställa en teoretisk sammanfattning genom ett ramverk är att skapa en djupare förståelse kring områden vi valt beröra för att besvara forskningsfrågan. Figur 2.6 nedan beskriver förhållandet mellan organisationers tekniska beroende och IT-säkerhetsmässiga ansvar, för att säkerställa organisationens arbete.

Figur 2.6 beskriver denna studies vitala undersökningsområden som ligger till grund för studiens genomförande. Den övre och undre pilen beskriver studiens riktning genom dess viktiga forskningsområden som studerats, men även det ökade säkerhetshotet som efterföljs av ökat tekniskt beroende. Cirklarna som överlappar varandra beskriver organisationens omgivande hot och ständiga krav på säkerhet för att nå god IT beredskap där säkerhetsorientering är ett måste.



Figur 2.6 Undersökningsmodell

1. Säkerhetshot

Allt eftersom verksamhetens tekniska beroende ökar, höjs även deras exponering för såväl interna som externa hot, därmed krävs ett högre krav på säkerhet. Detta eftersom IT-brottslingar blivit allt mer sofistikerade och riktade i sina attacker. Katastroferna att överväga och planera för kan vara många men brukar vanligtvis delas in i tre generella grupper; naturkatastrofer, mänskligt orsakade katastrofer samt oavsiktliga eller tekniska katastrofer. Dessa tre generella grupper ligger till grund för scenarier samt ett riskestimeringsavsnitt i intervjuguiden, se bilaga 1 och bilaga 2. Vilka risker som bör prioriteras högst baseras på ett otal faktorer, bland annat hotbild, organisationsstorlek och interna samt externa krav.

En viktig aspekt vid planering inför eventuella katastrofer är att sätta utvecklingskostnaderna i relation till vad ett haveri hade kunnat kosta organisationen samt vilka konsekvenser det kan få i organisationen.

2. Riskhantering och Estimering

Åtgärdsplanering hör till vad som kallas för riskhantering, som syftar till att försöka hantera ovisshet. I denna process ingår att göra en hotbedömning, sårbarhetsbedömning, konsekvensbedömning samt riskreducerande strategiutveckling, för att på så vis bedöma vilka risker som måste prioriteras. Två viktiga faktorer i bedömningen är frekvens och omfattning.

Det finns generellt fyra områden av åtgärdsstrategier: avskräckande, förebyggande, upptäckande samt återställning.

System har under de senaste åren blivit mer integrerade i organisationer och har en därmed fått en betydelsefull roll. För att hantera system på ett effektivt sätt finns metoder och riktlinjer som kan underlätta vid bland annat säkerhetsarbete, däribland COBIT och GAIT.

3. Ledningens roll

Organisationens ledning har en viktig roll i att kontinuerligt motverka och reducera de risker som organisationen utsätts för. Därför är det väsentligt att kunskap och förståelse gällande risker finns i ledningen, och att de genom interna utbildningar och lärande bland personal arbetar proaktivt för att reducera organisationens riskfaktor.

4. Underhåll

Slutligen är underhåll en väsentlig del i en åtgärdsplan. Planen bör sporadiskt revideras i takt med att verksamheten förändras. Revideringen bör göras på årsbasis för att inte bli inaktuell och dåligt anpassad till organisationens arbete. I underhållsarbetet ingår även utbildning såväl som dagliga felsökningar och proaktivt arbete i områden som teknik samt dess miljö.

5. IT Beredskap

För att nå en god beredskap måste dessa ovanstående områden tas på allvar av organisationens ledning samt personal. Personalen måste uppdateras med aktuell information och deras proaktiva säkerhetstänk bör premieras. Det är även mycket viktigt att organisationens säkerhet årligen revideras då organisationen är i ständig förändring men även dess interna samt externa hotbild.

3 Metod

I detta kapitel redogörs de tillvägagångssätt och val som gjorts under arbetet i denna uppsats. Denna metod gjordes även för att klargöra hur vi valt att lägga upp arbetet, såsom under insamlandet av empirin men även under dess analysering. Syftet med detta kapitel är att genom klarläggning för våra val av metoder, på detta vis skapa en ytterligare tydlighet samt trovärdighet i såväl utförande som dess resultat.

3.1 Tillvägagångssätt

Vi ansåg att intervjuformen borde ske genom datainsamling med hjälp av presentation av scenarier. Dessa scenarier var menade att presentera ett antal potentiellt förödande situationer organisationen skulle kunna ställas inför. Vi valde även att komplettera dessa scenarier med kompletterande frågor för att ytterligare tillvarata informantens expertis i ämnet. (Wallén, 1993)

Den empiriska undersökningen genomfördes i enlighet med intervjuguiden (bilaga 1) bortsett ifrån intervjun med Försvarsmakten som skickades in som frågeformulär(bilaga 2). Under sammanställning av empiri identifierades problemområden samt skillnader i respektive studerad organisations struktur. Organisationerna klassades av oss som: internationella, nationella, såväl som regionala. Detta låg senare till grund för vår diskussion där material analyserades med förankring till respektive organisationstyp där dessa typer jämfördes och diskuterades.

3.2 Undersökningsmetod

Jacobsen (2002) beskriver en ansats som går från empiri till teori. Vi valde att i förstudien, kartlägga basen genom att studera olika teorier kring problemområdet, vilka senare låg till grund för en undersökningsmodell som senare resulterade i intervjuguiden (bilaga 1 och bilaga 2). Denna intervjuguide låg sedan till grund för vår studie varigenom vi avsedde att fokusera på organisationers olika säkerhetsfokus och prioritering av risker samt scenariohantering.

Utöver intervjufrågorna valde vi att använda oss av ett antal riskscenarier. Den scenariobaserade delen av intervjun gav oss insikt kring individens handlande under specifika

förhållanden. Dessa presenterade scenarier var baserade på studiens bakgrundsanalys samt studiens teoretiska material. Presentation av scenarier gav oss möjlighet att kunna dra paralleller mellan informantens expertis och handlande mot våra teoretiska fakta samt gentemot de två andra organisationerna. Informantens expertis för prioritering samt risksannolikhet kunde även jämföras genom en enkätdel varigenom informanten hade möjlighet att klassificera sannolikhet samt prioritering för ett antal risker.

Vi valde även att komplettera scenariostudien med utrymme för dialog under intervjutillfället. Den kompletterande dialogen gav oss en mycket god uppfattning kring intervjupersonens omgivning och dagliga arbetsrutiner, såväl som underlag för förslag på en bästa lösning. Denna studie var senare ämnad att undersökas genom teori samt empiri vilket senare kunde tas till vara inom intervjupersonens område för säkerhet. Under studien i den nationella organisationen valde vi att komplettera med information från deras webbsida, eftersom att undersökningen gjordes genom utskickande av enkäter och därför fick vi även begränsad information såväl som i möjlighet för frågeformulering.

Uppsatsen behandlar triviala såväl som komplexa entiteter vilka i sin tur krävde informationsrika svar vilka var nödvändiga för vår undersökning på grund att vi i vår studie ville nå en klarhet kring ett ämne som annars kan uppfattas som svårgreppbart. Genom att utvinna även de svårdefinierbara nyttorna, såväl som de nyttor som inte är fördefinierade ville vi presentera komplex data som kanske inte annars hade kommit fram på ett simpelt vis. (Trost, 2005) De svårdefinierbara entiteterna innebar en högre komplexitet vilket bidrog till ett helt annorlunda sätt att närma sig problemområdet vilket annars med stor säkerhet vid ett annorlunda angreppssätt endast skulle granskas ytligt. En kvantitativ undersökning bidrar vanligtvis till att endast siffror och statistik undersöks, detta angreppssätt var inte lämpligt för vår undersökning eftersom att vi valt att behandla i stor utsträckning komplexa relationer och svårkvantifierbara förhållanden. Under intervjun och i scenariobeskrivningen arbetade vi enligt den kvalitativa undersökningsmetoden vilken ökar användbarheten av våra resultat som i sin tur skapade en starkare koppling till verkligheten. (Alvesson & Deetz, 2000)

3.3 Informationsinsamling

Information till studien samlades in empiriska studier på tre olika organisationer. Dessa studier presenteras i kapitel 4, material finns även att tillgå genom studiens bilagor (bilaga 3, 4, 5, 6).

De tre tidigare nämnda katastroftyperna (delkapitel 2.1) låg senare till grund för vår empiriska undersökning på de tre organisationerna. Denna undersökning skapades och genomfördes enligt vår bakomliggande studie beskriven ovan. Frågorna gjordes för att ge oss en helhetsbild utav organisationen samt informantens ståndpunkt och förhållande till organisationen. Vi undersökte även informantens kunskaper för IT-beredskap i organisationen genom att presentera för denne tre potentiella riskscenarier. Med koppling till forskningsfrågan valde vi

att utforma dessa ur ett mer långvarigt perspektiv. För att tydliggöra organisationernas riskprioriterings- samt risksannolikhetsskillnader utformade vi även för intervjun en mindre enkät där informantens uppfattningar om IT-beredskapshot skulle presenteras. Denna gav oss underlag för senare diskussion där karaktärisering utav organisationernas faktiska IT-beredskap kunde granskas och sammanställas.

3.3.1 Intervjuer med scenarier

Heijden (2005) menar att dessa kvalitativa expertkunskaper ytterligare kan tas till vara och prövas genom scenarier. Vid konfrontering av scenarier prövas informantens IT-beredskapsplan, estimeringar och tankar kring potentiella risker, vilka även dessa resulterar i informationsrika svar som tydligt förankrade de övriga frågorna. Dessutom prövar organisationer idag sin framförhållning inom IT-säkerhet och ekonomi genom scenarier, på detta vis menade vi att detta även skulle gynna oss då området vi vill beröra just var IT-beredskap i praktiken. Detta skulle ge oss ytterligare en aspekt på hur organisationen faktiskt hanterade olika fall av systemhaveri. Även teorier i studiens teoretiska ramverk (se Figur 2.6) kommer att användas under utarbetandet av scenarier, riskestimeringsanalys samt kompletterande frågor se bilaga 1 och bilaga 2.

Med den teoretiska studien till grund hade vi utformat scenarier samt kompletterande frågor som resulterade i ett intervjumaterial som skulle hjälpa oss under insamlandet av empiri. Undersökningen är uppdelad i de två tidigare nämnda delarna *scenarier* och *kompletterande frågor*. Tre intervjuer gjordes med representanter från en internationell, en nationell och en regional organisation som alla arbetar med IT-säkerhet. Av dessa skedde intervjun i den nationella organisationen på distans genom ett utskickat frågeformulär. En kompletterande intervju genomfördes i den regionala organisationen med en anställd som jobbar i en annan position inom organisationen. Detta medförde att vi kunde undersöka hur dessa olika verksamhetstyper hanterar IT.

Området för kompletterande frågor syftar till att ge oss en uppfattning kring hur intervjupersonen arbetar idag samt, under de personliga intervjuerna, dialog med plats för djupare muntlig intervju kring intervjupersonens arbete med möjlighet för klargörelse för specifika oklarheter. Intervjun grundade sig i en scenariodel behandlande tre scenarier vår informant skulle kunna konfronteras med, val av scenarier baserades på sannolika händelser utifrån organisationernas placering och organisationstyp. För att utforma dessa scenarier fick vi då beakta hur organisationerna arbetade och sätta ihop fiktiva scenarion som skulle kunna ha stor inverkan på organisationens vardagliga arbete.

Genom ett antal följdfrågor skulle dessa beskriva hur organisationen hanterar samt proaktivt arbetar för att tillhandahålla metoder designade för att möta dessa potentiella risker. Vi utformade intervjufrågorna som komplettering för intervjumaterialets scenarier vilka vi baserade intervjun på. Dessa frågor utformades enligt Trost (2005) och var en fas för datainsamlande av det empiriska material detta senare skulle utmynna i. Intervjufrågorna

baserades på den tidigare presenterade i undersökningsmodellen. Verksamhetsintervjuerna var utformade enligt den kvalitativa metoden som influerade intervjuformen som även denna blev kvalitativ (Trost, 2005). (Alvesson & Deetz, 2000)

Denna intervjuform är enligt Trost (2005) ett mycket gott sätt att forma intervjuer på då de resulterar i informationsrika svar, vilka var nödvändiga för vår undersökning. Det ansågs att dessa kvalitativa intervjuer var ytterst lämpliga då de skapade en närmre dialog och kommunikation med informanterna. Denna nära dialog medförde att deras expertkunskaper togs till vara, vilket hade varit svårare under andra former av datainsamling.

Intervjuerna utfördes i enlighet med delkapitel 3.2, undersökningsmetod. Materialet presenterades för informanten i form av tidigt underlag denne kunde ha för att känna sig säker på kommande frågor under intervjun. För att vi skulle få en bild av informantens bakgrund och ställning i organisationen, men även för att denne skulle känna sig bekväm i intervjun presenterades först mer mjukare frågor som informanten lättare kunde besvara. Då dessa steg var avklarade blev den presenterad ett antal scenarier som gav prov på informantens kännedom för IT-beredskap och hantering. För att tydliggöra denna skillnad i riskhantering bland de tre organisationstyperna blev respektive informant även presenterad en riskestimeringsmatris där denne fick möjlighet att själv klassificera potentiella hot samt hotens sannolikhet.

3.4 Analys och kategorisering

Under arbetet med analys av intervjuer valde vi att strukturera vårt material genom kategorisering. Denna kategorisering lät oss arbeta med ett kreativt tänk där vi framarbetade intressanta avdelningar för empiri där vi tillsammans ledde analysarbetet framåt. (Bryman, 2002)

Kreativiteten sågs som viktigast under fasen för sammanställning där vi iterativt analyserade det empiriska framtagna material och jämförde detta med vartannat. Denna process var menad för att hitta mönster i det empiriska materialet som vi sedan speglade mot litteraturen. Vilket medförde att vår gemensamt analyserade insamlad data kritiskt blev granskad och tillvaratagen högsta möjliga grad. (Trost, 2005)

Trost (2005) menar att det finns ett flertal uppfattningar kring analysprocessens utförande, endel hävdar att denne ska ske simultant med intervjun medan andra hävdar att det är bäst att analysera detta när materialet väl samlats in. I vårt fall utfördes merparten av analysen i efterhand då vi under intervjun främst valde att fokusera på att hålla en god dialog med informanten. Under intervjun sammanställdes dialogen genom inspelning samt notering, viket gjorde att intervjun gick relativt snabbt och tillfälle för djupare reflektioner ägde därför rum under transkribering samt analys av materialet.

Vi utarbetade vår kvalitativa dataanalys enligt Brymans(2002) modell, genom att urskilja det insamlande materialet genom kodning. Innehållskodningen innebar att genom markerande urskilja de intressanta data, detta gjordes genom kategorisering baserad på undersökningsmodellen. Kategoriseringen baserades på olika teman, såsom ” Hur de lägger upp åtgärdsplaner”, ”Hur anställda involveras i säkerhetsarbetet” samt ”Riskprioriteringar”. Kodningen gjordes genom diskussion och granskande av utskrivna exemplar av våra transkriberingar, och resultatet av denna kodning finns i Bilaga 7. De data vi fått fram genom scenarier och kompletterande frågor diskuterades senare i diskussionen och jämfördes med det tidigare insamlade teoretiska materialet. Urskiljandet gjordes främst genom nivåstrukturering av intervjuguiden där vi strukturerade frågorna karaktäriserade dessa till tre områden för senare validitetsprövning. Urskiljandet bland scenarierna ägde rum på ett mer visuellt plan där materialet diskuterades och jämfördes med vartannat vilket senare jämfördes med intervjumaterialets övriga frågor. Detta fungerade inte bara för att analysera verksamhetens faktiska försvar utan även för att analysera informanternas faktiska orientering till IT-säkerhet samt deras faktiska IT-beredskap vid krissituationer.

3.5 Urval och informanter

Jacobsen (2002) resonerar kring urval av intervjupersoner, han menar att dessa kan väljas ut baserat på deras erfarenhet och kunskap inom det område undersökningen berör. Vi valde att först fokusera på verksamhetstyp för att utifrån dess verksamhetsområde samt organisationsstruktur på; internationell, nationell, samt regional nivå, kontakta informanter med eftersökta kunskaper och erfarenheter. Detta gjorde att organisationsstrukturerna såväl som intervjupersonernas tillvägagångssätt i dess arbete varierande mellan organisationerna såväl som mellan intervjupersonerna. Under inledningsfrågorna i intervjuguiden (bilaga 1) kunde vi utröna informantens position och tankar kring dennes organisation, vilka sedan låg till grund för en validitetsprövning. Denna validitetsprövnings var en prövning för senare beslutsfattande angående en eventuell kompletterande intervju, då materialet ej ansågs reliabelt.

Vi utförde expertintervjuer i de tre olika verksamheterna. På det internationella företaget valde informanten total anonymisering och nämns endast som ”logistikchefen”, bilaga 4, resultatet kan även granskas på delkapitel 4.1. När vi sedan skulle intervjua den nationella organisationen, Försvarsmakten, skickade vi ut ett speciellt frågeformulär (bilaga 2) via vår kontakt vid organisationen. Kontakten säkrade vårt informationsinsamlande och såg till att vi fick fram relevant fakta från relevanta informanter i ämnet, studiens resultat kan granskas i delkapitel 4.3. När vi slutligen gjorde de kvalitativa expertintervjuerna på regional nivå valde vi att intervjua Hans-Åke Olsson, IT Supportschef, Svedala Kommun. Denna intervju ansågs som något osäker ur ett validitetsperspektiv (bilaga 5) och kompletterades därför genom intervju av en anonym person vid Svedala Kommun (bilaga 6). Detta gjorde att materialet blev insamlat på både ansvarigs, såväl som på användarnivå.

3.6 Validitet och reliabilitet

För att skapa en god uppsats med korrekt data valde vi att utforma arbetets mätverktyg utifrån samt enligt erkänd forskning. Genom att använda vetenskaplig fakta till grund för studien vill vi uppnå en god reliabilitet då källan då anses som tillförlitlig. Valideringsprocessen bestod av en diskussion kring referensmaterialet där vissa oklarheter kunde lyftas fram och diskuteras. Vi valde senare att genom noggrann validering av dessa kategorier vi fann, basera vår slutgiltiga empiriska studie på valideringsprocessernas resultat.

Dessa resultat kommer på så vis stärka vår empiriska studies giltighet och validitet (Oates, 2006). Detta skedde genom kritisk granskning av data ifrån intervjuer. Vi diskuterade därför det individuella forskningsresultat med varandra för att på detta vis stärka vår opartiska grund. På så vis blev uppgifterna kritiskt granskade i förhållande till varandra samt mot varandra under arbetets gång och vid osäkerheter kring den insamlade teoretiska fakta, diskutera denna. (Martin, 2005)

Den insamlade litteraturen sågs först som idag något föråldrad men vi fann efter vidare litteraturstudier att dessa problem kvarstår även idag. Detta gör att materialet även idag är synnerligen aktuell för vår empiriska forskning.

3.7 Etik

Under våra intervjuer underrättades informanterna angående deras deltagande, som är helt frivilligt, att de kunde välja att vara anonyma om de så önskade. Vi valde även att utforma frågorna på ett vis som ska få informanten att känna sig trygga och bekväma under intervjun. Informanterna fick även senare godkänna det empiriska materialet föra att säkerställa deras verksamhet framställts på ett korrekt vis. (Jacobsen, 2002)

4 Empiri

I följande kapitel presenteras den information som vi fått under våra intervjuer med de tre valda organisationerna angående hur de jobbar med åtgärdsplaner.

4.1 Internationellt företag – Anonymt

Informanten önskade total anonymisering av intervjumaterialet. Eftersom verksamheten arbetar såväl inom som utanför Sveriges gränser har vi valt att nämna företaget i materialet som ”det internationella företaget”(bilaga 4). Informanten arbetar idag på verksamheten som logistikchef och kommer därför i denna uppsats benämnas som ”Logistikchefen”.
Sedan attacken mot World Trade Center i USA den 11 september 2001, har internationella verksamheters säkerhet blivit förändrad såväl inom transport som inom IT-säkerhet. Det har idag satt ett stort krav från internationella verksamheter, och i detta fall kunder till det internationella företaget.

4.1.1 Bakgrund

Under informantens tid i verksamheten har denne sett att verksamhetens struktur och arbete ständigt förändras, detta för att förbli konkurrenskraftiga och förbättra effektiviteten i verksamheten.

Det svenska dotterbolaget ses som en liten men ändå mycket viktig komponent i det internationella företaget som är stationerat utomlands. Dotterbolaget har genom outsourcing nästan hälften av sin verksamhet förlagd hos andra organisationer, men främst sin lagerhållning.

Den svenska enhetens styrka är dess mycket nära samarbete med dess kunder. De har ett stort antal kunder i Asien, USA samt Sverige och övriga Europa.

4.1.2 IT-säkerhet

Organisationens kunder kräver idag god säkerhet så individer, utrustning och varumärken inte skadas. Logistikchefen menade att vi såg detta på verksamheter som Kronfågel, samt i barnmatsburkar för inte allt för länge sedan där de fann glasskärvor i maten. Organisationens

säkerhet innefattas idag av in- och utpassagekontroller, restriktioner, ID kort, lösenord, säkerhetskopiering, regler samt policys. Därmed finns ett mycket stort fokus på just IT-säkerhet.

Logistikchefen menar att de arbetar ur både en extern som en intern syn, och att de har ett nära samarbete med arbetsmiljöverket, räddningstjänsten och liknande. Detta samarbete är extra viktigt då verksamheten ses som ett högriskföretag då de hanterar vissa kemikalier. Den externa vinkeln påverkas dels utifrån kunder men även genom lagar, regler samt moderbolaget.

Vart femte år revideras hela Sverigekontoret och förses med en ny IT-säkerhetsplanering, detta görs genom en grovriskanalys utformad genom en extern konsult från moderbolaget. Det sker även internt i Sverigekontoret varje dag genom att verksamhetsdata noggrant granskas på heltid av en fysisk IT-specialist. De anställda involveras ständigt i IT-säkerhetsarbetet genom deras proaktiva arbetssätt och starka kommunikation med lokala IT-säkerhetsavdelningen, liksom med moderbolaget.

Informanten menar även att ibland är anställda mer förvånade kring hur små restriktioner de själva har och hur stor mängd data de kan ta del av. På detta vis upptäcks ofta datafel i systemet direkt av logistikavdelningen som enligt logistikchefen har större IT-kunskaper än de övriga i verksamheten. Detta är fallet på grund av deras användning av det breda antalet IT-system. Då en individ på verksamheten ska föreslå säkerhetsförbättringar tar moderbolaget alltid detta meddelande på största allvar och problemet granskas.

Organisationen har idag vissa IT-säkerhetsutbildningar, utöver detta har de erfarna säkerhetsexperter som har god kännedom och vet hur de ska agera under riskscenarier. Anställdas kännedom angående säkerhetsbrister samt hur de ska arbeta innan dessa är åtgärdade är även tillräckliga menar informanten. Detta grundas på att de alla vet hur de ska agera i en potentiell krissituation. Informanten menar även att de skulle guidas genom katastrofen av det erfarna lokala eller IT-säkerhetskontoret vid moderbolaget.

Logistikchefen menar att genom erfarenhet har denne sett organisationens säkerhet i ständig förändring utifrån omvärldens ständigt nya krav genom lagar och regler, kundkrav, certifikat och kvalitetssäkringar, ISO, AEB, AEO och liknande. Personalen har även ett gott sinne för kvalitet och kan därför se hur arbete tidigare fungerat och har på så vis ett riskmedvetande tänk, de har på detta vis möjlighet att identifiera problemmönster.

”*Den som inte väljer att utveckla sin organisations säkerhet blir inget långvarigt företag på marknaden*.”
(Logistikchefen, internationell organisation, bilaga 4)

För dagens säkerhetskrav anser informanten att säkerheten i organisationen är tillräcklig, däremot framhäver informanten även att det alltid tillkommer nya krav på förbättring, policys och att regler skärps men att det i alla aspekter pågår ständig förändring.

”*Det är viktigt att inte motverka användbarhet genom säkerhetsåtgärder*.”
(Logistikchefen, internationell organisation, bilaga 4)

Skulle verksamheten inte vara nöjd med nya tänkta förbättringar eller om en individ fått restriktioner så denne inte kan utföra sitt tänkta arbete så meddelas huvudkontoret och hanterar detta. Informanten menar att det ofta är internationella krav som alla måste anpassa sig efter. Anställda under en stor koncern måste till viss grad även kunna anpassa sig till nya förändringar.

4.1.3 Riskhantering

Informanten menar att den värsta typ av systemhaveri verksamheten skulle lida av vore den långvarigare typen av problem, såsom en pågående attack mot Sverigekontoret i samband med förlorad koppling till moderbolaget. Om flera system skulle haverera under en attack skulle även verksamhetens produktion kunna stanna. Detta är även organisationens högst prioriterade områden. Informanten påtalar att just områden som ”tillgänglighet” och ”säker drift” är två områden som alltid varit mycket högt prioriterade. Tillgänglighet säkerställs genom säkerhetskopiering, elförsörjningsreserv, stabila servrar, PC-datorer samt laptops. Säker drift säkerställs genom åtkomstkontroller, användarrestriktioner, krypteringar och liknande.

Under samtliga typer av katastrofscenarier skulle verksamheten kontakta myndigheter menar logistikchefen. Detta för att få en uppdaterad katastrofbild och för att meddela myndigheter då verksamheten är en högriskverksamhet. Organisationen arbetar idag även med skydd av teknisk utrustning såsom skydd av servrar och liknande. Detta skydd är ett krav från moderbolaget, dess kunder såväl som regering. Sverigekontoret har även möjlighet då deras egna servrar skulle gå ner att koppla upp sig och arbeta emot moderbolagets datorpark.

4.1.4 Scenarier

Under våra intervjuer konfronterades informanten med ett antal scenarier och dessa scenariers genomslagskraft kommer här att presenteras.

Under *scenario ett* (bilaga 1) konfronterades informanten med ett fiktivt åskoväder som slog ut verksamhetens elförsörjning. I organisationen finns såklart reservelverk men om även de skulle sluta fungera, menar Logistikchefen att detta skulle kunna leda till att verksamhetens hela produktivitet och arbetsprocedurer skulle slås ut. Logistikchefen menar att de kan arbeta manuellt men detta skulle medföra en mycket stor arbetsbelastning och komplexitet i arbetet. Sverigekontoret är idag helt beroende av att jobba på en extern plats ifall deras nuvarande inte skulle fungera. Kortsiktigt skulle en katastrof innebära förseningar som de senare skulle

kunna ta igen. Långsiktigt skulle detta scenario haft en kraftigare inverkan och omstationering till en extern plats vore ett måste. Detta menar informanten annars kunde medföra förseningar och att kunder skulle kunna gå förlorade.

Logistikchefen menar att de idag arbetar för att reducera risker genom säkerhetskopiering av databas samt dubbla, speglade hårddiskar för den mest vitala informationen på verksamhetens servrar.

Det berättas i *scenario två* (bilaga 1) att vatten börjat läcka in i verksamhetens lokaler genom en trasig vattenledning. Detta vatten har nått verksamhetens tekniska utrustning, förstört denna och mörklägger även lokalen. Informanten menade att fabriken skulle tvingas stänga ner. Detta skulle innebära produktionsförluster samt förseningar snarare än kundförluster, då verksamhetens kunder är mycket lojala. Denna typ av skada beräknas bli åtgärdad relativt snabbt.

Sverigekontoret har varit med om något liknande tidigare fast då genom regnvatten som trängt upp ur källarens golvbrunnar (där servrarna då befann sig). Därför står idag den tekniska utrustningen på betongfundament och brunnarna är förberedda med backventiler och liknande. Tidigare hade även en sub-server gått sönder på grund av ett rör på en toalett, idag är dock tekniken som tidigare nämnt säkrare placerad och dessa risker är närmast obefintliga.

Scenario tre (bilaga 1) beskriver en individ som vill organisationen illa och försöker sabotera dess verksamhet. Detta resulterar i en systemkrasch vilket resulterar i försvunnen affärskritisk data. Det skulle även ta en längre tid att reparera detta sabotage.

Informanten menar att detta skulle medföra att anläggningen skulle stanna upp. Detta menar logistikchefen skulle återställas genom lokala säkerhetskopieringar och externa säkerhetskopieringar hos moderbolaget. Systemet skulle få återställas för att förhoppningsvis avlägsna problemet. Denna externa säkerhetskopiering styrs via program som styr om datatrafiken och ändrar serverplats för att arbetar mot moderbolagets SAP.
Idag arbetar verksamheten utan trådlösa nätverk, informanten menade att detta var en lösning för att undvika nätverksintrång i verksamheten. Logistikchefen påtalar att deras val av endast kabeltrafik innebär att intrång görs mycket svårare. De använder sig även av McAfee för att motverka spam och liknande på persondatorerna. Systemet övervakas av fysiska personer som hela tiden studerar serverstatistik och liknande.

Dotterbolaget arbetar idag proaktivt genom att sända PM till moderbolaget då riskområden upptäcks. Dotterbolaget har idag även ett mycket nära samarbete med sitt egna säkerhetsbolag. Även ett gott samarbete med moderbolaget som sporadiskt skickar ut säkerhetsrevisioner, samt diagnostiserar verksamhetens potentiella riskområden.

Moderbolaget arbetar med ett ”vem ska ha tillgång till vad?” tänkande och bedömer på detta vis ständigt vem som ska ha behörighet till vad. Ibland ökar och ibland sjunker dina rättigheter. Informanten menar även att det är mycket viktigt att meddela huvudkontoret om

så är fallet att säkerheten blir för stark. Detta kan även ha en negativ inverkan på den berörda individens arbete. Nya krav från kunder och omgivning skapar även dessa nya säkerhetskrav.

Dotterbolaget har tidigare fått vara med om vattenläckor, brutna nätverksförbindelser samt explosioner i deras industri, som moderbolagets frankrikekontor fått erfara för bara ett antal veckor sedan påtalade informanten. Logistikchefen menar även att internetattacker med stor sannolikhet också äger rum men deras omfattning är ingen information denne fått ta del av.

Vidare lät vi den intervjuade bedöma hur de i organisationen prioriterade några olika katastrofsituationer och sannolikheten för att särskilda risker skulle inträffa.

Tabell 4.1 Riskestimeringsmatris – Internationell organisation

Riskkategori	Risktyp	Beskrivning	Uppskattad sannolikhet (1-5)[6]	Prioritering (1-10)[7]	N/A Icke relevant
Naturkatastrof	Jordbävning/vulkanutbrott/tsunami	Skadad utrustning	1	10	X
Naturkatastrof	Storm	Strömavbrott, översvämning	5	2	
Naturkatastrof	Snöoväder	Hög belastning av verksamhetens infrastruktur	4	7	
Mänskligt orsakade katastrofer	Terrorism	Explosion	5	1	
Mänskligt orsakade katastrofer	Cyberterrorism/ Crackers	Dataskadegörelse	5	3	
Mänskligt orsakade katastrofer	Internetattack	Systemet överbelastas, offlineläge	4	4	
Mänskligt orsakade katastrofer	Sabotage	Dataförlust	3	9	
Mänskligt orsakade katastrofer	Social engineering/ Hackers	Dataintrång	3	8	
Oavsiktliga eller tekniska katastrofer	Felanvändning	Ogiltig data	4	5	
Oavsiktliga eller tekniska katastrofer	Tekniskt konstruktionsfel	Systemhaveri	4	6	

Naturkatastrofer sågs inte som några sannolika riskområden och prioriterades därför inte i dagsläget men skulle kunna vara för moderbolagets kontor placerade i riskländer. Även prioriteringen skulle kunna vara något förändrad ur moderbolagets synvinkel. Storm och

[6] Lågt nummer = Låg sannolikhet
[7] Lågt nummer = hög prioritering

snöoväder är dock desto vanligare och prioriteras därför högre. Terrorism ses också som ett mycket sannolikt område då verksamheten är aktivt i ett stort antal länder, explosioner ses också på med mycket stor oro. Internetattacker såväl som felanvändning är även orosområden som logistikchefen hade liten eller dålig information angående fast det är frågor som med stor säkerhet äger rum på dagsbasis.

4.2 Nationell organisation – Försvarsmakten

Informanten önskade att vara anonym men organisationen, Försvarsmakten, får nämnas i uppsatsen. Organisationen arbetar såväl på nationell- som på internationell nivå, verksamhetsområdet för vår studie förekom främst på nationell nivå (bilaga 3). Försvarsmakten ville endast nämnas som en organisation och den enskilda informanten valde att vara anonym därför anonymiseras dennes uppgifter i såväl empiri som i intervjumaterial. I riskestimeringsmatrisen fick inte vår kontaktperson lov att uppge alla posters prioritering då dessa är sekretessbelagda.

Försvarsmakten arbetar för att utbilda; armé-, marin-, och flygförband för att i framtiden kunna stå till förfogande för insats. Organisationens utbildningsförband innefattas av insatsresurser för beredskap i form av bland annat skyddsstyrkor, beredskapstroppar samt hemvärnsförband.

4.2.1 Bakgrund

I Försvarsmaktens uppdrag ingår att hävda Sveriges nationella integritet och stödjande av det svenska samhället vid större kriser. Varje år genomför verksamheten ett antal nationella insatser, bland annat i form av brandbekämpning, ammunitionsröjning samt eftersök av försvunna personer. (Försvarsmakten, 2011)

4.2.2 IT-säkerhet

Försvarsmakten reviderar och utvecklar sin IT-säkerhetsplan och åtgärdsplan regelbundet. Interna samt externa krav på säkerhet och verksamheten behandlas i en riskanalys med värdering och beslut om säkerhetsåtgärder. Åtgärder sker grundat på bland annat det skyddsvärde av information som hanteras i organisationens respektive system.
I organisationen har de årlig utbildning samt proaktivt tänk genom allmän vardaglig livsföring (ADL), såsom regelbunden information om risker. Försvarsmakten menar att säkerheten aldrig är 100-procentig. Förändringar i regelverk, organisation, arbetssätt och teknik ligger till grund för kontinuerlig riskhantering. Nationella och internationella standarder och best practices samt nationellt fastställda normer är några av värderingskriterierna.

4.2.3 Riskhantering

Vår informant får inte delge Försvarsmaktens bedömning av aktuell hotbild men menade att det värsta som skulle kunna hända ur ett haveriperspektiv vore risker som skulle medföra att någon eller några individ(er) skulle kunna komma till skada eller bli drabbade på något vis. Detta är risker som verksamheten idag arbetar mest på att reducera. Detta görs bland annat i vår informants arbete där denne arbetar dagligen med att förbättra verksamhetens område för IT. Då vår informant föreslår förändringar i verksamheten som gynnar säkerhet blir denne individs förslag på förbättringar mestadels accepterade hos ledningen.

4.2.4 Scenarier

I vårt frågeformulär fick även informanten konfronteras med ett antal scenarier och dessa scenarions inverkan och prioritering i verksamheten kommer här att presenteras.

Under *scenario ett* (bilaga 2) konfronteras verksamheten med ett E-posthaveri som omöjliggör all kommunikation via e-post. Detta menade vår informant framförallt skulle leda till att verksamheten förlorade tid och därigenom resurser, det främsta problem detta skulle medföra vore de ökade svårigheterna i att uppfylla offentlighetens krav. Idag arbetar verksamheten genom goda redundanta system samt säkerhetssystem för att inte dessa riskscenarier ska kunna uppstå. Detta scenario skulle innebära stora svårigheter vid kommunicering med omvärlden och detta skulle tvinga organisationen att hitta alternativa sambandsvägar och redundanta system. Denna verksamhet liksom många andra är idag högst beroende av Informationsteknik (IT) och därför skulle verksamheten inte kunna fortgå under så lång tid utan användande av IT.

Vid *scenario två* (bilaga 2) kraschar organisationens webbsida på grund av en internetattack på webbplatsens server, vilken ägde rum precis under ett rekryteringstillfälle. Detta menade vår informant skulle innebära att organisationens förtroende i någon mån skulle skadas. Förtroendet skulle skadas eftersom att intressenten inte skulle få den information denne önskar. Skadan kan reduceras genom redundanta system.

Under *scenario tre* (bilaga 2) uppdagas en skandal inom Försvarsmakten och organisationen får på så vis stort fokus i media, detta sker i anslutning till att webbservern skadas genom en vattenläcka vilket gör att webbplatsen går ur bruk. Försvarsmakten menade att mediedrev alltid hanteras genom information och saklighet, media skulle därför på något annat vis underrättas om läget på verksamheten vid en presskonferens. Verksamheten tillåter idag inga former av vatten i deras serverrum och risken anses därför obefintlig. Verksamheten arbetar på samtliga plan genom att kontinuerligt kontrollera sin teknik och kräver ständigt ett godkännande före drift.

Försvarsmakten menar att tekniska fel samt möjligheterna för sabotage i verksamheten är obefintliga då de har goda principer och policys med åtkomstkontroller och säkerhetssystem för att proaktivt reducera dessa risker. Informanten fick inte lov att beskriva organisationens prioriteringar bland dessa risker. Informanten fick heller inte uppskatta sannolikhet för IT-brottslighet riktad mot organisationen såsom terrorattentat, IT-attacker och liknande.

Informanten fick även fylla i en riskestimeringsmatris där denne fick bedöma hur stor sannolikhet vissa risker har och hur de prioriteras i organisationen. Dessvärre var en del sekretessbelagt, dessa representeras av de gråa raderna.

Tabell 4.2 Riskestimeringsmatris - Nationell organisation

Riskkategori	Risktyp	Beskrivning	Uppskattad sannolikhet (1-5)[8]	Prioritering (1-10)[9]	N/A Icke relevant
Naturkatastrof	Jordbävning/vulkanutbrott/tsunami	Skadad utrustning			N/A
Naturkatastrof	Storm	Strömavbrott, översvämning	4		
Naturkatastrof	Snöoväder	Hög belastning av verksamhetens infrastruktur	4		
Mänskligt orsakade katastrofer	Terrorism	Explosion	--------	--------	--------
Mänskligt orsakade katastrofer	Cyberterrorism/ Crackers	Dataskadegörelse	--------	--------	--------
Mänskligt orsakade katastrofer	Internetattack	Systemet överbelastas, offlineläge	--------	--------	--------
Mänskligt orsakade katastrofer	Sabotage	Dataförlust	1		
Mänskligt orsakade katastrofer	Social engineering/ Hackers	Dataintrång	--------	--------	--------
Oavsiktliga eller tekniska katastrofer	Felanvändning	Ogiltig data	4		
Oavsiktliga eller tekniska katastrofer	Tekniskt konstruktionsfel	Systemhaveri	1		

Naturkatastrofer i Sverige sågs inte som något sannolikt riskområde och var därför inte relevant för en verksamhet i Sverige. Stormar och snöoväder är däremot några riskfaktorer som är vanliga i norden och prioriteras därför högre.

[8] Lågt nummer = Låg sannolikhet
[9] Lågt nummer = hög prioritering

4.3 Regional organisation - Svedala kommun

I vår uppsats ville vi intervjua personer ifrån organisationer som befinner sig på olika nivåer. Vi valde därför att kontakta Svedala kommun. I och med att Svedala är en offentlig organisation var anonymitet inget som önskades av organisationen. Två intervjuer utfördes hos Svedala kommun. Först tillsammans med intervjupersonen, Hans-Åke Olsson, som är enhetschef på Svedala kommuns IT-support samt en kompletterande intervju i en annan del av organisationen, där den intervjuade har valt att förbli anonym.

4.3.1 Bakgrund

På den avdelning där Hans-Åke sitter sköts allt som berör IT inom kommunen, alltifrån förläggning av fiber, till installationer samt drift av system (bilaga 5). Han har jobbat på den positionen i ungefär 6 år och har därmed god kunskap inom hur organisationen fungerar och de risker som de stöter på.

Vår andra intervjuperson sitter i en annan del av organisationen och har inget ansvar gällande IT i sin position nu, men har tidigare arbetat med IT och organisationens riskhantering (bilaga 6). I och med att organisationen är av mindre karaktär jobbar intervjupersonen brett och har flera personer att rapportera, inom flera olika projekt.

I kommunen finns ett flertal system som alla drivs och hanteras på denna avdelning. Deras jobb syftar till att övriga verksamheter som ingår i kommun ska kunna fortskrida med sitt arbete, detta involverar bland annat både vård och skola. Som en avdelning i Svedala kommun sker all rapportering till kommunledningen, där de huvudsakliga och betydande besluten fattas.

Hans-Åke beskriver organisationen som en bra organisation och att han trivs att jobba i den. Han beskriver också att det särskilda i organisationen är att alla ska kunna göra allt. Det finns såklart specialiseringar men att det är viktigt att allt förtroende samt beroende inte ligger på en enskild individ utan att det ska finnas flera kunniga inom området. Ett viktigt arbetsmål för Svedala kommun och särskilt IT-avdelningens är att kunna erbjuda bästa möjliga service och utveckling till en så låg kostnad som de möjligt kan.

Även vår andra informant beskriver organisationen som en bra och välfungerande kommun, där de betonar att insatsen som utförs alltid ska vägas mot nytta. Informanten menar att det är viktigt att varje insats tillför kommunen något. Därmed har de i organisationen ett ständigt ifrågasättande av insatser och de vill uppmuntra medarbetare till att göra just detta, för att förbättra samt utveckla organisationens arbete. Intervjupersonen beskriver även att det i organisationen ska gå att påverka organisationens arbete, och att det tänket är viktigt. Frihet

under ansvar och att anställda ska kunna ta egna initiativ, detta ska driva kommunen framåt.

Svedala kommuns organisation är indelad i fyra verksamhetsområden, alla dessa har sin egen kultur och har kommit olika långt i sin IT-utveckling. Denna utveckling håller nu på att förbättras och kommer att vidare utvecklas framöver.

I och med att det är en kommun där ledning förändras var fjärde år i samband med val, är det viktigt att det finns kunnigt folk i organisationen som kan sköta arbetet så att inte arbetet stannar upp.

För att förbli konkurrenskraftig jämför de sig själva gentemot andra kommuner, gällande både kostnader och effektivitet.

4.3.2 IT-säkerhet

Hans-Åke förklarar att organisationen självklart utsätts för både interna och externa hot; exempelvis att någon skulle kunna ta sig in i deras system eller att någon form av haveri skulle ske. Organisationen jobbar därför aktivt internt med att försöka begränsa detta till den grad att det inte ska vara möjligt. I sitt arbete har de i kommunen använt sig av fiktiva scenarion för att förutse eventuella händelser. För att reducera organisationens risker, både interna och externa, använder de sig bland annat av policys. Om någonting trots flertalet åtgärder skulle inträffa finns olika former av larm som gör anställda uppmärksamma på vad som sker eller har inträffat.

Svedala kommun utvecklar och reviderar inte helt själva sin åtgärdsplan utan hyr in konsulter ifrån KPMG som granskar arbetet och planen. Under denna granskning använder sig KPMG av en checklista för att analysera de risker som finns i organisationen, vad som bör prioriteras och framförallt planeringen inför dessa risker. De har även i organisationen använt sig av BITS plus (Basnivå för informationssäkerhet), där det finns en samling åtgärdsplaner med steg för hur arbetet ska hanteras och vem som ska ha ansvar i särskilda situationer. Detta arbete sker utefter det mönster som finns BITS och är inget som de avviker ifrån, samtliga frågor ifrån BITS ska besvaras.

Vår andra informant ser inga särskilda hot, däremot påpekar denne att de tillsammans med SÄPO har gått igenom vilka risker som organisationen ställs inför. Sen dess har organisationens fastigheter gjorts säkrare med exempelvis låsta dörrar, så att obehöriga inte ska kunna gå som de vill. För att anställda ska veta hur de ska agera i särskilda krissituationer sätter riskhanteringsansvariga ihop ett antal scenarier en gång om året där anställda får öva på hur de ska hantera sådana situationer. Dessutom plockar räddningstjänsten fram risk- och sårbarhetsanalyser varje år, där de värderar alla risker. Vidare har kommunen ett nätverk när det gäller säkerhetsarbete ihop med Lomma kommun, Staffanstorp kommun och Kävlinge kommun. Där de fyra kommunerna samarbetar för att förbättra sin säkerhet. Svedala kommun jobbar mycket med just säkerhetsarbete och det involverar även särskilda möten på olika orter

i Sverige som behandlar ämnet. Som tidigare nämnt använder de sig även av BITS i sitt arbete och har speciella revisioner på säkerheten.

IT-avdelningen som har ansvaret för det som berör organisationens system och eventuella haverier, har försökt engagera kommunens anställda i åtgärdsplanerna och dess utveckling men har inte fått något gehör ifrån kommunledningen. På IT-avdelningen vill de gärna att samtliga anställda genomgår en introduktionskurs på en timme, dessvärre anser ledningen att det skulle kosta för mycket och utbildning har därför uteblivit. Kostnadsargumentet grundas på att med 1500 anställda skulle detta nästan motsvara ett helt manår, 1700 timmar, vilket är mycket.

Svedala kommun vill givetvis att deras system ska finnas tillgängliga samt fungera, därför strävar de efter att inte låta systemet ligga nere i mer än två timmar. För att organisationen ska erhålla en högre säkerhet måste budgeten för det dubblas och det finns det inte resurser till. Vidare jobbar organisationen kontinuerligt för att hålla obehöriga borta. Detta sker med hjälp av kort med chip, bank-id eller liknande.

På IT-avdelningen anser de anställda att utbildningen som gäller åtgärdsplanerna är väldigt viktig, men tid och pengar användes till annat. Så trots IT-avdelningens förslag på förbättring i säkerheten får detta inte alltid acceptans i ledningen. Vidare har de försökt höja säkerheten genom att förlänga de anställdas lösenord eller göra dem mer komplexa. De har också föreslagit att samtliga ska byta lösenord var 60:e dag, och den då sparar de 12 senaste lösenorden så att anställda inte ska kunna gå tillbaka till ett tidigare använt. Dessvärre har samtliga förslag slagits ner av ledningen då det blir för svårt för användarna och för svårhanterligt.

Vår andra Informant håller med Hans-Åke om att en introduktionskurs borde finnas för att underlätta hela arbetet, men påpekar också att förslag troligtvis hade fått acceptans om de lyft ärendet till politiken istället för enbart inom tjänstemannaorganisationen. Informanten menar här att förslaget inte lagts fram på bäst sätt och inte heller tillräckligt förklarats så de som nekade förslaget troligtvis inte förstått orsaken.

Finns det tydliga och övertygande argument till ändringarna, så accepteras de flesta fall. Det kan ofta vara svårt att övertyga i början men till slut går det oftast igenom.

Vidare hanterar kommunen system som de flesta privatpersoner inte känner till, bland annat vårdplanering. Där en person behandlas på sjukhus och när denne är färdigmedicinerad kontaktar de kommunen som då har 24 timmar på sig att fixa en vårdplats om så behövs. Annars blir kostnaden 5000 kronor per dygn, vilket snabbt kan bli mycket pengar. Därför är det väsentligt att detta system fungerar, så att kommunen får informationen snabbt och kan behandla den.

4.3.3 Riskhantering

Enligt Hans-Åke är det absolut värsta som organisationen skulle kunna ställas inför inte att ett system tillfälligt rasar utan att de förlorar data. Vilket skulle kunna hända om säkerhetskopiering saknas eller att det har blivit fel när den görs. En sådan förlust skulle kunna påverka ett flertal verksamheter i kommunen. Detta i sig skulle också leda till att arbetet i kommunen skulle kunna stanna upp i ett par dagar, i de fall där de använder sig av ett system som förlorat data. Det blir genast mycket omständigare och tidskrävande om data saknas. Att lägga in data förhand är idag nästan omöjligt då det finns väldigt mycket data i systemen. Idag använder sig system av redundans, minst två servrar, säkerhetskopiering, speglingar innan säkerhetskopior. Vidare gör Svedala kommun en säkerhetskopiering av all sina data varje natt.

Vår andra informant anser däremot att det absolut värsta som skulle kunna hända ur ett systemhaveriperspektiv, går att se ur fler aspekter än just de tekniska. Exempelvis om avlopp och reningsverkssystem skulle haverera skulle allt det rinna ut i Sege Å och förorena vatten och miljö. Det värsta som intervjupersonen själv varit med om är när det inte har gått att betala ut socialbidrag och det har kommit personer till kommunhuset och varit arga samt hotat med exempelvis yxa. Vidare så skulle bland det värsta vara om någon hackade sig in och stal stora summor av pengar. För att säkert hantera organisationens ekonomi får inte en person göra utbetalningar till sig själv, gällande lön eller liknande. Vidare så måste två oberoende personer skriva under en faktura.

Båda informanter är överens om att om någon katastrof eller risk skulle inträffa prioriteras de mest samhällskritiska systemen och risker som är samhällsfarliga, därtill hör; löne- och personaladministrativa system, vård, mejl, inloggning, webbservrar samt vatten- och avloppssystem. Vidare Följer de även de policys och prioriteringar som de statliga myndigheterna har utfärdat. Detta genom att prioritera de funktioner och personal som är mest nödvändig.

Vidare nämner Hans-Åke risken att någon bonde ska gräva av en fiberoptik kabel, vilket har förekommit. Detta hindrar internetuppkoppling i organisation, så därför ändrar de nu i dessa så att om en kabel grävs av kan det köras någon annan väg.

Svedala kommun uppmuntrar även sin anställda till att lämna förslag på förbättringar, både gällande säkerhet och resterande arbete. De har därför satt upp en förslagslåda, där anställda kan lämna in sina förslag och tilldelas då med en biobiljett, och i vissa fall även en mindre ekonomisk ersättning. Detta gäller främst anställda där detta arbete inte ingår i deras arbetsuppgifter. Sen kan givetvis vissa ändringar vara svåra att göra och kan dröja, just för att personer är rädda för förändringar.

4.3.4 Scenarier

Under intervjun ställs personen inför tre fiktiva scenarier där de ska förklara hur ett sådant fall skulle påverka dem och hur de arbetar med risken nu.

I *scenario ett*(bilaga 1) konfronteras den intervjuade med ett åskväder som slår ut strömmen hos organisationen. Situationer likt denna har de på Svedala kommun planerat för och har dubbla reservkraftlösningar som går in om de skulle få ett strömavbrott. Främst använder de sig av UPS/reservkraft som genererar tillräckligt för att det väsentligaste ska fungera, såsom server. Om den också skulle sluta fungera finns ett dieselkraftverk som går in som en extra reserv. I och med att dessa reservlösningar inte kan generera lika mycket, har de på kommunen prioriterat ungefär 10 system som är samhällskritiska. Detta för att de viktigaste och de mest betydelsefull systemen ska finnas tillgängliga ändå.

Skulle de ställas helt utan ström, skulle klara problem uppstå. Detta eftersom bland annat vården kräver att system finns tillgängliga dygnet runt. Det finns säkerhetskopior i pappersformat till systemen, däremot skulle det bli betydligt komplexare och arbetet kan inte fortgå särskilt länge på så vis. Likadant gäller vatten och avloppssystem som är datastyrt, även detta kan skötas manuellt men är betydligt svårare. Därmed skulle organisationen få tydliga och stora problem om de fick ett långvarigt strömavbrott.

Vår andra informant framhäver här att denne kan klara sina arbetsuppgifter utan tillgång till informationssystem och menar att alla inte påverkas av en sådan situation. Informanten håller med om vad Hans-Åke sagt om komplexitet, men tilläger också att det inte är omöjligt att sköta det manuellt. Vidare framhävs att det även finns särskilda delar på året då det är extra kritiskt om särskilda IT-system havererade under en längre tid.

I *scenario två* (bilaga 1) har ett vattenläckage orsakat en kortslutning. Svedala har planerat inför just sådan situation också, detta genom att ha redundanta serverrum. Så att det alltid finns ett som fungerar. Servrarna är visserligen vattenkylda men om ett läckage skulle uppstå där skulle finns en ventil som stänger av det.

Vår andra informant lyfter även här fram konsekvenserna varierar beroende på vilken position de har i organisationen. Den intervjuade påverkas likt tidigare scenario, och kan sköta sitt arbete ändå eller ta ledigt då denne inte har några löpande arbetsuppgifter. Däremot hade en sådan situation varit katastrof för exempelvis de som jobbar i kassan eller för kärnverksamheten. Som tidigare nämnt finns papper men det blir mer komplicerat att sköta arbetet så.

I *scenario tre* (bilaga 1) försöker någon sabotera verksamheten genom att förstöra utrustning och i systemen. Hans-Åke menar här att det i organisationen är väldigt få som har tillgång till serverrummet och för att hålla obehöriga ute använder de sig av lösenord, brickor och hänglås på en andra dörr. En sådan situation skulle i organisationen främst leda till förlorad arbetstid och ett omfattande återställningsarbete. Om organisationen skulle stå utan system under en

tid, skulle det kunna leda till en mindre finansiell förlust. Detta eftersom arbetet helt skulle stanna upp framtill problemet lösts.

De sker vidare även en viss övervakning över trafik ut och in, så att felanvändning kan upptäckas. Detta har förekommit i organisation och det har då resulterat i en uppsägning av den anställda.

Vår andra informant förmodar att om personen lyckats så hade blivit en ganska jobbig situation däremot hade inte lett till någon personlig skada. Återigen handlar det om att det hade blivit besvärligare att göra allting manuellt. Vidare skulle det bli mycket jobb att ta igen allt som kommunen inte kunnat göra. Situationer likt dessa kan även vara utvecklande för organisationen, då de kan lära sig ifrån en sådan situation, vad som ska prioriteras och vad som måste hanteras.

Svedala kommun håller just nu på med ett projekt där de ska sätta ihop ett råd kallat trygghet och säkerhet med medlemmar ifrån både tjänstemanna organisation samt ifrån politiken. I detta råd ska alla säkerhetsfrågor diskuteras.

Organisationen har under de senaste 5 åren inte stött på någon större katastrofsituation, utan främst kablar som har grävts sönder, mejlstopp och telefonstopp. När fiberoptikkablar har förstörts har givetvis internetuppkoppling stoppats men det har ofta lösts snabbt. I fallet då den fasta telefonin låg nere fanns fortfarande tillgång till mobiltelefoner och de kunde därmed använda sig av dem till problemet blivit löst. Främst hanterar de sådana situationer genom att meddela samtliga anställda så de är medvetna om situationen.

Informanterna fick båda fylla i en riskestimeringsmatris där de skulle göra en bedömning på sannolikhet och vilken prioritering organisationen gjorde (se Tabell 4.3). Nedan följer de två informanternas bedömningar. De blå kolumnerna representerar Hans-Åkes svar och de vita representerar vår andra informants svar. Tydligt framgår här deras olika bedömning och prioriteringar är väldigt olika.

De risker som organisationen prioriterade och arbetade för att reducera enligt Hans-Åke, var främst sabotage, Social engineering, hackers, felanvändning samt tekniska konstruktionsfel. Dessa prioriterades alla lika mycket, och det var inte någon som hade högre fokus. Naturkatastrofer och terrorism hade mindre eller inget fokus i säkerhetsarbetet, utan främsta fokus låg på de mänskligt orsakade katastroferna samt oavsiktliga eller tekniska katastrofer.

Informanten i den kompletterande intervjun framhäver att IT-avdelningen håller de tekniska problemen för sig själv om det skulle vara några problem, därmed är inte övriga särskilt insatta i just det. De risker som bedöms ha högst sannolikhet och därför har fått högst prioritering är storm och snöoväder. Terrorism och exempelvis jordbävning anses inte vara relevanta.

Tabell 4.3 Riskestimeringsmatris - Regional organisation

Riskkategori	Risktyp	Beskrivning	Uppskattad sannolikhet (1-5)[10]		Prioritering (1-10)[11]		N/A Icke relevant	
Naturkatastrof	Jordbävning, vulkanutbrott, tsunami	Skadad utrustning	1	1	10		X	X
Naturkatastrof	Storm	Strömavbrott, översvämning	2	5	9	2		
Naturkatastrof	Snöoväder	Hög belastning av verksamhetens infrastruktur	2	5	9	1		
Mänskligt orsakade katastrofer	Terrorism	Explosion	1	1	10		X	X
Mänskligt orsakade katastrofer	Cyberterrorism, Crackers	Dataskadegörelse	2	2	5	5		
Mänskligt orsakade katastrofer	Internetattack	Systemet överbelastas, offlineläge	4	2	5	4		
Mänskligt orsakade katastrofer	Sabotage	Dataförlust	2	1	1	8		
Mänskligt orsakade katastrofer	Social engineering, Hackers	Dataintrång	3	1	1	6		
Oavsiktliga eller tekniska katastrofer	Felanvändning	Ogiltig data	5	1	1	7		
Oavsiktliga eller tekniska katastrofer	Tekniskt konstruktionsfel	Systemhaveri	2	2	1	3		

4.4 Jämförande studie

I detta delkapitel kommer vi göra en jämförelse mellan de tre organisationernas metoder, bedömningar och prioritering. Här kommer vi att lyfta fram vad som skiljer de organisationer åt och vilka likheter det finns mellan dem.

4.4.1 Anställdas involvering

På den regionala organisationen hanterades verksamhetens IT-säkerhet av driftstekniker på IT-kontoret. Organisationen reviderade säkerheten enligt externa krav för att etablera en basnivå för informationssäkerhet genom att undersöka verksamheter enligt bestämda mönster, liknande de som finns i GAIT(delkapitel 2.9). Denna revidering utformades med hjälp av

[10] Lågt nummer = Låg sannolikhet
[11] Lågt nummer = hög prioritering

externa konsulter från KPMG, samt genom viss statlig inblandning.

Även på det internationella företaget involverades verksamhetens anställda genom proaktivt arbete och god kommunikation med sin IT-säkerhetsavdelning där riskfaktorer snabbt skulle lyftas fram. Den internationella organisationen innehåller ett flertal likheter med den nationella organisationen, Försvarsmakten, genom deras mycket likartade arbete och prioriteringar. Då båda organisationer hade stora förlagda resurser på drift och tillgänglighet så hade de på så vis en mycket stor IT-säkerhetsavdelning både vid det internationella företagets dotterbolag såväl som hos dess moderbolag. Dessa avdelningar på den nationella- såväl som på den internationella organisationen hade fysiska personer som dygnet runt granskade in-, och utdata samt nätverksstatistik. Denna diagnostisering skedde med ständigt fokus på att hitta brister i informationssystem samt i verksamhetens tekniska utrustning. På båda dessa organisationer var därför användarnas involvering inte lika överhängande som vid den regionala organisationen då de avsatt personal för systematisk granskning och proaktivt arbete.

IT-säkerheten på samtliga organisationer var även god för avvärjning av icke-legitima användare genom åtkomstkontroller och liknande enligt delkapitel 2.7. Åtkomstkontroller finns i form av in- och ut kontroller samt lösenord på verksamhetens utrustning. Dessa åtkomstkontroller och starka säkerhetsarbete var påtvingat från staten på den internationella organisationen då denna klassades som en högriskverksamhet. Den regionala organisationen hade även de dessa typer av kontroller för att hindra illasinnade personer från att ta sig in i organisationens lokaler och förstöra organisationens informationssystem eller skada de anställda. Vilket betyder att samtliga organisationer är väl medvetna om hur de fysiskt ska förhindra obehöriga ifrån att komma åt informationssystem och informationsteknik.

Om en obehörig person skulle ta sig igenom denna barriär in i verksamhetens informationssystem så skulle organisationens möjlighet att upptäcka illasinnad användning spela en enormt stor roll. Detta skulle vid den internationella, samt nationella organisationen snabbt upptäckas av fysiska personer anställda för granskning av all ut-, och in- trafik sökande efter misstänksam aktivitet. Däremot skulle detta inte vara fallet hos IT-säkerhetspersonalen vid den regionala verksamheten där denne individ skulle kunna vistas en något längre tid innan förövaren skulle identifieras av verksamhetens automatiserade detekteringssystem.

Den internationella organisationen hade idag vissa IT-säkerhetsutbildningsprogram bland cheferna, men presenterade också att de redan visste hur de skulle arbeta genom att de dagligen indirekt arbetar med säkerhet. De blir då uppdaterade genom inströmmande rapporter och liknande. Den nationella organisationen hade utbildningar samt individuellt lärande hos individer i verksamheten med vissa likheter hos den internationella verksamheten. Den regionala organisationen saknade tyvärr utbildningar, men här såg vi även att de anställda inte uppdaterades med ny information i sitt arbete. De hänvisade endast till IT-avdelningen som arbetade på sitt håll med IT samt övrig personal på sitt respektive område.

4.4.2 Utveckling och underhåll av åtgärdsplaner

Idag revideras samtliga organisationer i det närmsta på årsbasis av IT-säkerhetsavdelningen. Den internationella organisationen reviderades även av moderbolagets avdelning för IT-säkerhet, samt vart femte år skedde en totalrevidering av denna organisation grundligt av ett externt säkerhetsföretag. Samtliga organisationers revideringar utformades enligt omvärldskrav så som vid den internationella organisationen genom kundkrav, lagar och kvalitetssäkringskrav. För att inte kunna hålla en viss säkerhet i sin verksamhet och sina affärer skulle detta skapa en osäkerhet bland kunder vilket i sin tur skulle medföra att kunderna skulle välja en annan verksamhet. Det var inte mycket fakta tillgänglig i denna del hos den nationella organisationen dock kunde vi se mycket tydliga likheter på såväl nationell som på internationell nivå.

Den internationella verksamheten som var aktiv i såväl Europa som USA och Asien hade självklart större krav på sig. Även den nationella organisationen; Försvarsmakten hade även ett större krav på sig då bristande IT-säkerhet skulle kunna leda till mänskliga förluster såsom i krig. Dessa krav är inte lika stora på en regional organisation som på högre organisationsnivåer men verksamheten är viktig även på sin regionala nivå.

4.4.3 Riskprioritering

I riskestimeringsmatrisen ansåg sig den internationella organisationen ha stor sårbarhet om en explosion skulle inträffa, därför har det prioriteras högst och är den risk som de arbetar mest för att reducera. Det gäller inte bara terrorism utan explosioner som helhet. Medan det för den regionala organisationen inte är en risk som är relevant, som de arbetar med eller egentligen har med i sin riskhantering.

Vidare gällande skillnader i prioritering går det att se att av de kategorier av katastrofer, som redovisas i delkapitel 2.1, prioriterar den internationella organisationen några av de mänskligt orsakade katastroferna, och framförallt Terrorism, cyberterrorism/crackers samt internetattacker, högre än den regionala organisationen. Detta eftersom de anser att sannolikheten för dessa är hög, gentemot regionala som inte satt särskilt högt på just dessa.

I vår inledande intervju med den regionala organisationen, påpekades att det värsta som skulle kunna hända hos dem var ett informationssystemhaveri som ledde till dataförlust. Därmed har de satt en hög prioritering på just den risken. Denna risk är den enda mänskligt orsakade risk som den regionala organisationen prioriterat högre än den internationella.

4.4.4 Största säkerhetshot

Det värsta som kunde hända den internationella organisationen var en långvarig attack där de förlorade kontakten med moderbolaget. Den regionala organisationen har i den inledande intervjun nämnt dataförlust som det värsta som kan hända, men att det inte är särskilt troligt. Vilket överensstämmer någorlunda med vad som bedömts i matrisen. Den nationella organisationen däremot menar att det värsta som kan hända hos dem ur ett informationssystemhaverisammanhang är att någon individ skulle kunna komma till skada. Vilket vi tolkar som någon form av informationssystemhaveri som antingen berör personligintegritet eller som på något vis kan orsaka en fysisk skada. Dessa skillnader i bedömning av den absolut värsta situationen tyder på att de har olika omvärldskrav och mål att uppnå.

4.4.5 Tekniskt beroende

Angående tekniskt beroende i organisationerna kan vi se att samtliga organisationer har ett tydligt beroende av sin informationsteknik, och de data som informationssystem hanterar. Samtliga organisationer påpekar att de då skulle tvingas sköta arbetet manuellt fram till att systemhaveriet blivit löst, men de tillägger också att detta skulle bli betydligt mer komplicerat och att de inte fullt ut skulle kunna sköta sina arbetsuppgifter. Vidare poängteras att ett långvarigt haveri skulle kunna orsaka kraftiga förseningar.

4.4.6 Säkerhetsplan

Som nämnt har en del organisationer papperskopior, men i hopp om att slippa använda det har samtliga planerat för att säkra sin teknik. Detta genom att ha säkerhetskopiera sin information och använda sig av två servrar, redundans, så att verksamheten inte stannar upp om en server slutar fungera. Överlag uppfattar vi samtliga organisationer medvetenhet av just den tekniska aspekten och att säkra sin teknik som hög. De har alla redogjort för hur de har flera servrar, speglingar, lösenordskydd samt låsta dörrar. Samtliga organisationer som intervjuats arbetar på något vis med att skydda sin informationsteknik och även anställda från exempelvis externa hot. Detta genom att på olika sätt exempelvis skydda sina servrar från olika risker, där de har höjt upp dem från marken, flera låsta dörrar och endast viss behörig personal för att nämna några. Det finns alltså god kunskap inom just dessa områden i organisationen, vilket klart är positivt.

5 Diskussion

I detta kapitel kommer vi att diskutera hur de olika organisationerna arbetar med åtgärdsplaner samt sätta dessa metoder i relation till den litteraturen som presenterats i kapitel 2. Denna diskussion bygger på de empiriska studier som gjordes inom de tre organisationstyperna: internationell, nationell samt regional nivå. Här kommer resultatet av empirin diskuteras och jämföras med tidigare erkänd forskning. Genom vårt val av organisationer fick vi på detta vis möjlighet att empiriskt undersöka de tre tidigare nämnda organisationstyperna, vilka hade olikheter såväl som vissa gemensamma nämnare. Diskussionen kommer även utmynna i eventuella förslag på förbättringar, utifall att deras nuvarande IT-säkerhet skulle ses som bristfällig.

5.1 Anställdas involvering

I litteraturen lyftes vikten av involvering av anställda i säkerhetsarbetet tydligt fram, för att på detta vis gynna organisationernas proaktiva tänk. Samtliga studerade organisationer hade IT-säkerhetskontor som hanterade verksamhetens in-, och utströmmande data samt supportärenden. Dessa studerade organisationer hade även personal som i viss omfattning granskade denna nätverksstatistik med vissa skiljaktigheter. Beroende på organisationens storlek ökade även dess krav på säkerhet och på så vis i sin tur storleken på IT-säkerhetsavdelningen.

Det är mycket viktigt att IT-säkerhet är något verksamheten tar på största allvar, och inte endast arbetas med vid en säkerhetsavdelning, vilket beskrevs i delkapitel 2.5. På den regionala organisationen gynnade förslag och nya idéer genom en förslagslåda där förslag premierades beroende på dess vidd för detta att utveckla sitt erhållna IT-säkerhetsprogram. Intressant vore att se hur många som faktiskt lägger ner det lilla extra arbetet på att lägga fram ett ordenligt begrundat förslag om det kan belönas jämfört med om de inte fick något för det. Att be anställda att lämna förslag är ett bra sätt att få in åsikter på förbättring ifrån olika delar i organisation, även om belöningen för arbetet inte alltid innebär något stort så är ett bra sätt uppmuntran anställda till att vilja förbättra och driva organisationen framåt. Dock så kan denna metod leda till att anställda lägger i dåligt utarbetade förslag bara för att få biobiljetter eller annan kompensation. Var dras i så fall gränsen för var ett förslag är tillräckligt bra för att belönas och vilka belönas med ekonomisk ersättning?

Det intressanta i den internationella organisationen är att, då problem uppstår ska denna avdelning hjälpa till genom att lämna direktiv på hur arbetet ska skötas, då de har god

kunskap inom området. Om det däremot uppstår mer omfattande problem vilka berör flera delar eller många anställda skulle denna avdelning kunna utsättas för mycket kraftiga påfrestningar då ett stort antal användare skulle behöva support. Det är i sådana situationer det kan vara bra att anställda har någon form av introduktionsutbildning, så de på en grundläggande nivå vet hur de förväntas handla under specifika omständigheter till dess problemområdet avlägsnas enligt delkapitel 2.6. (Loch et al., 1992; Dixon et al., 1992; Straub, 1998)

Den internationella samt nationella organisationen har särskilda personer avsedda för att granska ut- och in- trafik tolkar vi som att detta är ett stort riskområde för dem, i jämförelse med den regionala organisationen. Detta skulle kunna ses ur två perspektiv. Antingen har den internationella samt nationella organisationen ännu inget IT-system för detta, eller också vill de inte ha det. Vill de inte ha det skulle det kunna bero på att de prioriterar denna övervakning högt och därför inte litar på ett system. Vidare har den nationella och internationella organisationen haft bättre beredskap än den regionala, därmed kan detta också vara en kostnadsfråga. Resurser kanske inte finns för att ha någon som kontrollerar trafiken på så vis. Tänkvärt är också om den internationella och nationella organisationen verkligen tjänar så mycket på att ha personer som kontrollerar, gentemot enbart ett IT-system som gör det? Är det egentligen någon större skillnad i effektivitet?

Organisationernas informanter påtalade även vikten av kommunikation, eftersom detta spelar en mycket stor roll i en verksamhet, där ett gott klimat ska genomsyra hela verksamheten. Denna mer familjära känsla kunde vi tydligast se i verksamheter allt eftersom dessa blev mindre; i avdelningar, projektgrupper eller i mindre organisationer där alla kände alla. Detta samspel fann vi tydligast i den regionala organisationen där kommunikationen var bred. Denna typ av kommunikation skulle vi därför ha svårt att se mellan ett dotterbolag och ett moderbolag där språket skulle ske något striktare, i annan form och även mer åtdragen. Vad vi kan se är alltså hur kortare avstånd inom den egna organisationen bidrar till en enklare kommunikation genom hela organisationen, vilket i sig kan vara en betydande faktor om deras informationssystem skulle haverera eller dess internetförbindelse skulle ligga nere. Däremot kan vi i den regionala organisationen antyda en viss brist på kommunikation. Däribland att de kan hålla problem för sig själva och att förslag ifrån IT-avdelningen inte har framförts på ett korrekt och bra sätt.

Delkapitel 2.7 (Brodie, 2008) beskrev att en organisations säkerhetsberedskap skulle kunna gynnas genom utbildande inom IT-säkerhet, eftersom att säkerhetsprinciper måste kännas till för att efterföljas. Dessa kurser förmedlar även den vitala kunskap om risker som medförs av den miljö de i organisationen arbetar i. Dessa kurser skulle även som skildrat i delkapitel 2.4, förvissa personal om åtgärder som vidtagits under året för att öka verksamhetens IT-säkerhet och detta skulle även fungera i avskräckande syfte för att sänka potentiellt ej legitimt användande. Angående att den regionala organisationen inte hade någon egentlig utbildning är ett intresseväckande resultat, då vi i litteraturen fann att en åtgärdsplan eller planering generellt för en krissituation var meningslös om anställda inte utbildades enligt verksamhetens principer och säkerhetspolicys. Är det i så fall värt att lägga pengar på att försöka planera

inför ett informationssystemhaveri om de anställda ändå inte vet något om det, eller hur haverisituationer skall hanteras? Utbildningen bör vara en väldigt väsentlig del i planeringen, finns det inte ekonomi till att utbilda samtliga kan istället ledarroller prioriteras och sen får de i uppdrag att sprida informationen till övriga anställda och leda samtliga anställda genom krissituationen. Att utbildning behövs är tydligt men hur kan de utbilda anställda utan en för stor resursåtgång?

I den internationella organisationen lägger de stor vikt vid tidigare kunnande, vilket skapar ett beroende till personen och dennes kunnighet. Vidare innebär det inte att en person som arbetar med säkerhet och hanterar sådana ärenden på en daglig basis, lär sig allt eller informeras om allt. En utbildning skulle kunna generera tankar eller metoder som de tidigare förbisett eller helt missat. En IT-säkerhetsplan är aldrig felfri utan måste ständigt utvecklas allteftersom verksamheten samt dess omvärldskrav förändras. För att göra denna typ av revidering bör verksamheten grundligt stegvis metodiskt granskas som beskrivet av Snedaker (2007) och Rittinghouse et al. (2006). I och med att organisationerna och risker ständigt förändras, betyder det inte att anställda alltid hinner med i utvecklingen. Så utbildningar bör därför ses som ett sätt att säkerställa att kunskapen faktiskt finns hos personalen när den behövs. Ett problem som vi ser med att lägga för stort fokus på att anställda lär sig via sitt dagliga arbete och därför inte lägga så stor vikt vid utbildning, är att det kan vara lätt att fastna i ett mönster eller ett perspektiv. Att anställda därmed missar andra bra alternativ då de blivit väldigt låsta i hur det tidigare har hanterats eller att det blir någon form av grupptänk.

5.2 Utveckling och underhåll av åtgärdsplaner

Litteraturen säger att en åtgärdsplan är föråldrad inom ett år och måste revideras, detta är något som stämmer väl överens med hur de olika organisationerna arbetar. Vilket betyder att de är medvetna om de ständigt pågående förändringarna, vilket är klart positivt. Samtidigt menar Rittinghouse et al. (2006) att detta är ett minimikrav. Det kan ha skett stora förändringar på ett halvår och åtgärdsplanen redan kan ha blivit inaktuell. Hur kommer det sig att de intervjuade organisationen gör sin revidering enligt minimikravet? Om det händer många oväntade förändringar under några få månader och åtgärdsplanen inte längre passar, vad händer då om den plötsligt är felaktig när den behövs? På något sätt bör det därför finnas någon granskning tidigare som faktiskt undersöker om den överensstämmer med organisationen. Frågan som vi ställer oss är huruvida detta är en kostnadsfråga eller vad den egentliga bakomliggande orsaken är till att de reviderar enligt minimikravet?

Allt eftersom verksamheten ökar i storlek ökar även dess omfattning av omvärldskrav och dess hotbild. Inom de tre undersökta organisationerna hade de en internt uppfattad hotbild utefter vilken de reviderar organisationen. Hur denna hotbild faktiskt ser ut idag kan IT-säkerhetsexperter inte veta definitivt utan bygger därför sina revideringar på åtagandeprinciper enligt dagens forskning. Allt eftersom verksamheterna förändras, förändras även deras hotbild. Här återkommer lärande i organisationen, för att anställda ska vara

förvissade om dagens föreställda hotbild, verksamhetens policys och liknande spelar utbildningar en essentiell del i anställdas arbete. Detta för att de ska bli förvissade om förändringar som beskrivet av Rittinghouse et al. (2006) och Snedaker (2007) i delkapitel 2.10.

Då vi empiriskt studerade den regionala organisationen såg vi att de inte bedömde ett stort antal risker som överhängande hot, men även att de förlitade sig till stor del på sina informationssystem samt interna revideringar. Även under mötet med en annan anställd på organisationen hade denna inte tillräcklig kännedom i området säkerhet trots att denne varit aktiv inom det området tidigare. Det är viktigt att verksamheter inte slutar arbeta proaktivt, detta gynnas bland annat genom säkerhetslärande i organisationen. Det bör inte ske en gång vid anställning utan gärna i anslutning till verksamhetens årliga revidering. Då skulle systemets användare få djupare inblick i vedertagna åtgärder för IT som gjorts under året samt innebörden av revideringen. Bara genom en välutarbetad reaktionsplan skulle risker för en stor förlust, såsom en potentiell konkurs under ett haveri, reduceras.

Dessvärre saknar en stor del verksamheter en välutarbetad plan och ett flertal anställda blir sysslolösa om ett informationssystemhaveri skulle inträffa. Detta fenomen fanns i den regionala verksamheten, där beroende på vilket system som havererade kunde en del berörda anställda inte göra något förrän problemet var löst. En sådan situation är ett tydligt exempel på var en åtgärdsplanering skulle behövas. Om anställda skickas hem då de blir sysslolösa kan enorma förseningar och förluster uppstå, därför borde organisationen försöka planera för liknande situationer så de kan hanteras effektivare och reducera de negativa konsekvenserna bland IT-beroende organisationer. Denna beskrivning av tillvägagångssätt tydliggjorde för oss varför de procentuella siffrorna gällande konkurs som presenteras av Cummings, et al., (2005) i delkapitel 1.1 var så höga. Om många organisationer hanterar informationssystemhaveri på ett sådant sätt, där anställda skickas hem i väntan på lösning, är dessa siffror inte särskilt förvånande.

Angående de omvärldskrav som ställs på de olika organisationerna spelar det en essentiell roll att verksamheten sporadiskt totalrevideras och granskas för att uppnå högsta möjliga säkerhet. Vidare även att säkerheten underhålls som framhölls i delkapitel 2.10 så att de anställda blir uppdaterade kring vad den nya revideringen innebär för organisationens arbete.

5.3 Riskprioritering

Intressant är att sätta dessa olika organisationer, deras verksamhetsnivå samt säkerhetsprioriteringar i förhållande till varandra. I och med att organisationerna befinner sig på olika nivåer har de olika intressenter i verksamheten och även organisationernas omfattning skiljer sig, därmed exponeras de för olika risker som de måste hantera. I vår undersökning fick organisationerna prioritera olika risker, genom att göra detta förväntade vi oss att se skillnader i vilka risker som de ansåg ha störst konsekvens hos dem och som de

därför prioriterade högst. Till följd gick det att urskilja vilka risker som organisationen sannolikt arbetar mest för att reducera genom olika form av åtgärdsplaner. Det är under denna prioritering som faktorer som, till exempel placering i världen och organisationstyp, har en väsentlig del i utvecklingen(delkapitel 2.1).

Vi förväntade oss att genom denna bedömning se hur en internationell organisation utsätts för fler risker som kan orsaka stora negativa konsekvenser för verksamheten jämfört med en regional organisation som inte är känd utanför Sverige. Våra förväntningar var att den nationella organisationen skulle ha bättre planering än den regionala organisationen, men var osäkra kring hur deras arbete skulle vara i jämförelse med den internationella organisationen. Detta eftersom den nationella organisationens verksamhetstyp för oss antyder om hög prioritering av just säkerhet. Gällande riskestimeringsmatrisen har den intervjuade inte fått uttala sig kring detta i samma utsträckning som övriga intervjupersoner i uppsatsen.

Angående att den internationella organisationen de mänskligt orsakade katastroferna, framförallt Terrorism, cyberterrorism/crackers samt internetattacker, skulle detta mycket kunna bero på att den internationella organisationen har större allmän kännedom, då de även finns i andra länder. Därmed finns en betydligt större omfattning personer som skulle kunna ha intresse i att göra organisationen illa genom just dessa metoder. En ytterligare aspekt till detta är att en så stor organisation hanterar större summor och möjligtvis känslig information, vilket i sig kan vara lockande för vissa personer, exempelvis crackers.

Att den internationella organisationen är placerat på flera platser i världen kan vara en bidragande faktor till att de prioriterat internetattacker högre en den regionala organisationen. Då de har svårare att synkronisera och kommunicera med resterande delar av organisationen som finns utomlands gentemot en regional organisation, som enklare kan kommunicera med hjälp av telefon eller annan kommunikationsform. Detta skulle kunna tyda på att det huvudsakliga problemet som någon av dessa risker egentligen medför, och som organisationen är orolig inför, inte är risken i sig, utan snarare handlar om kommunikation. Kommunikation mellan den internationella organisationens delar är en relevant faktor för att de ska kunna arbeta. Om ett haveri bröt kommunikationen, hur skulle då synkronisering mellan dem ske? Det bör vara betydligt mer komplicerat att lösa kommunikationsproblemet när organisationens delar befinner sig långt ifrån varandra. Vem löser problemet? Hur hanteras kommunikationen under tiden?

En vidare intressant aspekt är att se hur olika positioner inom samma organisation prioriterar risker. Vad som är tänkvärt är hur prioriteringen skiljer sig, detta kan med stor sannolikhet bero på att de har olika fokus inom organisation och att de olika avdelningarna bedömer konsekvenserna av en särskild risk utifrån deras perspektiv. I detta fall går det att koppla det till figur 2.2, där organisatorisk omgivning, IS omgivning samt medvetenhet och kunskap påverkar den uppfattning som finns av risker. Intervjupersonernas uppfattning och bedömning i vår riskmatris baseras på just dessa faktorer. De sitter på olika avdelningar, har olika uppgifter samt kunskap, därmed blir uppfattningen av risker olika. Genom att göra två intervjuer på den regionala organisationen kunde vi urskilja att de tydligt hade vissa olikheter

i sin uppfattning, det var nu på efterhand bra att dessa utfördes då det gav ytterligare ett intressant moment att diskutera. Frågan som vi ställer oss är då hur det ser ut i större organisationerna, fungerar det på samma sätt där?

I en jämförelse av alla dessa riskestimeringsmatriser går det att urskilja att samtliga utom den intervjuade från den inledande intervjun med den regionala organisationen, har uppskattat storm och snöoväder till att ha hög sannolikhet. Detta utstick ifrån övrigas uppskattning är därför intresseväckande, vad i hans medvetenhet och bedömning som skiljer sig gentemot de andras. En möjlig förklaring till detta är att den intervjuade, Hans-Åke, hanterar det tekniska i organisationen och de delarna inte berör hans uppgifter. Det kan också vara ett exempel på underskattning av just dessa risker, som nämndes i delkapitel 2.6.1.

I vår inledande intervju med Svedala kommun, den regionala organisationen, bedömde den intervjuade att internetattacker var den risk med näst högst sannolikhet att inträffa, trots detta har risken inte en av de högre prioriteringarna utan återfinns på plats fem. Intressant är då varför den risken som de bedömer har stor sannolikhet att inträffa inte prioriteras högre, före andra risker med mindre bedömd sannolikhet. Detta fenomen skulle kunna grunda sig i en kostnadsfråga, genom planeringskostnad visavi haverikostnad. Där organisationen möjligen har bedömt att en sådan risk kostar för mycket att planera inför i hopp om att reducera den, gentemot den haverikostnad och konsekvens som det kan få för organisationen.

Riskestimeringsmatrisen som vi fick besvarad under vår inledande intervju med Svedala kommun, regionala organisationen, prioriterades flera risker lika högt då samtliga hade lika fokus. Detta fann vi intressant, även om det låter bra så kan det vara en bristande metod. Om plötsligt två eller fler av risker samtidigt skulle upptäckas i en sårbarhetsbedömning, tolkar vi det som om de vill planera inför och hantera dessa parallellt. Om inte mer personal tillsätts kommer planeringen dröja längre än om de prioriterade en risk före den andra. Vår tolkning av den riskhanteringsprocess, redovisad i delkapitel 2.3, är att det är viktigt att göra en tydlig prioritering där den risk som har störst sannolikhet att inträffa och störst konsekvens för organisation prioriteras först. Därmed borde Svedala kommun istället vidare tydliggöra sin prioritering för ett bättre resultat och tydligare fokus i sitt säkerhetsarbete.

5.4 Största säkerhetshot

Genom låta organisationerna svara på vad det värsta som skulle kunna hända dem, kan vi urskilja hur de tänker i sin riskbedömning, särskilt i sårbarhetsbedömningen, och hur det kan påverka verksamheten. Det värsta som kunde hända den internationella organisationen var en långvarig attack där de förlorade kontakten med moderbolaget. Vad som är intressant gällande är att sätta det i relation till den matris som också besvarades. I den så har en internetattack som kan leda till offlineläge, det vill säga organisation saknar tillgång till internet och kan inte kommunicera med moderbolaget, placerats som nummer fyra i riskprioriteringen. Detta är intressant, om det är en sådan situation som anses ha störst konsekvens och hög sannolikhet,

varför har den då inte prioriteras högre i matrisen?

Vidare tänkvärt gällande deras bedömning av största säkerhetshot är inverkan av deras organisationstyp. Konsekvenserna av det största säkerhetshotet för den regionala organisationen, Svedala kommun, är att flertal verksamheter i ställs utan IT-system. Medan det för det internationella snarare handlar om att deras produktion tillslut helt kan tvingas stanna upp. Vilket betyder att målet med deras riskreducering skiljer sig. För en regional organisation så som en kommun ligger stor fokus med åtgärdsplanering på att hålla samtliga kommunens verksamheter uppe, medan det för en internationell organisation inom näringslivet istället handlar om att inte förlora sin produktivitet och marknadsplacering. Vidare så är fokus i åtgärdsplaneringen för den internationella organisationen att inte förlora sin kommunikation till moderbolaget, varigenom deras arbete sker. För den nationella organisationen handlar de däremot om rikets säkerhet.

5.5 Tekniskt beroende

Som nämnts i uppsatsen inledning och litteraturgenomgång har beroendet av informationssystem ökat, och att problem uppstår om de inte finns tillgängligt. Detta fick vi även bekräftat under vår empiriinsamling, där intervjuade påpekade att arbetet skulle kunna skötas manuellt fast att det skulle bli omständigt. Fler sa även att de har papper som reservplan, men att det inte skulle kunna användas under en längre tid. Situationer där informationssystemen inte finns att tillgå skulle också leda till kraftiga förseningar som måste tas igen på efterhand. Papperskopior finns att tillgå, men vad säger att dessa är uppdaterad till senaste version? De kan vara gamla och därmed inte innehålla fel data, är detta verkligen en bra lösning? Om papperskopiorna kan arbete enligt dem egentligen också ställa till med mer problem utöver de orsakade av haveriet. Om något data inte korrekt och det används under tiden kan en del arbete och beslut ha fattats baserat på felaktiga underlag. Hur försäkrar sig organisationerna att papperskopiorna är korrekta, finns det någon som ansvarar för att hålla dessa uppdaterade?

Enligt litteraturen är det svårt att lyckas eller helt omöjligt att lyckas med en felfri åtgärdsplan första gången. Detta får oss att analysera de faktiska konsekvenserna av en risksituation. Många kan vara negativa men det kan även bidra till en ökad förståelse för den egna organisation och de planeringar samt prioriteringar som de saknar. Därmed kan en katastrof också vara lärande för organisationen, och vad som kan förbättras för att effektivare kunna hantera en liknande situation. Det kan därför ses som indirekttestning av deras planering, som kan leda till revidering av åtgärdsplaneringen och till slut en bättre lösning. Om en plan aldrig testas, aldrig används eller underhålls hur vet organisationen att den i så fall fungerar?

I delkapitel 2.10 påpekas att övning kan bidra till ökad förståelse och medvetenhet bland anställda. Ur ett annat perspektiv bör även en verklig händelse liknande dem som

organisationerna beskriver, med reservkopior i pappersformat, också bidra till just detta. Det tydliggör för anställda det tekniska beroende som finns i organisationen och hur mycket som sköts med hjälp av IT-system. Detta poängterar även den intervjuade under vår kompletterande intervju hos Svedala kommun.

Att arbetet blir försenat och arbetet blir mer komplext att sköta till följd av ett haveri, kan i sig även vara dålig kontroll över organisationens IT och den information som hanteras. Bra alternativ för att förbättra organisationens kontroll finns tillgängliga, vilket även bör minska den negativa konsekvensen av just systemberoende. COBIT och GAIT är två bra exempel på hur en organisation kan öka sin kontroll, resulterande i effektivare riskhantering. Detta genom att följa de steg och moment som lagts fram i delkapitel 2.8.1 och 2.9. Om en organisation analyserar viktiga moment kan de genom att införa kontroll av dessa moment i ett längre perspektiv inför en ökad kontroll av sitt IT. Samtliga intervjupersoner har ansett att det blir besvärligare utan tillgång till informationssystem. Förbättrad kontroll genom någon av dessa metoder kan underlätta arbetet och göra det mindre besvärligt.

5.6 Säkerhetsplan

Extra säkerhetsplaner, i form av säkrad tekniskutrustning, är tydliga exempel på vad som presenterades i delkapitel 2.7 (Forcht, 1994; Martin, 1973; Parker, 1981), de fyra åtgärdsstrategierna: *avskräckande, förebyggande, upptäckande* och *återställning*. Samtliga åtgärder som organisationerna har tagit för att säkert hantera sina informationssystem och sin informationsteknik har baserats på någon av dessa strategier. För att förebygga risker har samtliga organisationer försökt skydda sina servrar ifrån att exempelvis obehöriga ska kunna nå dem. Som beskrivs under den inledande intervjun med den regionala organisationen så har de larm som direkt meddelar om något otillåtet skulle ske. En intresseväckande aspekt är hur internationella organisationen har valt att skydda sin informationsteknik genom att höja den ifrån marken vilket är en förebyggandestrategi mot översvämningar, vilket betyder att de har tagit tekniksäkringen längre än övriga. Vår informant på försvarsmakten säger att de inte tillåter vatten i serverrum och på så vis hanteras eventuell kortslutningsrisken av servrar orsakat av vatten. Detta har troligtvis övriga organisationer som princip också, men vad är det som säger att det inte på något annat vis kommer in vatten i rummet, genom kraftigt regn eller en trasig vattenledning utanför serverrummet?

Vidare så redogör intervjuade på den regionala organisationen, Svedala kommun, att de har olika former av mindre elverk som ska ta vid och hålla de väsentligast och samhällskritiska systemen igång om det skulle inträffa ett långvarigt strömavbrott. I detta fall har organisationen analyserat de informationssystemrisker som finns, och bedömt att strömavbrott är en risk som måste hanteras. För att reducera denna risk har de köpt in några mindre elverk som ska driva de samhällskritiska informationssystemen i organisationen. De har här gjorts en tydlig bedömning och prioritering av vad som inte får sluta fungera. Detta är tydligt exempel på hur organisationen har identifierat en hotbild, gjort en sårbarhetsbedömning samt

konsekvensbedömning och sedan plockat fram en metod för hantera risken(se delkapitel 2.3).

5.7 Avslutande diskussion

Av den information som framlagts av informanterna kan vi urskilja hur organisationer idag använder sig av sina åtgärdsplaner. Ett generellt mönster i organisationerna är att denna åtgärdsplan kan vara uppdelad inom organisationens avdelningar. Det finns inte enbart en övergripande åtgärdsplan som gäller hela organisationen utan det kan också vara mer specifikt genom planeringen på avdelningsnivå. Vår tolkning av denna situation är att planeringen inte alltid delas mellan avdelningarna, utan hålls internt i avdelningarna. Oftast finns det någon form av planering som gäller hela organisationen, exempelvis Svedala kommuns planering för vilka informationssystem som måste prioriteras.

De större organisationerna har någon form avdelning som har god kunskap inom säkerhetsområdet och organisationens åtgärdsplanering. Denna ska hjälpa övriga delar i organisationen att effektivt hantera den situation som kan uppstå vid ett informationssystemhaveri. Metoden skulle kunna ses som en åtgärdsplanering i sig, eftersom det är en reservlösning som ska hjälpa organisationen genom systemhaveriet. Frågan är hur effektiv denna metod är, och om inte anställda förlitar sig mer på dem istället för att själva lära in hur de ska agera vid ett systemhaveri.

I litteraturen lyftes det fram att anställdas engagemang är en väsentlig del i planeringen, och att det effektivast görs genom utbildningar samt kommunikation i organisationen. Intressant gällande detta är att organisationen i praktiken faktiskt har utbildningar i åtgärdsplanering, men egentligen hur mycket får de anställda vara med i utvecklingen i åtgärdsplaneringen? Som tidigare poängteras i studien är det svårt att lyckas med planeringen redan första gången, men för att lyckas med detta bör anställda ifrån samtliga avdelningar på något vis involveras i planeringen. Om samtliga aspekter inte ses över har vi svårt att se att planeringen verkligen lämpas för hela organisationen. Medvetenhet och proaktivitet lyftes fram som en viktig faktor i planeringen. Tänkvärt är då hur medvetenheten kan anses fullständig om inte samtliga delar i en organisation involveras i planeringen. Trots att personen som är ansvarig för utvecklingen av planen har goda kunskaper, betyder inte det att samtliga perspektiv kring en sådan situation är inräknade. Det blir givetvis svårare och mer resurskrävande ju fler individer som är engagerade. Eftersom anställdas involvering anses som en viktig del bör detta ändå beaktas i enlighet med planeringskostnad visavi konsekvenskostnad.

Det framgår att en del organisationer hyr in konsulter som hjälper till med åtgärdsplaneringen och följer särskilda punkter i granskningen, beaktansvärt är hur mycket dessa punkter egentligen involverar och utnyttjar de anställdas medvetenhet och kompetens inom den egna organisationen? Vidare tänkvärt är hur mycket de anställda får ut av en årlig utbildning. Hur mycket lär de sig och hur länge kommer de ihåg det? I litteraturgenomgången (se delkapitel 2.10) framgår det att testning är ett viktigtmoment i åtgärdsplaneringen. Det framhävs att det

är en bra och lärande metod att kontrollera åtgärdsplanen och därmed även engagera organisationens anställda. Däremot har inte detta tydligt framkommit i alla organisationer huruvida testning görs eller hur ofta och till vilken nivå anställda engageras i denna testning. Om utbildningen sker en gång om året, hur blir det då för personer som anställs kort efter utbildningen? Om det bara sker en gång om året kan eventuella nyanställningar få vänta nästan ett helt år på att involveras i åtgärdsplanering, och får då förlita sig på att någon annan vet vad de ska göra vid systemhaveri.

6 Slutsats

Informationssystemhaveri är ett problem som kan vara svårt att planera inför, men ändå väldigt väsentligt att faktiskt planlägga. Detta planeringsarbete är omfattande och resurskrävande, både ekonomiskt och tidsmässigt. Trots den höga resursåtgången kan det ändå vara värt besväret, genom att på så vis säkra organisationens arbete och fortsatta existens.

Uppsatsens forskningsfråga är: *hur använder sig organisationer idag av åtgärdsplaner vid informationssystemhaveri och hur engageras anställda i planeringen?*

Utifrån den information som insamlats är våra slutsatser att organisationer idag använder sig av åtgärdsplaner för systemhaveri på olika nivåer, det kan finnas både organisationsövergripande och mer specificerade. Det är tydligt att denna typ av säkerhet har högre prioritering och är ett större moment i större organisationer jämfört med mindre. Generellt används åtgärdsplaner vid systemhaveri idag för att minimera risker för stora förluster, både ur ett ekonomiskt perspektiv, tidsmässigt och även förhållande till organisationens intressenter. En åtgärdsplan i en organisation är ofta ett försök att effektivt hantera svåra situationer som kan uppstå vid systemhaveri, detta för att i ett längre perspektiv säkerställa organisationernas fortsatta existens. Denna form av åtgärdsplanering används därmed som en reservplan på hur de ska sköta arbetet till systemhaveriet är löst. Åtgärdsplanen är därmed en proaktiv planering som ska underlätta för organisationens anställda att hantera den ovisshet som annars kan uppstå vid ett systemhaveri.

Med utgångspunkt i de organisationer som ingått i den här uppsatsen, består ofta åtgärdsplanen av att anställda tvingas plocka fram säkerhetskopior i pappersformat om det är möjligt eller att processer får skötas manuellt. Det framgår också att organisationer inte nödvändigtvis har en välutarbetad åtgärdsplan för hur de ska hantera systemhaveri. I den regionala organisationen som är den minsta verksamheten i vår uppsats, tydliggörs hur ett systemhaveri kan leda till att anställda istället kan gå hem eller blir sysslolösa om informationssystemen inte fungerar.

Viktigt att påpeka är också att organisationer gör prioriteringar av sina system, där de rangordnas efter vilka som är affärskritiska att vara utan, som en del av åtgärdsplaneringen.

När det gäller de anställdas involvering och engagering i åtgärdsplaneringen så sker detta huvudsakligen genom att anställda informeras under någon form av kortare utbildning, som sker på årligbasis. Denna engagering sker i sig inte under utvecklingen av åtgärdsplanen, utan främst när en plan är utvecklad. Det betyder att anställda snarare engageras i planeringen för

att den utvecklade åtgärdsplanen ska fungera. Orsaken bakom detta är att organisationer ofta har någon eller några ansvariga som tillsammans med konsulter utvecklar åtgärdsplaneringen. Med många anställda involverade i planeringen kan det lätt bli för komplicerat och resurskrävande. Vidare framgår att en del av det säkerhetslärande som gäller åtgärdsplaneringen sker dagligen i de vardagliga sysslorna. Framträdande i litteraturen är att anställdas engagemang är väsentligt, diskuterbart är om det är tillräckligt med endast en utbildning eller om det går att uppnå en förbättrad åtgärdsplanering genom att även involvera anställda i utvecklingen eller om det bidrar till en för hög och okontrollerbar komplexitet.

Den regionala organisationen i uppsatsen har ännu ingen egentlig utbildning för de anställda som gäller säkerhet. Därmed bör tydliggöras att vissa organisationer inte alltid engagerar sina anställda tillräckligt i åtgärdsplaneringen eller någon form av planläggning för att en utvecklad åtgärdsplan ska fungera. Det betyder att hur en åtgärdsplan används och hur anställda engageras ofta grundas på de resurser som finns i organisationen, men även organisationstyp och medvetenhet.

En del av organisationers åtgärdsplan är att försöka reducera riskerna som kan leda till systemhaveri. Detta görs både i informationssystemen och fysiskt; genom att kontrollera in- och ut-trafik från servrarna, genom att låsa dörrar och hindra obehöriga ifrån att komma åt informationsteknik samt affärskritisk information. På så vis är även riskreducering en väsentlig del i åtgärdsplanen, att reducera risken för att det ska kunna hända eller ske igen. En åtgärdsplan används i och med detta för att underlätta arbetet vid systemhaveri men även för att reducera riskerna för systemhaveri.

Om ett systemhaveri inträffar är tanken med en åtgärdsplan att anställda genom tidigare informering ska veta exempelvis hur de bör agera, hur de ska kommunicera med varandra och vem som de ska rapportera till om de vanliga rutinerna hindras. De ska då minnas det som de har lärt sig på utbildningarna gällande åtgärdsplanering, för att sedan kunna agera på ett korrekt vis som i ett längre perspektiv effektivt ska leda organisationen genom systemhaveriet. Denna information får de på utbildningar som i åtminstone större organisationer sker årligen. Utan en åtgärdsplan kan anställda bli osäkra på hur de ska agera och hur de ska sköta sitt arbete om nödvändiga informationssystem inte finns. På så vis talar en åtgärdsplan om vilka metoder som de anställda ska ta till och ovisshet uppstår inte i organisationen. Kan de anställda utföra en del av sina arbetsuppgifter trots ett systemhaveri blir det heller inte lika mycket för organisationen att ta igen efter att haveriet är löst.

Vidare så har de större organisationerna en särskild avdelning som ska ha god kunskap gällande åtgärdsplanen och därför ska kunna hjälpa de anställda genom systemhaveriet om det skulle behövas. Detta för att berört arbete i organisationen inte helt ska stanna upp eller kommunikation internt ska brytas.

Bilagor

Bilaga 1 – Intervjuguide till regional och internationell organisation

Nivå 1: Informanten

1. Vill du att organisation ska förbli anonym i uppsatsen?
2. Vill du som intervjuad vara anonym?

Namn på den intervjuade:
Position på organisationen:
Namn på intervjuare:
Datum/tid för intervju:
Intervjutid:

3. Vad har du för roll i organisationen idag?
    a. Vad innefattar dina arbetsuppgifter?
4. Hur länge har du haft den här positionen?
5. Vem rapporterar du till?

Nivå 2: Organisationen

1. Vad är dina tankar om din organisation?
2. Finns det någon märkbar/särskild kultur och karaktär i organisationen?
    a. Om ja, beskriv den kortfattat?
3. Hur anser du att det är att arbeta i organisationen, utifrån din position?
4. Finns det en särskild värdegrund i organisationen, i så fall vad?
5. Ur ditt perspektiv, vad är syftet och drivkraften bakom organisationen?
6. Hur arbetar ni för att vara konkurrenskraftiga?

Nivå 3: Scenarier

1. Hur skulle du agera under följande scenarier?

Scenario 1

Åskväder och kraftig blåst har slagit ut strömmen i ert kvarter. Efter ett samtal till ansvariga för er elförsörjning får ni höra att stormen har orsakat problem hos dem. Elledningarna som leder till er organisation har på något vis brutits och att det krävs ett omfattande arbete för att identifiera problemet, de jobbar så snabbt de kan men en lösning på problemet kan dröja. Till följd av detta står ni utan ström och tillgång till de system som ni dagligen använder.

2. Vad skulle detta kunna leda till?
    a. Finansiella förluster, förlorad arbetstid, förlorade kunder?
3. Hur arbetar ni idag för att reducera riskerna detta scenario skulle medföra, och vilka är dessa risker?

4. Hur hanterar ni en sådan situation?
5. Hur arbetar ni för att tillhandahålla en effektiv lösning?
6. Hur länge skulle organisationen kunna fortgå utan tillgång till Informations Teknik (IT)?

Scenario 2

Vatten har börjat läcka in i era lokaler till följd en trasig vattenledning, anledningen bakom vattenledningens skada är vid tillfället okänd. Vattnet når er server, vilket orsakar en kortslutning och mörklägger hela lokalen. Vattnet måste stängas av och ledningarna måste lagas. Mycket vatten har hunnit läcka in och det kan ta tid att få hjälp med att laga ledningen och få ut allt vatten, men även att få igång alla system igen.

7. Vad skulle detta kunna leda till?
    a. Finansiella förluster, förlorad arbetstid, förlorade kunder?
8. Hur arbetar ni idag för att reducera riskerna detta scenario skulle medföra, och vilka är dessa risker?
9. Hur hanterar ni en sådan situation?
10. Hur arbetar ni för att tillhandahålla en effektiv lösning?

Scenario 3

En individ med ond uppsåt vill organisationen illa och försöker sabotera dess verksamhet. I hopp om att organisationens arbete ska lida skada, saboterar individen alla IT-system som är verksamhetskritiska samt den tekniska utrustning som finns i serverhallen. Detta orsakar svårigheter att använda dessa system, systemen kraschar när det startar upp och det finns ingen möjlighet att komma åt data som behövs för verksamhetens arbete. Personen lyckades sabotera tekniken kraftigt och det kan ta tid att reparera.

11. Vad skulle detta kunna leda till?
    a. Finansiella förluster, förlorad arbetstid, förlorade kunder?
12. Hur arbetar ni idag för att reducera riskerna detta scenario skulle medföra, och vilka är dessa risker?
13. Hur hanterar ni en sådan situation?
14. Hur arbetar ni för att tillhandahålla en effektiv lösning?
15. Hur fungerar samarbetet mellan säkerhetsavdelningen och Human Resource avdelningen?

Nivå 4: Kompletterande frågor:

1. Hur går er process till för att utveckla en systemsäkerhetsplan/åtgärdsplan och inom vilka intervaller revideras denna?
2. På vilket sätt engageras de anställda i systemsäkerhetsplan/åtgärdsplan och dess utveckling?
3. Hur arbetar ni internt med säkerhetslärande och sker detta arbete på samtliga nivåer i organisationen?
    b. Om ja, inom vilka intervall sker denna utbildning?
4. Hur bedömer du att katastrofhotbilden för organisationen ser ut? Interna/Externa hot?
5. Vad är det värsta som skulle kunna hända hos er ur ett systemhaveri perspektiv?
    a. Vilka konsekvenser skulle det få för verksamheten?
6. Vilka risker har ni i er organisation prioriterat högst och arbetat mest med att reducera?
7. Hur bedömer du att säkerheten är ”tillräcklig”?
    a. Vilka kriterier använder du/ni i denna bedömning?
8. Står ledningen bakom dig om du föreslår förbättringar i säkerhetsarbetet?
9. Har motiverade säkerhetsförbättringar acceptans i ledningen och i organisationen?

Riskkategori	Risktyp	Beskrivning	Uppskattad sannolikhet (1-5)	Prioritering (1-10)	N/A Icke relevant
Naturkatastrof	Jordbävning, vulkanutbrott, tsunami	Skadad utrustning			
Naturkatastrof	Storm	Strömavbrott, översvämning			
Naturkatastrof	Snöoväder	Hög belastning av verksamhetens infrastruktur			
Mänskligt orsakade katastrofer	Terrorism	Explosion			
Mänskligt orsakade katastrofer	Cyberterrorism, Crackers	Dataskadegörelse			
Mänskligt orsakade katastrofer	Internetattack	Systemet överbelastas, offlineläge			
Mänskligt orsakade katastrofer	Sabotage	Dataförlust			
Mänskligt orsakade katastrofer	Social engineering, Hackers	Dataintrång			
Oavsiktliga eller tekniska katastrofer	Felanvändning	Ogiltig data			
Oavsiktliga eller tekniska katastrofer	Tekniskt konstruktionsfel	Systemhaveri			

10. Känner du till någon incident (systemhaveri) som har hänt på organisationen under de senaste 5 åren?
    a. Och i så fall hur hanterades det haveriet?
    b. Information om haveriet, vad orsakade haveriet och hur upptäcktes det?

Bilaga 2 – intervjuguide till nationell organisation (Försvarsmakten)

Nivå 1: Informanten

1. Vill du att organisation ska förbli anonym i uppsatsen?
2. Vill du som intervjuad vara anonym?

Om svaret på fråga 1 och/eller 2 är Ja, gå vidare till Nivå 2.

Namn på den intervjuade:
Namn på organisation:
Position på organisationen:
Datum/tid för intervju:
Intervjutid:

3. Vad har du för roll i organisationen idag?
    a. Vad innefattar dina arbetsuppgifter?
4. Hur länge har du haft den här positionen?
5. Vem rapporterar du till?

Nivå 2: Organisationen

1. Finns det någon märkbar/särskild kultur och karaktär i organisationen?
    b. Om ja, beskriv den kortfattat?
2. Hur anser du att det är att arbeta i organisationen, utifrån din position?
3. Finns det en särskild värdegrund i organisationen, i så fall vad?
4. Ur ditt perspektiv, vad är syftet och drivkraften bakom organisationen?
5. Hur arbetar ni för att vara konkurrenskraftiga?

Nivå 3: Scenarier

1. Hur skulle du agera under följande scenarier?

Scenario 1: Långvarigt e-posthaveri

En bugg i e-postsystemet har orsakat ett haveri av hela mejlsystemet. Ni ställs nu utan tillgång till systemet i ert vardagliga arbete. Det går inte att starta systemet vilket betyder att ni inte heller kan se tidigare e-post som har skickats till ert konto. En felsökning måste göras av systemet, för att identifiera buggen. I samband med arbetet upptäcker ansvariga att det finns flera brister som också måste åtgärdas för att fler haveri inte ska kunna ske i framtiden. Detta betyder att organisationen inte kommer ha tillgång till sitt e-postsystem förrän alla problem är lösta, vilket kan dröja.

2. Vad skulle detta kunna leda till?
    b. Finansiella förluster, förlorad arbetstid, förlorade kunder?
3. Hur arbetar ni idag för att reducera riskerna detta scenario skulle medföra, och vilka är dessa risker?
4. Hur hanterar ni en sådan situation?
5. Hur arbetar ni för att tillhandahålla en effektiv lösning?
6. Hur länge skulle organisationen kunna fortgå utan tillgång till Informations Teknik (IT)?

Scenario 2: Hemside-haveri i känsligt rekryteringstillfälle

En attack sker mot Försvarsmaktens hemsida, vilket leder till att hemsidan havererar och inte kan användas. Haveriet sker i samband med ett för försvarsmakten stort rekryteringstillfälle, som följd kan organisationen inte nå ut med information om rekryteringen till allmänheten via sin hemsida. Ansvariga jobbar med att få upp hemsidan och hindra en liknande attack från att inträffa igen. Därmed kan det dröja innan hemsidan finns uppe igen.

7. Vad skulle detta kunna leda till?
    b. Finansiella förluster, förlorad arbetstid, förlorade kunder?
8. Hur arbetar ni idag för att reducera riskerna detta scenario skulle medföra, och vilka är dessa risker?
9. Hur hanterar ni en sådan situation?
10. Hur arbetar ni för att tillhandahålla en effektiv lösning?

Scenario 3: Hemside-haveri vid mediedrev mot Försvarsmakten

En skandal har uppdagats inom Försvarsmakten och organisationen har därför hög fokus inom media. I samband med denna skandal uppstår en vattenläcka som kortsluter organisationens webbserver, vilket leder till Försvarsmaktens hemsida havererar. Organisationen har därmed ingen möjlighet att använda sig av sin hemsida för att informera allmänheten om situationen. Att lös problemet är svårare än vad ansvariga trodde och en lösning dröjer.

11. Vad skulle detta kunna leda till?
    c. Finansiella förluster, förlorad arbetstid, förlorade kunder?
12. Hur arbetar ni idag för att reducera riskerna detta scenario skulle medföra, och vilka är dessa risker?
13. Hur hanterar ni en sådan situation?
14. Hur arbetar ni för att tillhandahålla en effektiv lösning?

Nivå 4: Kompletterande frågor:

1. Hur går er process till för att utveckla en systemsäkerhetsplan/åtgärdsplan och inom vilka intervaller revideras denna?
2. På vilket sätt engageras de anställda i systemsäkerhetsplan/åtgärdsplan och dess utveckling?
3. Hur arbetar ni internt med säkerhetslärande och sker detta arbete på samtliga nivåer i organisationen?
    d. Om ja, inom vilka intervall sker denna utbildning?
4. Hur bedömer du att katastrofhotbilden för organisationen ser ut? Interna/Externa hot?
5. Vad är det värsta som skulle kunna hända hos er ur ett systemhaveri perspektiv?
    b. Vilka konsekvenser skulle det få för verksamheten?
6. Vilka risker har ni i er organisation prioriterat högst och arbetat mest med att reducera?
7. Hur bedömer du att säkerheten är ”tillräcklig”?
    b. Vilka kriterier använder du/ni i denna bedömning?
8. Står ledningen bakom dig om du föreslår förbättringar i säkerhetsarbetet?
9. Har motiverade säkerhetsförbättringar acceptans i ledningen och i organisationen?
10. Hur fungerar samarbetet mellan säkerhetsavdelningen och Human Resource avdelningen?
11. Känner du till någon incident (systemhaveri) som har hänt på organisationen under de senaste 5 åren?
    c. Och i så fall hur hanterades det haveriet?
    d. Information om haveriet, vad orsakade haveriet och hur upptäcktes det?

Anvisningar för tabell nedan:

- **Sannolikhet**: 1 = låg sannolikhet, 5 = hög sannolikhet
- **Prioritering**: 1 = högsta prioritering, 10 = lägsta prioritering (varje siffra kan bara förekomma en gång)

Hur prioriterar ni i er organisation följande risker:

Riskkategori	Risktyp	Beskrivning	Uppskattad sannolikhet (1-5)	Prioritering (1-10)	N/A Icke relevant
Naturkatastrof	Jordbävning, vulkanutbrott, tsunami	Skadad utrustning			
Naturkatastrof	Storm	Strömavbrott, översvämning			
Naturkatastrof	Snöoväder	Hög belastning av verksamhetens infrastruktur			
Mänskligt orsakade katastrofer	Terrorism	Explosion			
Mänskligt orsakade katastrofer	Cyberterrorism, Crackers	Dataskadegörelse			
Mänskligt orsakade katastrofer	Internetattack	Systemet överbelastas, offlineläge			
Mänskligt orsakade katastrofer	Sabotage	Dataförlust			
Mänskligt orsakade katastrofer	Social engineering, Hackers	Dataintrång			
Oavsiktliga eller tekniska katastrofer	Felanvändning	Ogiltig data			
Oavsiktliga eller tekniska katastrofer	Tekniskt konstruktionsfel	Systemhaveri			

Bilaga 3 – Svar från nationell organisation (försvarsmakten)

Intervju

Nivå 1: Informanten

1. Vill du att organisation ska förbli anonym i uppsatsen?
2. Vill du som intervjuad vara anonym? JA

Om svaret på fråga 1 och/eller 2 är Ja, gå vidare till Nivå 2.

Namn på den intervjuade:
Namn på organisation:
Position på organisationen:
Datum/tid för intervju:
Intervjutid:

3. Vad har du för roll i organisationen idag?
    b. Vad innefattar dina arbetsuppgifter?
4. Hur länge har du haft den här positionen?
5. Vem rapporterar du till?

Nivå 2: Organisationen

6. Finns det någon märkbar/särskild kultur och karaktär i organisationen?
    c. Om ja, beskriv den kortfattat? Långvarig tradition av hög säkerhetsmedvetenhet
7. Hur anser du att det är att arbeta i organisationen, utifrån din position? OK
8. Finns det en särskild värdegrund i organisationen, i så fall vad? Värdegrunden omfattar människors förhållningssätt gentemot varandra. Stödordet är ÖRA som står för öppenhet, respekt och ansvar
9. Ur ditt perspektiv, vad är syftet och drivkraften bakom organisationen? Organisationen har en tydlig uppgift när det gäller Sveriges säkerhet
10. Hur arbetar ni för att vara konkurrenskraftiga? N/A

Nivå 3: Scenarier

1. Hur skulle du agera under följande scenarier?

Scenario 1: Långvarigt e-posthaveri

En bugg i e-postsystemet har orsakat ett haveri av hela mejlsystemet. Ni ställs nu utan tillgång till systemet i ert vardagliga arbete. Det går inte att starta systemet vilket betyder att ni inte heller kan se tidigare e-post som har skickats till ert konto. En felsökning måste göras av systemet, för att identifiera buggen. I samband med arbetet upptäcker ansvariga att det finns flera brister som också måste åtgärdas för att fler haveri inte ska kunna ske i framtiden. Detta betyder att organisationen inte kommer ha tillgång till sitt e-postsystem förrän alla problem är lösta, vilket kan dröja.

2. Vad skulle detta kunna leda till?

   c. Finansiella förluster, förlorad arbetstid, förlorade kunder? S: Framförallt förlorad tid men som myndighet skulle det också bli svårt att uppfylla offentlighetens krav
3. Hur arbetar ni idag för att reducera riskerna detta scenario skulle medföra, och vilka är dessa risker? S:<Risken är att inte kunna kommunicera
4. Hur hanterar ni en sådan situation? S: Alternativa sambandsvägar och redundanta system
5. Hur arbetar ni för att tillhandahålla en effektiv lösning? S: Se 4.
6. Hur länge skulle organisationen kunna fortgå utan tillgång till Informations Teknik (IT)? S: Inte länge alls

Scenario 2: Hemside-haveri i känsligt rekryteringstillfälle

En attack sker mot Försvarsmaktens hemsida, vilket leder till att hemsidan havererar och inte kan användas. Haveriet sker i samband med ett för försvarsmakten stort rekryteringstillfälle, som följd kan organisationen inte nå ut med information om rekryteringen till allmänheten via sin hemsida. Ansvariga jobbar med att få upp hemsidan och hindra en liknande attack från att inträffa igen. Därmed kan det dröja innan hemsidan finns uppe igen.

7. Vad skulle detta kunna leda till?
   c. Finansiella förluster, förlorad arbetstid, förlorade kunder? S: Förlorat eller åtminstone naggat förtroende
8. Hur arbetar ni idag för att reducera riskerna detta scenario skulle medföra, och vilka är dessa risker? S: Se 5. Risken är att intressent inte får den information han/hon önskar
9. Hur hanterar ni en sådan situation? S: Redundanta system
10. Hur arbetar ni för att tillhandahålla en effektiv lösning? S: N/A

Scenario 3: Hemside-haveri vid mediedrev mot Försvarsmakten

En skandal har uppdagats inom Försvarsmakten och organisationen har därför hög fokus inom media. I samband med denna skandal uppstår en vattenläcka som kortsluter organisationens webbserver, vilket leder till Försvarsmaktens hemsida havererar. Organisationen har därmed ingen möjlighet att använda sig av sin hemsida för att informera allmänheten om situationen. Att lös problemet är svårare än vad ansvariga trodde och en lösning dröjer.

11. Vad skulle detta kunna leda till?
   e. Finansiella förluster, förlorad arbetstid, förlorade kunder? S: Fråga 11a anses inte vara relevant till verksamheten
12. Hur arbetar ni idag för att reducera riskerna detta scenario skulle medföra, och vilka är dessa risker? S: Mediedrev hanteras med information och saklighet. Skada på serverhall hanteras med att vatten inte är tillåtet i serverrum
13. Hur hanterar ni en sådan situation? S: Vet inte säkert. Ev kalla till presskonferens
14. Hur arbetar ni för att tillhandahålla en effektiv lösning? S: Kontinuerliga kontroller och godkännande före drift

Nivå 4: Kompletterande frågor:

1. Hur går er process till för att utveckla en systemsäkerhetsplan/åtgärdsplan och inom vilka intervaller revideras denna? S: Fastställd ordning med kravsammanställning, riskanalys/värdering samt beslut om åtgärder. Revidering sker grundat på skyddsvärdet på den information som hanteras

2. På vilket sätt engageras de anställda i systemsäkerhetsplan/åtgärdsplan och dess utveckling? S: Information och utbildning. Utbildning via ADL och regelbunden information om risker.

3. Hur arbetar ni internt med säkerhetslärande och sker detta arbete på samtliga nivåer i organisationen? S: Genom kurser på självstudienivå
    f. Om ja, inom vilka intervall sker denna utbildning? S: Minst en gång årligen

4. Hur bedömer du att katastrofhotbilden för organisationen ser ut? Interna/Externa hot? – S: N/A
5. Vad är det värsta som skulle kunna hända hos er ur ett systemhaveri perspektiv?
    c. Vilka konsekvenser skulle det få för verksamheten? S: Någon kan komma till skada

6. Vilka risker har ni i er organisation prioriterat högst och arbetat mest med att reducera? S: Risker som kan drabba personer

7. Hur bedömer du att säkerheten är ”tillräcklig”? S: Checklistor, tester och lång erfarenhet. Säkerheten är aldrig 100%. Förändringar i regelverk, organisation, arbetssätt och teknik ligger till grund för kontinuerlig riskhantering. Nationella och internationella standarder och best practices samt nationellt fastställda normer är några av värdekriterierna.
    c. Vilka kriterier använder du/ni i denna bedömning? S: Fastställda normer

8. Står ledningen bakom dig om du föreslår förbättringar i säkerhetsarbetet? S: Mestadels

9. Har motiverade säkerhetsförbättringar acceptans i ledningen och i organisationen? S: Mestadels
10. Hur fungerar samarbetet mellan säkerhetsavdelningen och Human Resource avdelningen? S: Vet ej
11. Känner du till någon incident (systemhaveri) som har hänt på organisationen under de senaste 5 åren? S: Vet ej
    e. Och i så fall hur hanterades det haveriet?
    f. Information om haveriet, vad orsakade haveriet och hur upptäcktes det?

Anvisningar för tabell nedan:

- **Sannolikhet**: 1 = låg sannolikhet, 5 = hög sannolikhet
- **Prioritering**: 1 = högsta prioritering, 10 = lägsta prioritering (varje siffra kan bara förekomma en gång)

Hur prioriterar ni i er organisation följande risker: Får inte ange alla värden

Riskkategori	Risktyp	Beskrivning	Uppskattad sannolikhet (1-5)	Prioritering (1-10)	N/A Icke relevant
Naturkatastrof	Jordbävning, vulkanutbrott, tsunami	Skadad utrustning			N/A
Naturkatastrof	Storm	Strömavbrott, översvämning	4		
Naturkatastrof	Snöoväder	Hög belastning av verksamhetens infrastruktur	4		
Mänskligt orsakade katastrofer	Terrorism	Explosion	--------	--------	--------
Mänskligt orsakade katastrofer	Cyberterrorism, Crackers	Dataskadegörelse	--------	---------	----------
Mänskligt orsakade katastrofer	Internetattack	Systemet överbelastas, offlineläge	----------	----------	----------
Mänskligt orsakade katastrofer	Sabotage	Dataförlust	1		
Mänskligt orsakade katastrofer	Social engineering, Hackers	Dataintrång	---------	--------	---------
Oavsiktliga eller tekniska katastrofer	Felanvändning	Ogiltig data	4		
Oavsiktliga eller tekniska katastrofer	Tekniskt konstruktionsfel	Systemhaveri	1		

Bilaga 4 – Transkribering internationell organisation

Intervju

Nivå 1: Informanten

1. Vill du att organisation ska förbli anonym i uppsatsen? Ja, logistikchefen önskar att vara totalt anonym.
2. Vill du som intervjuad vara anonym? Ja, logistikchefen önskar att vara totalt anonym.

Namn på den intervjuade: ”Logistikchefen”.
Position på organisationen: Logistikchef.
Namn på intervjuare: Lars Lindvall.
Datum/tid för intervju: 25 April 2011.
Intervjutid: 12.00 – 13.40.

Sedan 9/11 har säkerheten blivit förändrad globalt till en allt mer amerikaniserad, såväl som inom tull om industri och IT-säkerhet, vilket idag krävs från den internationella verksamhetens kunder.

3. Vad har du för roll i organisationen idag?
    a. Vad innefattar dina arbetsuppgifter?

    Logistikchefens arbete är stationerat på produktionsenheten i Sverige. Logistikchefen har hand om allt inom logistik så som ankommande och avgående gods.

4. Hur länge har du haft den här positionen?
   Logistikchefen har formellt arbetat i denna position i ca. 15 år men har tidigare arbetat på ett annat sätt då deras struktur och arbete ständigt förändras för att öka deras konkurrenskraft och effektivitet. Tidigare hade Logistikchefen även hand om IT för Sverigekontoret.

5. Vem rapporterar du till?
   Logistikchefen rapporterar till Produktionschefen

Nivå 2: Organisationen

7. Vad är dina tankar om din organisation?
   Sverigekontoret är en liten viktig och extremt effektiv del till det stora moderbolaget som är stationerat i utomlands. Sverigekontoret har hälften av sin verksamhet outsourcad vilken främst är lagersidan i verksamheten.

8. Finns det någon märkbar/särskild Kultur och karaktär i organisationen?
   Internationell kultur med vissa utländska inslag. Sverigekontoret startades i mitten av 1900-talet av ett utländskt företag.

9. Hur anser du att det är att arbeta i organisationen, utifrån din position?
   Logistikchefen anser att arbetet fungerar mycket väl och denne har varit aktiv i organisationen sedan 1974, med vissa pauser för studier samt lumpen.

10. Finns det en särskild värdegrund i organisationen, i så fall vad?
    Logistikchefen menar att verksamheten jobbar starkt som ett team vilket genomsyrar hela deras arbete. God team anda är en stark faktor till organisationens framgångar.

11. Ur ditt perspektiv, vad är syftet och drivkraften bakom organisationen?
    Enligt logistikchefen arbetar verksamheten med att producera en god råvara, med marknadsledning på specialstärkelser för tillverkning och paketering utav livsmedelsprodukter till mycket konkurrenskraftiga priser.

    ”Vi är duktiga på att producera exklusivare råvaror i små serier, snabbt till en mycket god kvalitet. Vi har därför en mycket stor efterfrågan på våran produkt.”

12. Hur arbetar ni för att vara konkurrenskraftiga?
    Logistikchefen menar att de arbetar så nära kunden som möjligt och har även egen personal såsom tekniker ute hos kunderna. Organisationen har stora kunder i Sverige; i Asien med nudelföretag; såväl som bagerier och tillverkning av krämer. I USA levereras mycket till köttindustrin, snabbmat och micromat. Men även till kunder som tillverkar ”fejk”-ketchup samt majonnäs.

Nivå 3: Scenarier

1. Hur skulle du agera under följande scenarier?
   Kontakta myndigheter, så man får en uppdaterad katastrofbild. Nästa steg blir att kontakta moderbolaget. Sedan koppla upp sig till moderbolagets datorpark utomlands genom en extern plats, med hjälp av sin interna samt externa backup.

Scenario 1

Åskväder och kraftig blåst har slagit ut strömmen i ert kvarter. Efter ett samtal till ansvariga för er elförsörjning får ni höra att stormen har orsakat problem hos dem. Elledningarna som leder till er organisation har på något vis brutits och att det krävs ett omfattande arbete för att identifiera problemet, de jobbar så snabbt de kan men en lösning på problemet kan dröja. Till följd av detta står ni utan ström och tillgång till de system som ni dagligen använder.

2. Vad skulle detta kunna leda till? (Finansiella förluster, förlorad arbetstid, förlorade kunder?)
   Reservelverk finns men om även de slutade fungera skulle hela produktiviteten och arbetsproceduren slås ut. Logistikchefen menar att de kan arbeta manuellt men detta skulle medföra en mycket stor arbetsbelastning och komplexitet i arbetet. Sverigekontoret skulle vara beroende av att jobba på en extern plats. Kortsiktigt skulle en katastrof innebära förseningar men långsiktigt skulle detta innebära stationera om på en extern plats. Detta skulle annars medföra att kunder och offerter skulle gå förlorade.
3. Hur arbetar ni idag för att reducera riskerna detta scenario skulle medföra, och vilka är dessa risker?
   Logistikchefen menar att de idag arbetar för att reducera risker genom serverbackup samt dubbla, speglade hårddiskar för den mest vitala informationen på verksamhetens persondatorer. Flera utav säkerhetsfunktionerna i verksamheten är idag outsourcade.

4. Hur hanterar ni en sådan situation?
   a. Hur arbetar ni för att tillhandahålla en effektiv lösning?

   SE 1:AN. Kontakta myndigheter, så man får en uppdaterad katastrofbild. Nästa steg blir att kontakta moderbolaget. Sedan koppla upp sig till moderbolagets datorpark utomlands genom en extern plats, med hjälp av sin interna samt externa backup.

5. Hur länge skulle organisationen kunna fortgå utan tillgång till Informations Teknik (IT)?
   Manuellt arbete skulle öka arbetsbördan stort i verksamheten och detta skulle därför medföra att verksamheten skulle därför lida stora förluster såväl genom förseningar samt bortafall av kunder, detta innebär att verksamheten inte skulle kunna arbeta på samma vis under en längre period.

Scenario 2

Vatten har börjat läcka in i era lokaler till följd en trasig vattenledning, anledningen bakom vattenledningens skada är vid tillfället okänd. Vattnet når er server, vilket orsakar en kortslutning och mörklägger hela lokalen. Vattnet måste stängas av och ledningarna måste lagas. Mycket vatten har hunnit läcka in och det kan ta tid att få hjälp med att laga ledningen och få ut allt vatten, men även att få igång alla system igen.

6. Vad skulle detta kunna leda till? (Finansiella förluster, förlorad arbetstid, förlorade kunder?)
   Fabriken skulle tvingas stänga ner, detta skulle innebära produktionsförluster samt förseningar snarare än kundförluster, då verksamhetens kunder är mycket lojala. Sverigekontoret har varit med om detta tidigare fast genom regnvatten som trängt upp ur källarens (där servrarna då befann sig) brunnar. Därför står idag den tekniska utrustningen på betongfundament och backventilen och liknande i golvbrunnarna är tillsatta för att detta inte ska ske igen.

7. Hur arbetar ni idag för att reducera riskerna detta scenario skulle medföra, och vilka är dessa risker?
   SE 7AN. Fabriken skulle tvingas stänga ner, detta skulle innebära produktionsförluster samt förseningar snarare än kundförluster, då verksamhetens kunder är mycket lojala. Sverigekontoret har varit med om detta tidigare fast genom regnvatten som trängt upp ur källarens (där servrarna då befann sig) brunnar. Därför står idag den tekniska utrustningen på betongfundament och backventilen och liknande i golvbrunnarna är tillsatta för att detta inte ska ske igen.

8. Hur hanterar ni en sådan situation?
   b. Hur arbetar ni för att tillhandahålla en effektiv lösning?

   Tidigare gick en sub-server sönder pga. ett rör på en toalett, idag är tekniken säkrare placerad genom att dessa är högt placerade. Sverigekontoret arbetar även proaktivt och försöker förebygga problem genom att i ett tidigt skede meddela moderbolaget om dessa eventuella risker som upptäcks.

Scenario 3

En individ med ond uppsåt vill organisationen illa och försöker sabotera dess verksamhet. I hopp om att organisationens arbete ska lida skada, saboterar individen alla IT-system som är verksamhetskritiska samt den tekniska utrustning som finns i serverhallen. Detta orsakar svårigheter att använda dessa system, systemen kraschar när det startar upp och det finns ingen möjlighet att komma åt data som behövs för verksamhetens arbete. Personen lyckades sabotera tekniken kraftigt och det kan ta tid att reparera.

9. Vad skulle detta kunna leda till? (Finansiella förluster, förlorad arbetstid, förlorade kunder?)
   Anläggningen skulle stanna upp. Detta skulle återställas genom lokala backuper och externa backuper hos moderbolaget. Systemet skulle få återställas för att förhoppningsvis avlägsna problemet. Denna externa backup styrs via program som arbetar mot moderbolagets SAP utomlands, så de styr om sin trafik och ändrar serverplats till moderbolagets.

10. Hur arbetar ni idag för att reducera riskerna detta scenario skulle medföra, och vilka är dessa risker?
    Verksamheten har idag inget trådlöst nätverk för att undvika intrång. Att de endast har kabeltrafik innebär att intrång görs mycket svårare. De använder sig även av McAfee för att

motverka spam och liknande på persondatorerna. Systemet övervakas av fysiska personer dygnet runt som hela tiden studerar serverstatistik och liknande.

Den största risk för verksamheten skulle vara då kopplingen till moderbolaget skulle försvinna samtidigt som en attack mot Sverigekontoret skulle äga rum. Affärsdatasystemet skulle först slås ut och därefter de andra systemen i följd, skulle attacken fortgå skulle även verksamhetens produktion slås ut.

11. Hur hanterar ni en sådan situation?
    c. Hur arbetar ni för att tillhandahålla en effektiv lösning?

    De arbetar som tidigare nämnt proaktivt genom att ända PM till moderbolaget då riskområden upptäcks. Arbetet görs genom revisioner av IT-säkerheten vart femte år såväl som genom Sverigekontorets egna IT-säkerhetskontor, samt nya krav från kunder och omgivning.

12. Hur fungerar samarbetet mellan säkerhetsavdelningen och H/R avdelningen?
    Sverigekontoret har idag ett mycket nära samarbete med sitt säkerhetsbolag samt moderbolaget som sporadiskt skickar ut säkerhetsrevisioner samt diagnostiserar verksamhetens potentiella riskområden. Moderbolaget har även ett tänk kring ”vem ska ha tillgång till vad?” De bedömer hela tiden vem som ska ha tillgång till vad, ibland försvinner och ibland får individer rättigheter i systemet. Det är då viktigt att meddela huvudkontoret fall säkerheten blir för stark vilket kan även ha en negativ inverkan på den berörda anställdes arbete.

Nivå 4: Kompletterande frågor:

1. Hur går er process till för att utveckla en åtgärdsplan och inom vilka intervaller revideras denna?
   Detta sker internt i Sverigekontoret såväl som externt från deras moderbolag via inhyrda konsulter som totalreviderar verksamheten under femårsintervaller.
2. På vilket sätt engageras de anställda i åtgärdsplanen och dess utveckling?
   De arbetar ständigt genom ett proaktivt arbetssätt och stark kommunikation med moderbolaget där synpunkter framförs.

   ”Det är viktigt att inte motverka användbarhet genom säkerhetsåtgärder.”

   Ibland är anställda mer förvånade kring hur mycket de i själva verket har möjlighet att se, ofta upptäcks fel i systemet av Logistikavdelningen som har större IT kunskaper än de övriga i verksamheten. Detta är fallet på grund utav deras användning av olika IT system.
3. Hur arbetar ni internt med säkerhetslärande och sker detta arbete på samtliga nivåer i organisationen?
   - Om ja, inom vilka intervall sker denna utbildning?

     Organisationen har idag vissa IT-säkerhetsutbildningar men vill inte ge anställda för stor kännedom angående säkerhetsbrister innan dessa är åtgärdade. Endast omvärldens ständiga föränderliga krav som medförs genom lagar, regler, kundkrav samt kvalitetssäkringar, ISO, AEB, AEO och liknande.

4. Hur bedömer du att katastrofhotbilden för organisationen ser ut? (Interna/Externa hot?)
   Logistikchefens kunder kräver verksamheten har en mycket god säkerhet så individer och varumärken skadas, genom interna sabotage som vi såg på Kronfågel och barnmatsburkar med glasskärvor i maten och liknande. Organisationen arbetar mycket nära kunderna och har en stark

säkerhet. Säkerheten innefattas utav in- och ut- passage kontroller, restriktioner samt ID kort och lösenord.
Vart femte år ses dessa procedurer över genom en grovriskanalys, vilken görs genom en extern konsult. Detta ägde rum senast för cirka två år sedan. De arbetar ur en extern- såväl som ur en intern- vinkel och har ett nära samarbete med arbetsmiljöverket, räddningstjänsten och liknande. Detta samarbete är extra viktigt då verksamheten ses som ett högriskföretag då de hanterar vissa kemikalier.

5. Vad är det värsta som skulle kunna hända hos er ur ett systemhaveri perspektiv?
    - Vilka konsekvenser skulle det få för verksamheten?

    Långvariga typen av problem och förlorad koppling till moderbolaget.

6. Vilka risker har ni i er organisation prioriterat högst och arbetat mest med att reducera?
   Organisationen arbetar mycket på Tillgänglighet och Säker drift. Tillgängligheten säkerställs genom backup, batteribackup för servrar och datorer, samt laptops. Säker drift säkerställs genom åtkomstkontroller, restriktioner, krypteringar och liknande.
7. Hur bedömer du att säkerheten är ”tillräcklig”?
    - Vilka kriterier använder du/ni i denna bedömning?

Säkerheten förändras ständigt men kriterier är skapade utifrån omvärldskrav, från kunder samt genom kvalitetssäkringar och certifikat. Personalen har även ett gott sinne för kvalitet och kan se hur det tidigare fungerat, man har även lärt sig se risk och problemmönster, ”jaha är det dags för det igen.. och liknande”. Detta förekommer inte längre idag utan var vanligare under datorns barndom.

För kraven som finns idag är säkerheten tillräcklig men det tillkommer hela tiden ständigt krav på förbättring, policys och regler skärps och förändras sporadiskt.

”Den som väljer att inte utveckla sin organisations säkerhet är inget långvarigt företag på marknaden.”

8. Står ledningen bakom dig om du föreslår förbättringar i säkerhetsarbetet?
   Logistikchefen arbetar idag även med skydd utav tekniken, detta skyddande är ett krav från moderbolag såväl som från regering. Ledningen tar alltid anställdas på allvar såväl som Logistikchefen tar moderbolagets meddelanden på allvar.

9. Har motiverade säkerhetsförbättringar acceptans i ledningen och i organisationen?
   Är man inte nöjd med nya tänkta förbättringar, ofta är det internationella krav som alla måste anpassa sig efter. Så anställda under en stor koncern får till viss grad även anpassa sig till nya förändringar.

Riskkategori	Risktyp	Beskrivning	Uppskattad sannolikhet (1-5)	Prioritering (1-10)	N/A Icke relevant
Naturkatastrof	Jordbävning, vulkanutbrott, tsunami	Skadad utrustning	1	10	
Naturkatastrof	Storm	Strömavbrott, översvämning	5	2	
Naturkatastrof	Snöoväder	Hög belastning av verksamhetens infrastruktur	4	7	
Mänskligt orsakade katastrofer	Terrorism	Explosion	5	1	
Mänskligt orsakade katastrofer	Cyberterrorism, Crackers	Dataskadegörelse	5	3	
Mänskligt orsakade katastrofer	Internetattack	Systemet överbelastas, offlineläge	4	4	
Mänskligt orsakade katastrofer	Sabotage	Dataförlust	3	9	
Mänskligt orsakade katastrofer	Social engineering, Hackers	Dataintrång	3	3	
Oavsiktliga eller tekniska katastrofer	Felanvändning	Ogiltig data	4	6	
Oavsiktliga eller tekniska katastrofer	Tekniskt konstruktionsfel	Systemhaveri	4	5	

10. Känner du till någon incident (systemhaveri) som har hänt på organisationen under de senaste 5 åren? Och i så fall hur hanterades det haveriet? Information om haveriet, vad orsakade haveriet och hur upptäcktes det?
    Brutna interna internet/nätverksförbindelser, inget större.
    Inga intrång har ägt rum till Logistikchefens kännedom, men det kan dock hända dessa tystas ner från moderbolagets sida för att verksamheten inte ska framstå som sårbar.

Bilaga 5 – Transkribering inledande intervju regional organisation

Intervju

Nivå 1: Informanten

1. Vill du att organisation ska förbli anonym i uppsatsen?
   Nej det spelar ingen roll, Svedala kommun är en offentlig organisation.
2. Vill du som intervjuad vara anonym?
   Nej det finns inget behov.

Namn på den intervjuade: Hans-Åke Olsson
Position på organisationen: enhetschef på IT-support
Namn på intervjuare: Lars Lindvall & David Wahlström
Datum/tid för intervju: 27/4 -11
Intervjutid: 08.45 – 09.25

3. Vad har du för roll i organisationen idag?
   a. Vad innefattar dina arbetsuppgifter?
   Jag är enhetschef på IT-supporten i Svedala. Vi sköter allt som är IT-relaterat, förläggning av fiber, fixa med program, installationer, drift, allt som berör Svedala kommuns IT.

4. Hur länge har du haft den här positionen?
   i 5-6 år.

5. Vem rapporterar du till?
   Kommunledningen.

Nivå 2: Organisationen

1. Vad är dina tankar om din organisation?
   Mycket bra.
2. Finns det någon märkbar/särskild Kultur och karaktär i organisationen?
   Ja det kan man säga; alla ska kunna göra allt. Vi har inga som är specialiserade så där, eller jo det är klart, men i stort sett ska alla kunna göra allting.
3. Hur anser du att det är att arbeta i organisationen, utifrån din position?
   Jättebra, inga problem.
4. Finns det en särskild värdegrund i organisationen, i så fall vad?
   Hårt men hjärtligt, Jo men det skulle man väl kunna säga.
5. Ur ditt perspektiv, vad är syftet och drivkraften bakom organisationen?
   Jo alltså det är väldigt tydligt, bästa möjliga service och utveckling för så lite pengar som möjligt.
6. Hur arbetar ni för att vara konkurrenskraftiga?
   Jo alltså vi jämför oss alltid med att till exempel outsourca, det är väldigt enkelt mål på att säga att vi är konkurrenskraftiga. Vi kan ta ett exempel bara på skoj så, jag satt med en kille och så sa jag att varje arbetsstation kostar ungefär 4200kr. åh sa han det kan vi göra mycket billigare, men då ingår inte nätet sa han, men allting med arbetsstationerna, servrarna och sånt. Så sa jag vad kostar ni då? Ja 1500-1600kr i månaden sa han. Jaja men jag menar per år, då sa han att vi inte behöver prata mer. Det

visar att vi är konkurrenskraftiga. Vi jämför oss med andra kommuner, vad de har för kostnader, i hela landet och så vidare. Då vet vi att vi är fruktansvärt effektiva.

Nivå 3: Scenarier

1. Hur skulle du agera under följande scenarier?

Scenario 1

Åskväder och kraftig blåst har slagit ut strömmen i ert kvarter. Efter ett samtal till ansvariga för er elförsörjning får ni höra att stormen har orsakat problem hos dem. Elledningarna som leder till er organisation har på något vis brutits och att det krävs ett omfattande arbete för att identifiera problemet, de jobbar så snabbt de kan men en lösning på problemet kan dröja. Till följd av detta står ni utan ström och tillgång till de system som ni dagligen använder.

2. Vad skulle detta kunna leda till? (Finansiella förluster, förlorad arbetstid, förlorade kunder?)
3. Hur arbetar ni idag för att reducera riskerna detta scenario skulle medföra, och vilka är dessa risker?
4. Hur hanterar ni en sådan situation?
    a. Hur arbetar ni för att tillhandahålla en effektiv lösning?

    Svar på 2,3,4:
    Vi har dubbla reservkraftslösningar, vi har dels UPS som går in och när den inte håller längre så går dieselkraftverk in, så det ska inte vara några större problem. Så det håller igång servern även om vi får ström annanstans ifrån. Vi har ju gjort en bedömning på vilka system som är så att säga samhällskritiska och som då ställs i första hand. Det är ungefär 10 system som vi anser är samhällskritiska.

5. Hur länge skulle organisationen kunna fortgå utan tillgång till Informations Teknik (IT)?
    Ja alltså det är väldigt svårt att säga, men inom vården har man ju, dygnet runt, verksamheten pågår ju alltid. Men man har ju någon form av pappersbackup men det klarar man sig ju inte särskilt länge på. Det är ju vissa som är våra VA, vatten och avloppssystem, i och med att vi inte har något vattentorn så är ju allt datastyrt, pumpstationerna. Det är ju klart att det kan skötas manuellt men det är svårare.

Scenario 2

Vatten har börjat läcka in i era lokaler till följd en trasig vattenledning, anledningen bakom vattenledningens skada är vid tillfället okänd. Vattnet når er server, vilket orsakar en kortslutning och mörklägger hela lokalen. Vattnet måste stängas av och ledningarna måste lagas. Mycket vatten har hunnit läcka in och det kan ta tid att få hjälp med att laga ledningen och få ut allt vatten, men även att få igång alla system igen.

6. Vad skulle detta kunna leda till? (Finansiella förluster, förlorad arbetstid, förlorade kunder?)
7. Hur arbetar ni idag för att reducera riskerna detta scenario skulle medföra, och vilka är dessa risker?
8. Hur hanterar ni en sådan situation?
    b. Hur arbetar ni för att tillhandahålla en effektiv lösning?

    Svar på 6,7,8:
    Vi har redundanta serverrum, så sannolikheten att det ska läcka in vatten på båda skilda ställen är inte särskilt stor. Visserligen använder vi ju oss vattenkylning, så en läcka där skulle också kunna hända men det är ett slutet system så det ska inte kunna hända men man vet ju aldrig. Men det är en backventil som inte pumpar in mer vatten om det händer något.

Scenario 3

En individ med ond uppsåt vill organisationen illa och försöker sabotera dess verksamhet. I hopp om att organisationens arbete ska lida skada, saboterar individen alla IT-system som är verksamhetskritiska samt den tekniska utrustning som finns i serverhallen. Detta orsakar svårigheter att använda dessa system, systemen kraschar när det startar upp och det finns ingen möjlighet att komma åt data som behövs för verksamhetens arbete. Personen lyckades sabotera tekniken kraftigt och det kan ta tid att reparera.

9. Vad skulle detta kunna leda till? (Finansiella förluster, förlorad arbetstid, förlorade kunder?)
10. Hur arbetar ni idag för att reducera riskerna detta scenario skulle medföra, och vilka är dessa risker?
11. Hur hanterar ni en sådan situation?
    c. Hur arbetar ni för att tillhandahålla en effektiv lösning?

Svar på 9,10,11:

Om vi säger så är det väldigt få som har tillgång till serverrummet, det är skyddade med kod och bricka, båda ställena. Dessutom är det hänglås på det ena innanför och det är inget litet hänglås, och galler och sånt så det är väldigt litet chans att man kommer in utan nycklar och så. Men vad det skulle kunna leda till är väldigt svårt att säga. Finansiella förluster gör det ju inte, det är mer i form av förlorad arbetstid och återställningstid i så fall. Kunder förlorar vi inte direkt, eller alla som vi sköter är ju kunder. Man skulle kunna flyttar servern någon annanstans men det känns inte troligt. Det mest att man räknar ut hur länge de har stått utan systemet, utan att kunna göra vissa saker så kan det ju bli en peng på det. Det är väldigt förändring som har skett under en kort tidsperiod, som tidigare kunde vi stänga ner system i ett par timmar, alltså var tvungna till att göra det av olika skäl. Och då sa dem att de kunde göra annat, men senaste gången vi hade planerat ett avbrott, vi skulle fixa med fiber, var det stopp i två timmar. Då sa de att de lika gärna kunde ta semester för de kunde inte göra någonting. Det är väldig förändring som har skett, visserligen var det en fredag så det kanske var lite därför också men det har ändrats mycket.

12. Hur fungerar samarbetet mellan säkerhetsavdelningen och H/R avdelningen?

Säkerhetsavdelning har vi inte egentligen, på så vis. Men inom Svedala kommun, de anställda där är det bra kommunikation, det måste vi ju ha. Man har ju tillsatt en säkerhetsansvarig som skulle kunna räknas som säkerhetsavdelningen, men jag vet inte. Vi driftar deras system till exempel. Det är ett av de kritiska systemen, lönen kommer därigenom, så det är viktigt. Det är svårt att svara på det.
Vi har ju en viss övervakning som vi då har svarat för, att folk gör vad de ska. Och det har faktiskt hänt att vissa sysslat med en del, men då har ju jag gått till kommundirektören, så har hon kontaktat H/R / personalenheten, så det är så det sker. Övervakning på så vis att vi kollar den trafik som går ut och in. Och det har ju inträffat saker. Sen har personalenheten automatisk som sköter det, i de fall som det gällt har det gällt uppsägningar. Sen det här med sabotage, tänker man ofta att det skulle vara virus och så, men då har man så att man kan återställa via backup, spegling på olika lösningar. Men ibland gör man faktiskt mer skada med en kofot om man säger så. Går man in där och slår sönder grejerna så är det svårare att återställa och få fram data igen. Men det tänker man inte ofta på. Men som sagt ska det mycket till för att ta sig in i ett serverrum. Man ska in genom två dörrar och det är inte vilka dörrar som helst. Det är väldigt bra här i kommunen kan jag säga. Innan har man haft ett källarrum bara men så är det inte här. Vi ändrade om det för ungefär 2 år sedan, som vi byggde om serverrummen helt. Så vi allt sånt med gas som släcker bränder. Vi har slutna system i skåpen så rummen är inte brandceller på samma sätt utan det är skåpen som är brandcellerna. Så det kommer aldrig in något vatten där, utan de släcks med gas. Så man går tänka på att stänga av gasen när man ska jobba där för det tar bort allt syre, så det är lite halvfarligt annars. Om man ska sabotera skulle man kunna slå sönder kylanläggningen på utsidan av huset men då har vi reservvatten som går på istället och pumpar direkt ur kranen. Då kyls det med vanligt vatten, genom en värmeväxlare. Det vet vi att det fungerar för det

har hänt, att det har gått sönder. Så då fick man en fräck vattenräkning, eftersom det är många liter som pumpas igenom i minuten.

Nivå 4: Kompletterande frågor:

1. Hur går er process till för att utveckla en åtgärdsplan och inom vilka intervaller revideras denna?
   Vi har revision på det, det är KPMG som gör det. Då går dem igenom en checklista med allt som berör planeringen. Vi har ju gjort allting det här BITS Plus (Basnivå för informationssäkerhet), där har vi åtgärdsplaner och många, många steg och vem som har ansvar osv. Och det är utefter ett bestämt mönster, så det är inget som man kan avvika ifrån utan man ska svara på alla de frågor som finns.
2. På vilket sätt engageras de anställda i åtgärdsplanen och dess utveckling?
   Vi har försökt med det här men har inte fått gehör för det. Att alla ska genomgå någon kurs på en timme, men det har vi inte kommit till ännu. Man anser att det kostar för mycket. Alla anställda kommunen är 1500 st. Man säger att en timme är ingenting men det är ett helt manår, 1700 timmar, så det är rätt mycket. Så jag har förståelse för motargumenten.

3. Hur arbetar ni internt med säkerhetslärande och sker detta arbete på samtliga nivåer i organisationen?
   - Om ja, inom vilka intervall sker denna utbildning?
     Se 2.
4. Hur bedömer du att katastrofhotbilden för organisationen ser ut? (Interna/Externa hot?)
   Ja alltså vi har ju målat upp scenarior, som kan hända och sånt men de är inte sådär direkta utan det är mer konstruerade så. Det är klart, det finns ju alltid interna hot; att någon skulle kunna ta sig in för långt osv. Och likadant externa, men vi har ju försökt begränsa så att det inte är möjligt, genom användning av policy och olika typer av andra verktyg för att förhindra det. Och om någonting trots detta skulle inträffa har vi larm och sånt som går direkt.

5. Vad är det värsta som skulle kunna hända hos er ur ett systemhaveri perspektiv?
   - Vilka konsekvenser skulle det få för verksamheten?

   Det värsta som skulle kunna hända hos oss är egentligen inte att något rasar egentligen eller skulle släckas, utan förlust av data, det är det värsta som skulle kunna hända. Om man inte tagit backup eller om backupen har blivit felaktig. Dataförlust är det värsta som skulle kunna hända. Att det sen skulle vara stopp ett par dagar är en annan sak. Vissa system skulle vi säkert kunna få upp efter någon timme om de skulle rasa. Det händer ju att de stannar och att man får göra om det från början men då bygger det på att man har data. Men man har ju hört vissa ställen, sjukhus och så som har blivit av med data och fått ringa runt till patienter och knacka in data för hand. Det är ju bland det värsta. Det skulle vara väldigt svårt att få tillbaka all data, nästintill omöjligt för hand. Och i dagens läge är det inte möjligt. Jag kommer ihåg ett ställe, det var Simrishamn, deras ekonomi och lönesystem havererade och de hade ingen backup. Disken blev förstörd och man räknade på att det skulle ta 9 månader i tre skift personer att få in all data ifrån papper. Det var ingen som kunde återställa disken men sen skickade någon ut en fråga på internet så var det en kille som kunde återläsa disken, men det är ungefär 10 år sen det här hände. Och sen har vi ju Höganäs också, de låg nere i 4 eller 5 dagar. Men idag bygger systemen på att man har redundans, mins två servrar och backuper och andra speglingar innan backuperna, så det är ofta flera gånger säkrat. PA och lönesystemet har vi alltid, där skickar vi dessutom upp backup varje natt. Man skickar kontinuerligt upp en fil till leverantören som håller data. Plus att vi lägger över det till en server också. Vi har en så kallad utbildningsserver och en lyftserver och de är i stort sett alltid lika.

6. Vilka risker har ni i er organisation prioriterat högst och arbetat mest med att reducera?
   Det är de systemen som vi har satt som samhällsviktiga som prioriterar mest kring. De har vi fokus på hela tiden och väldigt bra övervakning på. Det är Systemen; PA, vård, mail, inloggning, webbservrarna, VA. Om man räknar otillgänglighet som en risk, vilket man gör då kan det vara att man har dålig kapacitet, dvs dåligt när/fiber. Så vi har prioriterat vårt bygga upp vårt nät också så att det klara av lite mer trafik. Annars finns risken för flaskhalsar, att trafiken stannar upp. Nätet är därmed också en del av prioriteringen. Vi håller på redundanta ringar så om man gräver av på ett ställe kan man köra det en annan väg.

7. Hur bedömer du att säkerheten är ”tillräcklig”?
   - Vilka kriterier använder du/ni i denna bedömning?

   Det är att systemen ska fungera och vi har sagt att den som mest ska få ligga nere i två timmar. Men det anser ju inte alla inom organisationen. Men ska man komma upp i högre säkerhet där kräver det att man dubblerar budgeten, nät och serverrum och så, men för vår kommun är inte det realistiskt och inte med den budget vi har heller. Det är en typ av säkerhet, en annan är att se om vi har tillräcklig säkerhet för de som loggar in datorerna, man kan tänka antivirus och så. Och där att göra på som kommunen och som staten strävar på är säkrare inloggning, som vi också håller på med. Stark inloggning, i form av kort med något chip, bank-id eller något sånt. Vi har tekniken men det är mycket som ska till, många läsare osv som ska ut
   Vi har 1500 anställda och ungefär 3200 arbetsstationer och till nästa år ökar det med 1200 till. Så vi kommer ha nästan 5000 arbetsstationer. Så det är inte en så lite organisation som man tror. Man tycker att det är en liten kommun.
   Bara internetabonnemang är en miljon kronor i kostnader för kommun. Medelpriset för en arbetsstation, pris per dator per år, inköp av dator osv, normalkommun ligger det på ungefär 18 000kr per arbetsstation/år för allting, vi ligger på strax över 4000kr, så vi ligger bra till. Lund ligger i jämförelse på över 20 000.
8. Står ledningen bakom dig om du föreslår förbättringar i säkerhetsarbetet?
   Nja, det svarade jag lite på innan egentligen. Det här med att man prioriterade bort den utbildningen som jag tycker jätteviktig (och gick på teater istället(skämt)). Sen kan man se det på en väldigt enkelt nivå om man tar ett förslag att idag har vi 6 tecken minimum gräns för lösenordet, ett förslag är att ändra enligt KPMG och höja säkerheten till 8 eller lite komplexitet/komplitet då. Då fick man motstånd direkt, för folk inte kommer komma ihåg sina lösenord. Sen vill vi ju ändra från 90 till 60 dagar också, att man måste byta sitt lösenord lite oftare, men då blir det lite mer svår hanterligt. Och sen historik också, så at man har 12 lösenord i minnet, så att man inte kan gå tillbaka till ett tidigare lösenord.

9. Har motiverade säkerhetsförbättringar acceptans i ledningen och i organisationen?
   Delvis, men inte alltid. Men det alltid så att det är en övergångsfas där, i början är det svårt men sen tänker man inte riktigt på det.

Riskkategori	Risktyp	Beskrivning	Uppskattad sannolikhet (1-5)	Prioritering (1-x)	N/A Icke relevant
Naturkatastrof	Jordbävning/vulkanutbrott/tsunami	Skadad utrustning	1	10	X
Naturkatastrof	Storm	Strömavbrott, översvämning	2	9	
Naturkatastrof	Snöoväder	Hög belastning av verksamhetens infrastruktur	2	9	
Mänskligt orsakade katastrofer	Terrorism	Explosion	1	10	X
Mänskligt orsakade katastrofer	Cyberterrorism/ Crackers	Dataskadegörelse	2	5	
Mänskligt orsakade katastrofer	Internetattack	Systemet överbelastas, offlineläge	4	5	
Mänskligt orsakade katastrofer	Sabotage	Dataförlust	2	1	
Mänskligt orsakade katastrofer	Social engineering/Hackers	Dataintrång	3	1	
Oavsiktliga eller tekniska katastrofer	Felanvändning	Ogiltig data	5	1	
Oavsiktliga eller tekniska katastrofer	Tekniskt konstruktionsfel	Systemhaveri	2	1	

Storm – Vi får problem med radiolänkarna vid storm, så då är det alltid mycket problem. Med en del mindre verksamheter kör vi med VIMAX(radiolänk) och då tappar man kontakten när det blåser för mycket.
Prioritet – Allt har givetvis högsta prioritet om det skulle inträffa för sig.

10. Känner du till någon incident (systemhaveri) som har hänt på organisationen under de senaste 5 åren? Och i så fall hur hanterades det haveriet? Information om haveriet, vad orsakade haveriet och hur upptäcktes det?
Sista 5 åren, har vi haft en fiberavgrävning, så att internetuppkoppling bröts. Sen har telefonin legat nere, det var ungefär 2 år sedan. Där har vi en reservplan också om det händer, då lägger vi ut på internet, så kopplas det till mobilnummer istället. Det finns ju ganska mycket mobil idag. Mailstopp har vi haft också, men det var på en helg så det påverkade inte så mycket, då vi hann fixa det snabbt. Det hanteras väl främst genom att vi går ut med meddelande på internet till alla. Vi har ju hittills inte haft några stora grejer, tur nog. Det finns ju massvis med system som privatpersoner inte känner till, som är fruktansvärt viktiga. Så annars tickar det jäkligt mycket pengar. Sen finns ju vårdplanering också, om någon finns på sjukhus, så ringer de därifrån och säger at personen är medicinskt färdigbehandlad och då kan det vara ett kolli som inte klara sig själv. Då har kommunen 24 timmar på sig att fixa en vårdplats inom kommunen annars tickar ungefär 5000kr per dygn, då är man rätt beroende av att sådana system fungerar så att man får reda på det så snabbt som möjligt. Det är rätt tuffa grejer men det äringen som tänker på sånt, det blir snabbt pengar. Vi har som sagt annars varit väldigt skonade ifrån problem.

Vi har mycket spridning på användarna, det är fruktansvärt mycket system. Det är från alla medborgares användande av våra prylar till.. och alla anställda osv. Men det är ju våran främsta uppgift, att serva medborgarna i kommunen. Så vi har många kunder på det sättet, och skolarna blir en väldigt stor kund, dels ungarna men sen gäller det deras vårdnadshavare också.

Bilaga 6 – Transkribering kompletterande intervju regional organisation

Intervju

Nivå 1: Informanten

1. Vill du att organisation ska förbli anonym i uppsatsen? Nej
2. Vill du som intervjuad vara anonym? Ja

Namn på den intervjuade:
Position på organisationen:
Namn på intervjuare: David Wahlström & Lars Lindvall
Datum/tid för intervju: 6/5 - 2011
Intervjutid: 10.00 – 11.00

3. Vad har du för roll i organisationen idag?
    a. Vad innefattar dina arbetsuppgifter?
4. Hur länge har du haft den här positionen?

Svar på 3 &4:

Man kan säga att min position har förändrats, för 5 år sedan var jag IT-ansvarig inom miljö/teknik och gjorde sådana här risk- och sårbarhetsanalyser. Och tog fram ett dokument som skulle vara vägledare för hela övriga kommunen. Så vi har penetrerat de här grejerna med att ha, vad ska man säga, alternativa planer. Typ som ni har tagit upp här med avloppsreningsverket, att man kan köra det manuellt, att man har dokumentation framme, pappersvägar som man kan få fatt i. Och vi gick igenom alla dem dåvarande programmen som fanns då. Så utifrån det tycker jag att man har haft ett säkerhetstänk men jag säga det att sen jag lämnade det har det inte hänt ett dugg på det området utan det är mer att IT-enheten har tagit ett övergripande mer ansvar för det här. Man kan väl säga att det är så utvecklingen har varit. Och idag har jag inte ett dugg ansvar för det här. Jag blev tillfrågade om jag ville bli IT-säkerhetsansvarig men det ville jag inte. Så det ansvaret ligger nere på räddningstjänsten idag, från och med februari 2011.

5. Vem rapporterar du till?
Det är inte så lätt. Jag har ju min chef här på avdelningen, men jag jobbar mest åt miljö/teknik fortfarande, så då är det tekniska chefen. Och sen har jag ett uppdrag inom vård och omsorg där jag rapporterar till socialchefen. Och sen på en fjärdedel av min tjänst så rapporterar jag till kommundirektören. Så är det i en liten organisation, det därför det är kul att jobba i en liten organisation. Det passar mig personligen. Man kan jobba brett i en liten kommun.

Nivå 2: Organisationen

1. Vad är dina tankar om din organisation?
Det är en jättebra. Det är en välfungerande kommun. Man kan säga att vi alltid har haft ett motto; ”du ska alltid tänka på vilken insats du gör i förhållande till nytta”, alltså man ska väga nytta och insats. Alltså när du gör en arbetsuppgift så ska den verkligen tillföra kommunen göra det, du sitter inte gör någonting för de har ni gjort i hundra år. Det finns ett ständigt ifrågasättande, så upplever jag och det är så jag jobbar i kommunen här. Det finns en möjlighet att ifrågasätta också att bli hördhet. Man utvecklar organisationen hela tiden, bra arbetsmetoder och tar till sig ny teknik. Och då är det viktigt att de här grejerna funkar, med säkerhetsbiten. Vi har en väldigt duktig IT-avdelning, väldigt kreativ IT-avdelning, med hög servicegrad. Hans-Åke är så duktig som han säger.

2. Finns det någon märkbar/särskild kultur och karaktär i organisationen?
    d. Om ja, beskriv den kortfattat?

    Jag kan nog säga att Svedala kommuns organisation är indelad i fyra olika verksamhetsområden, som jobbar mot olika verksamhetsområden, fyra olika kulturer. Där när det gäller IT-utvecklingen är man klart längst fram inom miljö/teknik, med det är klart där har man ju jobbat med tekniskt program så pass länge, och det är mycket ingenjörer. Och sen tror jag att man kan säga att kommunledningen med sina övergripande system är väldigt framåt, ekonomisystem. Jag har själv varit projektledare för införandet av ett nytt PA/lönesystem. Det är bara att vi ska få mer digitaliserad posthantering, det är ju det som är kvar där i den processen, men vi en duktig ny utvecklingsstrateg som jobbar mycket med processutveckling och så. Så vi ska titta ännu mer på organisationen där.

3. Hur anser du att det är att arbeta i organisationen, utifrån din position?
   Det är jättebra, det är mycket frihet under ansvar. Vill du påverka så kan du påverka och det är ju det som är viktigt.
4. Finns det en särskild värdegrund i organisationen, i så fall vad?
   Vi har haft lärande organisation under en period, men nu har vi öppen kommun. Alltså vi har medborgarperspektivet i fokus. Stärka kommunfullmäktige, i den nya politiska organisationen, tydliggöra det politiska ansvaret och utveckla medborgardialogen. Vi ska ha en god service mot.., alltså tjänsteorganisationen ska jobba mot politiker och mot medborgare, om man då inte säger att företagen är medborgare, kallar man dem för judiskperson, så är ju det vårat uppdrag; att ta hand om dem och hjälpa dem på bästa sätt, och ge dem bästa möjliga underlag.
5. Ur ditt perspektiv, vad är syftet och drivkraften bakom organisationen?
   Drivkraften iden här organisationen är alla duktiga medarbetare som finns här. Det är dem som driver. Och har man frihet under ansvar så frigör man den möjligheten, just att man inte har frustrerade medarbetare. För det lägger locket på, för då vågar dem inte, men om inte det finns så kan ju folk utvecklas och ta egna initiativ och det är det som driver kommunen framåt. Om man säger en företagsledning så är den mer permanent, men vi har ju val fjärde år vilket gör då kan vi få en helt annan styrning, som nu har vi väldigt många nya politiker, som ska hitta sina roller och lära känna kommunen och då kan ju inte kommunen helt avstanna då bygger det på att kunnigt folk i organisationen som fortfarande kan serva de här viktiga grejerna; vi har älderboende, vi har barnomsorg, gator och park ska skötas, och sen har vi den här tillsynsverksamheten, bygg och miljösidan, de ska ge bygglov. Det måste ju fungera allting sånt här.
6. Hur arbetar ni för att vara konkurrenskraftiga?

Nivå 3: Scenarier

1. Hur skulle du agera under följande scenarier?

Scenario 1

Åskväder och kraftig blåst har slagit ut strömmen i ert kvarter. Efter ett samtal till ansvariga för er elförsörjning får ni höra att stormen har orsakat problem hos dem. Elledningarna som leder till er organisation har på något vis brutits och att det krävs ett omfattande arbete för att identifiera problemet, de jobbar så snabbt de kan men en lösning på problemet kan dröja. Till följd av detta står ni utan ström och tillgång till de system som ni dagligen använder.

2. Vad skulle detta kunna leda till?
    d. Finansiella förluster, förlorad arbetstid, förlorade kunder?
3. Hur arbetar ni idag för att reducera riskerna detta scenario skulle medföra, och vilka är dessa risker?
4. Hur hanterar ni en sådan situation?

5. Hur arbetar ni för att tillhandahålla en effektiv lösning?

Svar 2, 3, 4, 5:

Om jag ställs utan system så gör det ingenting, jag har ingen sådan funktion. Men jag vet ju att, och det har Hans-Åke sagt, jag vet att det finns reservelverk, stationärt reservelverk i kommunhuset som slår på så här snabbt. Men om inte det skulle fungera så är det ingen katastrof, utan jag kan vara hemma en vecka, jag är inte ute i kärnverksamheten, jag undervisar inte, så det är ingen fara. Man har jobbat mycket med det här med reservkraftverket men det gjorde man redan.., 1995 köpte man in både stationär elkraftverk och sen har vi då mobila som för närvarande finns nere på vattenverket. Som vi faktiskt lånar ut till andra kommuner, i samband med Gudrun lånade vi ut upp småland. Så vi har goda resurser, överhuvudtaget har vi väldigt god ordning på beredskapsorganisationen vid kristider. När andra tekniska chefer har kommit hit och tittat på vad som är gjort i Svedala så blir det flesta väldigt imponerade av att vi har så god kontroll, plus att vi då varje år som organiseras av beredskapsansvariga olika scenarier vid kris, så att de får öva på det. Det vet jag inte om Hans-Åke har berättat men det är väldigt gott ställt i det här tänket, man har väldigt hög riskmedvetenhet och det ett grundläggande dokument är ju risk- och sårbarhetsanalysen som tas fram varje år, av räddningstjänsten. Där man värderar alla risker, plus att vi har ett nätverks när det gäller säkerhetsarbete. Främst då fyra Yes, Lomma, Staffanstorp, Kävlinge och Svedala har ett starkt nätverk när det gäller samarbete på all områden, och förutom det så går man ju ut ännu längre där det finns olika träffar i hela Sverige kring säkerhetsarbete, så man hjälps åt hela tiden. Så jag tycker att har mycket hög fokus plus att, jag tänker på det här med BITs, som Hans-Åke nämnde, ett speciellt system som man följer och sen att vi har haft speciella revisioner här med just fokus på säkerhet, så jag tycker vi jobbar väldigt mycket med det. Angående utbildningar, där hansåke har framfört, att det borde finnas en liten introduktionsutbildning. Och jag tror att om man hade packat in det som ett ärende och lyft det till politiken typ i en budgettprocess så hade man fått acceptans på att göra detta. Så det kommer jag råda IT-avdelning, att man paketerar det på ett lite annorlunda sätt. För det är så att när vi från verksamheten för fram ärenden som vi tycker är viktigt så kör vi den via politiken, inte bara inom tjänstemanna organisationen, för det är ju det IT-avdelningen har gjort hittills. Genom att bara vända sig till kommunledningsgruppen. Men det kan också ha sin historia att det inte är förrän nu som vi har tydlig politisk fullmäktigeberedning mot IT's område, för då har vi fått en ny beredning som heter ekonomi och demokrati, och att man då lyfter ärendet där.

6. Hur länge skulle organisationen kunna fortgå utan tillgång till Informations Teknik (IT)?
   Det är lite hur viktigt man tycker att det man håller på med är. Men om man säger det som jag håller på med, det viktigast är att jag följer lagstiftningen. Jag som då i dagsläget jobbar med ekonomi, den lagstiftning vi följer det är att vi ska budget dokument som ska beslutas i fullmäktige i november månad, vi ska ta fram uppföljningar och då finns en lagstadgad i uppföljning i augusti, en i september som vi tar fram som är delårsbokslut och sen finns det bokslut eller årsredovisning som tas fram i januari. På hösten är det mest kritiskt om ekonomisystemet skulle haverera fullständigt, men vi hade kunnat anta en budget trots att vi inte har tillgång till systemet eller fungerande nätverk men vi hade knackat på maskiner, skriva för hand, alla ärenden. Men vi hade kunnat ta beslut om en budget, rent praktiskt hade vi kunnat göra det. Så jag menar på att det för min del är det inte hela världen.

Scenario 2

Vatten har börjat läcka in i era lokaler till följd en trasig vattenledning, anledningen bakom vattenledningens skada är vid tillfället okänd. Vattnet når er server, vilket orsakar en kortslutning och mörklägger hela lokalen. Vattnet måste stängas av och ledningarna måste lagas. Mycket vatten har hunnit läcka in och det kan ta tid att få hjälp med att laga ledningen och få ut allt vatten, men även att få igång alla system igen.

7. Vad skulle detta kunna leda till?
    d. Finansiella förluster, förlorad arbetstid, förlorade kunder?
8. Hur arbetar ni idag för att reducera riskerna detta scenario skulle medföra, och vilka är dessa risker?
9. Hur hanterar ni en sådan situation?
10. Hur arbetar ni för att tillhandahålla en effektiv lösning?

Svar 7,8,9,10:

I en sådan situation kan jag ta ledigt, då får jag gå hem. Jag har inga löpande arbetsuppgifter utan det är bara utredningar och olika projekt som jag jobbar med. Men det är klart att för dem som jobbar i kassa är det fullständig katastrof med dagbokföring, då hade det ju inte funkat, om man ser i det perspektivet. Men utifrån min synpunkt hade jag kunnat ta ledigt istället. För kärnverksamheten hade det varit en fullständig katastrof, för då hade inte dem kunnat beställa mat, laga mat till barnen och äldre, eller de har ju inom ålderomsorgen journalbokföring. Allt det hade varit en fullständig katastrof. Så det hade inte alls varit bra, men ur mitt perspektiv påverkas inte det mitt arbete så mycket.

Scenario 3

En individ med ond uppsåt vill organisationen illa och försöker sabotera dess verksamhet. I hopp om att organisationens arbete ska lida skada, saboterar individen alla IT-system som är verksamhetskritiska samt den tekniska utrustning som finns i serverhallen. Detta orsakar svårigheter att använda dessa system, systemen kraschar när det startar upp och det finns ingen möjlighet att komma åt data som behövs för verksamhetens arbete. Personen lyckades sabotera tekniken kraftigt och det kan ta tid att reparera.

11. Vad skulle detta kunna leda till?
    g. Finansiella förluster, förlorad arbetstid, förlorade kunder?
12. Hur arbetar ni idag för att reducera riskerna detta scenario skulle medföra, och vilka är dessa risker?
13. Hur hanterar ni en sådan situation?
14. Hur arbetar ni för att tillhandahålla en effektiv lösning?

Svar 11,12,13,14:

Angående Hackers tror jag det är enkelt, om man är riktigt duktig och vill det så kan man nog göra det. Det hade varit en ganska jobbig situation, men det hade inte lett till någon personlig skada, om bara barnen hade kommit dagis och personal hade varit där och skött om det så kan de sköta barnen trots att de inte har en dator, så är det ju. Men det är bra om de kan laga mat, så barnen får mat. Och avloppsreningsverket det kan man ju driva utan, men det är lite jobbigare att köra det manuellt. Allting försvåras men det är klart att det går. Det hände ju Höganäs för två år sedan, det tog ju mer än en vecka att får ordning på det och då är det väldigt mycket som man ska ta igen efteråt naturligtvis. Men sen samtidigt kanske man prioriterar att det är vissa grejer som man inser att det var inte så viktigt så man slutar göra det. Sådana här incidenter gör ju att man tänker till lite, det kan också vara utvecklande, kom jag på nu precis. Då är det vissa grejer som man får prioritera bort, för man hinner inte med allt.

15. Hur fungerar samarbetet mellan säkerhetsavdelningen och Human Resource avdelningen?

Det kommer att bli ännu bättre nu för jag är projektledare för att sätta ihop ett råd som vi kommer att kalla trygghet och säkerhet, som ska vara av besatta av dels politiken, dels de högre tjänstemännen och är ska alla sådana här säkerhetsfrågor lyftas fram och bli ännu tydligare och ännu bättre än vad de är idag. Idag så kan man diskutera säkerhet i brottsförebyggande rådet, man diskuterar trafiksäkerhet i trafiksäkerhetsrådet, sen har vi ett folkhälsoråd, där säkerhetsbiten också kan komma in, typ fall in vård och omsorg. Nu slår man ihop allt detta, så man diskuterar de här grejerna i ett forum. Och sen i det här forumet, de ska då bestämma ”what to do”, vad ska göras. Och de besluten baserar sig på en arbetsgrupp där inte politiken ska vara inblandad i ”How to do”, hur vi ska göra. Alltså i högsta enheten - vad ska göras, och sen en grupp – hur ska vi göra, och sen ”do it”, det är liksom verksamheterna som ska utföra det sen. Och då ska vi få en tydlig organisation kring det här, så att det

kommer att bli ännu bättre än vad det har varit tidigare. Och detta greppet är taget ifrån en kommun uppe i Göteborg, och där har Staffanstorp kommun blivit inspirerade av dem, för 10 år sedan. Jag är då övergripande projektledare för fyra Yes samarbetet och är Svedalas representant. Så det är egentligen jag som har satt igång det här, hur ska vi kunna utvecklas vi kommuner tillsammans, inom det här området. Så det som pågår nu, samma arbete pågår i Lomma kommun och Kävlinge kommun, och sen 2012 och i Staffanstorp som redan har det ska man utvärdera sin verksamhet. Sen 2012 ska detta projektet fortsätta, så att man dels ska kunna få en bättre organisation lokalt i vår kommun men dels utnyttja förmågan när vi blir fyra stycken som tänker kring de här frågorna. Om man slår ihop alla dessa fyra kommuner är vi lika många invånare som i lunds kommun,100 000. Och det är det perspektivet, att då kanske man kan göra mycket mer. Skillnad med lunds kommun är då att vi har fyra olika politiska organisationer som ska samsas men de har ju bara en politisk organisation i Lund, och det är ju det som är det svåra. Så jag tycker vi har väldigt mycket fokus just på säkerhetsbiten och IT-säkerheten är väldigt viktigt, det är en av de viktigaste bitarna i det här området och det ingår i det här paketet

Nivå 4: Kompletterande frågor:

1. Hur går er process till för att utveckla en systemsäkerhetsplan/åtgärdsplan och inom vilka intervaller revideras denna?
   Svarats på tidigare
2. På vilket sätt engageras de anställda i systemsäkerhetsplan/åtgärdsplan och dess utveckling?
   Jag kan väl säga som så här, förr i tiden blev jag involverad för då kom det ett förslag ifrån miljö/teknik, när jag gjorde det men det är väldigt länge sedan. Jag har väl lite den känslan att här skulle jag inte bli involverad, men det är mer att jag inte har den rollen.
3. Hur arbetar ni internt med säkerhetslärande och sker detta arbete på samtliga nivåer i organisationen?
   h. Om ja, inom vilka intervall sker denna utbildning?

   Se tidigare svar

4. Hur bedömer du att katastrofhotbilden för organisationen ser ut? Interna/Externa hot?
   Jag ser inga speciella hot, inte så men det är ju mer ett positivttänk. För jag har inte de ögonen heller, det är inte mitt uppdrag att ha dem ögonen, så så är det ju. Men ni märkte ju när ni kom in här att det är lite fort knox över det här huset. Man kan inte gå rakt in här utan man måste anmäla sig i receptionen och det är ju bara 6 år sedan som man gjorde så, för innan kunde man komma utifrån och gå rakt upp till kommunalrådet direkt. Och då kunde man ha vapen och så med sig och det var ju ingen stoppade eller hade kontrollen. Så det var SÄPO som var med och gjorde en riskinventeringsarbetet om vilka som var de yttre hoten. Så jag tycker att vi har haft SÄPO med också i det här arbetet.
5. Vad är det värsta som skulle kunna hända hos er ur ett systemhaveri perspektiv?
   d. Vilka konsekvenser skulle det få för verksamheten?

   Då kan du titta på olika perspektiv det finns det ekonomiska perspektivet men jag tycker att miljöperspektivet är precis lika viktigt. Om du tänker dig avloppsreningsverket om det skulle haverera fullständigt, då kommer allt ut i Segeå, och kommer det ut där förorenar det hela vägen ut och kan förstöra ganska mycket på vägen. Men det är kanske inte det man tänker i första hand. Sen blir det ju inte så att folk dör om det inte skulle fungera för vi har ju inte som ett sjukhus, hjärtlungmaskiner som ska vara igång, utan det är främst vård. Och medicin kan man ge ändå. Barnen blir inte heller påverkade så. Det värsta som jag har, inte varit med om men det var någon som var som inte fick socialbidrag och som är psykisktsjuka eller något sånt och kommer hit och vill hot med vapen, yxa eller dylikt, och ska slå ihjäl folk. Det är egentligen det som är det mest

farlig, men det är inte IT, IT-säkerhet utan det är annat hot/våld. Och det är sånt som inspektörer också kan bli utsatta för. Alltså när man har den härmyndighetsrollen och folk blir förbannade då är det väldigt utsatt men det är inte IT-perspektiv utan det är annat hot. Sen är det klart jobbigt om det skulle hända som hände Perstorp att de hackade sig inte och stal massor miljoner. Det var så att det var en medarbetare som hade ont syfte att skada Perstorps kommun, så han började jobba där, lärde sig rutinerna, hur alltingfungerade, så det pågick under en lång period, innan det skred till verket. Och det han gjorde då var att han anlade en vattenläcka som förstörde mycket plus att all organisation var fokuserad på att fixa den här vattenläckan och då kunde han hålla på med de här grejerna och sen hade han misshandlat socialchefen så han hade får ut ett lösenord som gjorde att han hade möjlighet att betala ut socialbidrag. Under den här perioden så gick han in i systemen och betalade ut till sina egna konton, miljonbelopp. Och det knepiga här var att när man upptäckt det så kunde inte banken stoppa utbetalningarna utan de gick vidare, det var vissa som man kunde stoppa men inte alla. Så det var flera miljoner som inte fungerade, som man gick miste om och sånt kan ju hända för vi har inte så otrolig säkerhet. Och när man så medvetet vill gå in och göra någon, den här socialchefen var hemma och var sjukskriven så han kunde inte stoppa det heller. Vill man verkligen gör en sån grej och tillhöra kriminella kretsar så är det klart det kan man göra. Men vi har mer den uppfattning att vi misstänkliggör inte all personal vi har inte det synsättet, vi har det sättet att personal tillför saker och gör så gott de kan. Och de systemen som vi har skall mer säkerhetskälla att man inte misstänkliggör personalen. Innan man betalar en faktura är det två stycken som ska skriva på. Är det pengar som ska gå till mig får jag inte vara inblandad överhuvudtaget, alltså två helt andra personer som ska skriva. Vi har sådana testreglemten. Jag kan inte gå in i procapita det har vår och omsorg det systemet så där kan inte jag gå in i. så där är behörighetssystem för varje verksamhetssystem som är separat och lösenordsskyddade, så jag har behörighet som går till närverket och som gäller ekonomisystemet. Men jag har inga möjligheter att göra utbetalningar till mig själv till exempel. Och jag har sett till att jag inte har attesträtt överhuvudtaget, det är många ekonomer som har attesträtt men jag har inte det. Det är cheferna som får ta ansvar för det. Man kan olika sätt att se på det

6. Vilka risker har ni i er organisation prioriterat högst och arbetat mest med att reducera?
   Det är de som är samhällsfarliga, de riskerna. Det går enligt den säkerhetpolicy/säkerhetsarbetet och det är egentlige utfärdat av de statliga myndigheterna att vi ska prioritera det, typ när de skulle ha den här svininfluenssprutan så var det främst den personal som höll på med det mest nödvändiga i kommunen som fick först, så prioriterades det ner. Alla sådana sammanställningar har gjorts och det är ett förebyggande arbete
7. Hur bedömer du att säkerheten är ”tillräcklig”?
   d. Vilka kriterier använder du/ni i denna bedömning?
      Jag tror att det är jättesäkert, men prata med Hans-Åke så är det inte det. Men han har ju en helt annan kunskap, jag har inte kunskapen att göra den bedömningen.
8. Står ledningen bakom dig om du föreslår förbättringar i säkerhetsarbetet?
   Vart man vänder sig beror på om man vill ha en biobiljett eller inte, vill man ha en biobiljett så gör jag ett formellt ärende av det och så ger jag det till förslagslådan. Den lådan bearbetas av kommunledningsgruppen, alla som lämnar förslag till förändringar i organisation som kan göra jobbet effektivare/bättre, bara man lämnar in ett förslag blir man belönad med en biobiljett och kanske fler ekonomiska konsekvenser/förbättringar, så kan man även få en peng. Men Hans-Åke har en roll som gör att han ska förbättra IT-arbete, det ska han göra inom sitt arbete så han får ingen ekonomisk kompensation, om ni förstår skillnaden där emellan. Så jag tycker att vi har väldigt goda incitament till förändringar, sen kan jag väl säga att jag är en sådan person som har varit här så länge och känner så mycket folk så jag planterar ut idéerna hos flera, som kan föra det fram. På det viset tycker jag att det finns stora möjligheter att påverka till förändringar/förbättringar.
9. Har motiverade säkerhetsförbättringar acceptans i ledningen och i organisationen?

Ja, det finns ett väldigt gott klimat när det gäller att förändra/förbättra saker och ting. Sen får man vara realist, vissa saker tar två år. Men det gör inget om det till slut blir en förändring, så är det. För vissa personer tar det väldigt lång tid att förändra och det krävs nästan ett personalbyte innan. Som när det gäller vår posthanteringsprocess så får vi nog vänta i 5 år för då går den här personen i pension, sen kommer vi att kunna effektivisera den här processen. Man ska alltid vet att folk blir väldigt rädda vid förändringar, när man skakar om, när inte allting är som det brukar vara. När folk är osäkra, och då kan de bli lite aggressiva. Då måste man ha en organisation som tar hand om det här, den mjuka biten, det är allt förändringsarbete. Och har man båda de här bitarna kan man driva ett bra förändringsarbete där inte folk tar skada. Vissa förändringar är bättra att göra när folk slutar. Jag var ändå med när man knackade in fakturor och sen övergick vi till att scanna in alla fakturor. Och då hade man ju egentligen assistent.. , det var en arbetsuppgift hos assistenten att betala fakturorna. Idag har vi alltid kört den, regeln inom miljö/teknik att den som ger upphov till kostnad ska ta hand om kostnader, alltså för jobbet. Så går man ut och handlar spik eller rep eller något så får man ta omaket att kontrollera och kontera faktura som kommer innan man skickar den till den som budgetansvarig som är slutsteget där fakturan betalas. I vissa organisationer har man lagt den uppgiften på assistent, att hon gör den här kontrollen , vilket betyder att hon måste gå och prata med personen som har köpt in det här och då blir det en ineffektiv process. Vi har försökt minimera dem stegen i de olika processerna. Det är likadant när det gäller självservice av lönehanteringen, innan fyllde man i ett papper för semesterledighet eller man fyllde i att man hade övertid eller något sånt. Nu registrerar man allt det här på datorn, sen går det till av sig självt chefen så man inte behöver knappa någonting och sen betalas det ut direkt istället för flera personer som det här annars skulle gå igenom. Dels personalredogörare på miljö/teknik, dels vi lönekontoret, och sen skulle det vara någon knappade in allt det här och då har det varit lyckosamma projekt, och folk har varit rädda men i slutändan är det bra att man slipper alla dessa papprena nu. Vilket gör att den här interna kostnadshanteringen dramatiskt minskat, plus att det bli mer rätt lön till medarbetaren istället för att det var en massa grejer som släpade. Så det blir en bättre produkt till medarbetarna, så blir det mindre som lönekontoret ska rätta till.

Riskkategori	Risktyp	Beskrivning	Uppskattad sannolikhet (1-5)	Prioritering (1-10)	N/A Icke relevant
Naturkatastrof	Jordbävning, vulkanutbrott, tsunami	Skadad utrustning	1		N
Naturkatastrof	Storm	Strömavbrott, översvämning	5	2	
Naturkatastrof	Snöoväder	Hög belastning av verksamhetens infrastruktur	5	1	
Mänskligt orsakade katastrofer	Terrorism	Explosion	1		N
Mänskligt orsakade katastrofer	Cyberterrorism, Crackers	Dataskadegörelse	2	5	
Mänskligt orsakade katastrofer	Internetattack	Systemet överbelastas, offlineläge	2	4	
Mänskligt orsakade katastrofer	Sabotage	Dataförlust	1	8	
Mänskligt orsakade katastrofer	Social engineering, Hackers	Dataintrång	1	6	
Oavsiktliga eller tekniska katastrofer	Felanvändning	Ogiltig data	1	7	
Oavsiktliga eller tekniska katastrofer	Tekniskt konstruktionsfel	Systemhaveri	2	3	

Sen tror jag att IT-avdelningen håller allt det här tekniska för sig själva om det skulle vara någonting, så jag är inte så insatta i det.

10. Känner du till någon incident (systemhaveri) som har hänt på organisationen under de senaste 5 åren?
    g. Och i så fall hur hanterades det haveriet?
    h. Information om haveriet, vad orsakade haveriet och hur upptäcktes det?

Inget IT-baserat, vad jag känner till.

Bilaga 7 – Kategorisering

- Hur anställda involveras
    - Hur de prioriterar utbildningar
    - Om särskilda anställda prioriteras
    - Förhållande mellan anställda - ledning

- Hur de lägger upp åtgärdsplaner
    - Hur ofta de revideras
    - Vem sköter det
    - Hur ser processen ut
    - Omvärldskrav
    - Hotbild

- Riskprioriteringar
    - Scenarier
        - Största säkerhetshot
            - Konsekvenser
        - Teknisktberoende
            - Konsekvenser
        - Säkerhetsplaner
            - Säkringar av teknik
    - Matris
        - Hur de skiljer sig
        - Varför är/skulle det kunna vara så

Referenser

ABA. (1984): *Report on Computer Crime*. The Task Force on Computer Crime. American Bar Association. Section on Criminal Justice.

AICPA. (1984): *Report on the Study of EDP-Related Fraud in the Banking and Insurance Industries.* American Institute of Certified Public Accountants. Inc. New York.

Alvesson, M. & Deetz, S., (2000): *Kritisk samhällsvetenskaplig metod*, Studentlitteratur, Lund.

Arnum, E. (1995): Doing Business on the Internet-A Question of Balance. *Business Communications Review (25:8)*. August, s. 35-38.

Ball, L., and Harris, R. (1982): SMIS Member: A Membership Analysis. *MIS Quarterly (6:1)*. March, s. 19-38.

Blumstein, A., (1978*): "Introduction," in Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates,* A. Blumstein, J. Cohen och D. Nagin (eds.), National Academy of Sciences, Washington, DC.

Brancheau, J., and Weatherbe, J. C. (1987): Key Issues in Information Systems: 1986. *MIS Quarterly (11:1)*. March, s. 23-45.

Brancheau, J. C., Janz, B. D., and Wetherbe, J. C. (1996): Key Issues in Information Systems Management: 1994-95 SIM Delphi Results. *MIS Quarterly (20:2)*. June, s. 225-242.

Breivold H., Crnkovic I., Land R. & Larsson S. (2008): Using Dependency Model to support Software Architecture Evolution. *2008 23rd IEEE/ACM International Conference on Automated Software Engineering – Workshops*. IEEE.

Brodie, C. (2008): Importance of Security Awareness Training. *SANS Institute Reading Room*. Tillgänglig: http://www.sans.org/reading_room/whitepapers/awareness/importance-security-awareness-training_33013
Senast hämtad: 2011-04-20

Brown, R. O. (1993): *What* You Need to Know to Plan for Disaster. *Networking Management*, (11:4). April, s. 25-27.

Bryman, A., (2002): *Samhällsvetenskapliga metoder*, Liber, Malmö

Burger, K. (1993): The New Age of Anxiety. *Insurance & Technology (18:10)*. October, s. 48-54.

BusinessDictionary(2011):*Best practices*.
Tillgänglig: http://www.businessdictionary.com/definition/best-practice.html
Senast hämtad: 2011-06-13

Colton, K. W., Tien, J. M., Davis, S. T., Dunn, B., and Barnett, A. I. (1982a): *Computer Crime: Electronic Fund Transfer Systems and Crime*. U.S. Department of Justice. Bureau of Justice Statistics. Washington DC.

Colton, K. W., Tien, J. M., Davis, S. T., Dunn, B., and Barnett, A. I. (1982b): *Electronic Funds Transfer Systems and Crime*. U.S. Bureau of Justice Statistics. Washington DC.

Cummings E., Haag S. & McCubbrey D. (2005): *Management Information Systems for Information Age.* McGraw-Hill.

Day R. (1998): Leadership of fast track projects. *Aerospace Conference, 1998. Proceedings., IEEE*. IEEE.

Dickson, G. W., Leitheiser, R. L., Wetherbe, J. C., and Nechis, M. (1984): Key Information Systems Issues for the 80's. *MIS Quarterly (8:3).* September, s. 135-159.

Dixon, R., Marston, C., and Collier, P. (1992): Report on the Joint CIMA and IIA Computer Fraud Survey. *Computers & Security (11:4).* July, s. 307-313.

Flanagan, W. G., and McMenamin, B. (1992): The Playground Bullies are Learning How to Type. *Forbes*. 21 February, s. 184-189.

Forcht, K. (1992): Bolstering Your Computer's Immune System. *Security Management (36:9).* September, s. 134-140.

Forcht, K. A., (1994): *Computer Security Management*, Boyd & Fraser, Danvers, MA.

Försvarsmakten (2011): *Försvarsmaktens verksamhet, Nationell verksamhet*. Svenska Försvarsmakten.
Tillgänglig: http://www.forsvarsmakten.se/sv/Om-Forsvarsmakten/Verksamhet/
Senast hämtad:2011-05-18.

Gips, M. (1995*):* Tales of Woe. *Security Management (39:5).* May, s. 10.

Goodhue, D. L., and Straub, D. W. (1991): Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security Measures. *Information & Management (20:1).* January, s. 13-27.

Gopal, R., and Sanders, G. L. (1992): The Effect of Preventive and Deterrent Software Piracy Strategies on Producer Profits, *Proceedings of the Thirteenth International Conference on Information Systems*, J. I. DeGross, J. D. Becker, and J. J. Elam (eds.), Dallas, TX, s. 161-170.

Gopal, R. D., and Sanders, G. L. (1997): Preventive and Deterrent Controls for Software Piracy, *Journal of Management Information Systems (3: 4)*, s. 29-47.

Hartlog, C., and Herbert, M. (1986): 1985 Opinion Survey of MIS Managers: Key Issues. *MIS Quarterly*. (10:4). December, s. 351-361.

Heijden, K. van der (2005): *Scenarios. The art of strategic conversation*. Hoboken, N.J.: Wiley.

Hoffer, J. A., and Straub, D. W. (1989): The 9 to 5 Underground: Are You Policing Computer Crimes?. *Sloan Management Review (30:4)*. Summer, s. 35-44.

IT Governance Institute (2011), COBIT 4.1.
Tillgänglig: http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf
Senast hämtad: 2011-03-28

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

Jøsang A., AlFayyadh B., Grandison T., AlZomai M. & McNamara J. (2007): Security Usability Principles for Vulnerability Analysis and Risk Assessment. *Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007)*. IEEE.

Keil, M. (1995): Pulling the Plug: Software Project Management and the Problem of Project Escalation. *MIS Quarterly* (19:4). December, s. 421-447.

King, J. (1995,): Survey Finds Computer Fraud Often an Inside Job. *Computerworld, (29:12)*. March 20, s. 16.

Kusserow, R. P. (1983): *Computer-Related Fraud and Abuse in Government Agencies*. U.S. Depertment of Health and Human Services.

Latimer, M. (2011): *Combating e-Crime in a rapidly evolving digital market.* Annual Future of Security in Banking & Financial Services. March 2011. Suncorp.

Local Government Audit Inspectorate. (1981): *Computer Fraud Survey*. Department of the Environment, Bristol.

Loch, K. D., Carr H. H., and Warkentin, M. E. (1992): Threats to Information Systems: Todayís Reality, Yesterdaís Understanding. *MIS Quarterly (17:2)*, s. 173-186.

Martin, J., (1973): *Security, Accuracy, and Privacy in Computer Systems*, Prentice-Hall, Englewood Cliffs, NJ.

Martin, R. (2005): *Validity vs. Reliability: Implications for Management*. Rotman Magazine Publication date: Jan 01, 2005. Prod. #: ROT011-HCB-ENG
Tillgänglig: http://hbr.org/product/validity-vs-reliability-implications-for-managemen/an/ROT011-HCB-ENG

Morimoto S. (2009): Application of COBIT to Security Management in information Systems Development. *2009 Fourth International Conference on Frontier of Computer Science and Technology*. IEEE.

Neumann, P. G. (1994): Inside Risks. *Communications of the ACM (37:5)*. s. 146.

Niederman, F., Brancheau, J. C., and Wetherbe, J. C. (1991): Information Systems Management Issues for the 1990s. *MIS Quarterly (15:4)*. December. s. 475-495.

Oates, B. J., (2006): *Researching Information systems and Computing*. Sage, London

Panettieri, J. C. (1995): InformationWeek/Ernst & Young Security Survey. *InformationWeek*. 27 November.

Parker, D. B. (1976): *Crime By Computer*, Scribner's. New York.

Parker, D. B., (1981): *Computer Security Management*, Reston Publishing, Reston, VA.

Parker, D. B. (1983): *Fighting Computer Crime*, Scribner's. New York.

Peach, S. (1998*):* Disaster Recovery: An Unnecessary Cost Burden or an Essential Feature of Any DP Installation?. *Computers & Security (10:6)*. October. s. 565-568.

Pearson, F. S., och Weiner, N. A., (1985): Toward and Integration of Criminological Theories, *Journal of Crime and Criminology (76:1)*, s. 116-150.

Radovanović D., Radjević T., Lučić D. & Šarac M. (2010): IT audit accordance with Cobit standard. *The 33rd International Convention MIPRO*. IEEE.

Ridley G., Young J. & Carroll P. (2004): COBIT and its Utilization: A framework from the literature. *Proceedings of the 37th Hawaii International Conference on System Science*. IEEE.

Rittinghouse J., Ransome J. (2006): *Business Continuity and Disaster Recovery for InfoSec Managers*. Elsevier Inc.

Schwartz, M. (1990): Computer Security: Planning to Protect Corporate Assets. *Journal of Business Strategy (11:1)*; January – February. s. 38-41.

Simon, H. (1960): *The New Science of Management Decision*. Harper and Brothers. New York.

Siponen M., Willison R. (2009): Information Security Management Standards: Problems and solutions. *Information & Management*. (46:5).

Sjoholm, H. (1997a): *cracker*. SearchSecurity.com
Tillgänglig: http://searchsecurity.techtarget.com/definition/cracker
Senast hämtad: 2011-06-13

Sjoholm, H. (1997b): *hacker*. SearchSecurity.com
Tillgänglig: http://searchsecurity.techtarget.com/definition/hacker
Senast hämtad: 2011-06-13

Snedaker S. (2007): *Business Continuity and Disaster Recovery Planning for IT Professionals.* Elsevier Inc.

Stoneburner, G., Gougen, A., och Feringa, A. (2002): *Risk Management Guide for Information Technology Systems.* National Institute of Standards and Technology. Technology Administration U.S. Department of Commerce.
Tillgänglig: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
Senast hämtad: 2011-05-31

Stoneburner, G., Hayden, C., och Feringa, A. (2004): *Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A.* National Institute of Standards and Technology. Technology Administration U.S. Department of Commerce.
Tillgänglig: http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

Straub, D. W., and Widom, C. S. (1984): Deviancy by Bits and Bytes: Computer Abusers and Control Measures. *In Computer Security: A Global Challenge*, J. H. Finch and E. G. Dougall (eds.). Amsterdam. S. 431-442.

Straub, D. W. (1986a): Computer abuse and Computer Security: Update on an Empirical Study. *Security, Audit, and Control Review (4:2).* Spring. s. 21-31.

Straub, D. W. (1986b): *Deterring Computer Abuse: the Effectiveness of Deterrent Counter measuers in the Computer Security Environment.* Unpublished doctoral dissertation. Indiana University Graduate School of Business.

Straub, D. W., (1990): Effective IS Security: An Empirical Study, *Information Systems Research (1:3),* s. 255-276.

Straub, D. W., and Nance, W. D. (1990): Discovering and Disciplining Computer Abuse in Organizations: A Field Study. *MIS Quarterly* (14:1), March 1990, s. 45-62.

Straub, D. W., Carlson, P.J., and Jones, E. H. (1992): Deterring Highly Motivated Computer Abusers: A Field Experiment in Computer Security. *In IT Security: The Need for International Cooperation*, G. G. Gable and W. J. Caelli (eds.), Amsterdam, s. 309-324.

The Institute of Internal Auditors (2009): Case Studies of using GAIT-R to Scope PCI DSS Compliance. *EDPACS.* (39:1). Informaworld.

TheFreeDictionary, (2011): *Risker.*
Tillgänglig: http://www.thefreedictionary.com/Risker.
Senast hämtad: 2011-04-14.

Trost, J., (2005): *Kvalitativa intervjuer*. Studentlitteratur, Lund

Woodhouse S. (2008): An ISMS (Im)- Maturity Capability Model. *2008 IEEE 8th International Conference on Computer and Information Technology Workshops*. IEEE.

Åsblom J. (2011): Så påverkar krisen i Japan it-branchen. *IDG*, 2011-03-18.
Tillgänglig: http://mobil.idg.se/2.1085/1.374838
Senast hämtad: 2011-03-25