LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Informationssäkerhet i små och stora vårdorganisationer:

en jämförelsestudie mellan två organisationer

Kandidatuppsats 15 hp, kurs SYSK02 i informationssystem

Författare: Markus Dahlman Ström
David Hall

Handledare: Anders Svensson

Examinatorer: Odd Steen
Styliani Zafieroupolou

Slutseminarium: 2017/05/26

Informationssäkerhet i små och stora vårdorganisationer: En jämförelsestudie mellan två organisationer

Författare: Markus Dahlman Ström och David Hall

Utgivare: Inst. för informatik, Ekonomihögskolan, Lund universitet

Dokumenttyp: Kandidatuppsats

Antal sidor: 84

Nyckelord: Informationssäkerhet, riskhantering, IS-policy, säkerhetsmedvetande, vårdorganisationer

Sammanfattning (Max. 200 ord):

Informationssäkerhet inom vården är inget nytt område utan har spelat en stor roll inom vården under en längre tid. Att patientuppgifter och journaler ska vara skyddade mot allmänheten är något varje person tar för givet. Även om det inte är något nytt att skydda patienters uppgifter så ställs det ständigt nya krav på vården för att säkra att uppgifterna skyddas på ett adekvat sätt. Informationssäkerhet har dock fått en viktigare roll i vårdorganisationer då riskerna blivit fler och konsekvenserna blivit allvarligare. Då informationssäkerhet inom vården är ett brett ämne har vi valt att avgränsa oss till att inte fokusera på de tekniska aspekterna och fokusera på de organisatoriska aspekterna så som styrande dokument, utbildning och riskhantering istället. Undersökningen är gjord på en mindre och en större organisation för att finna skillnaderna i arbetssätten mellan organisationerna och för att sedan undersöka hur skillnaderna påverkar slutresultatet av deras informationssäkerhetsarbete. Resultatet pekar på att den stora vårdorganisationen har en djupare förståelse för informationssäkerhet och har implementerat flera verktyg och processer för att sköta arbetet med informationssäkerhet jämfört med den mindre organisationen. Resultatet visar dock att även om den stora organisationen har en djupare förståelse har de svårare att förankra delar av informationssäkerheten i organisationen och genomföra säkerhetsarbetet i praktiken. Vi uppmuntrar vidare forskning kring ämnet och att då använda flera företag i undersökning för att då möjliggöra generalisering över branschen.

Innehåll

Figurer

Tabeller

Ordlista:

ISP - Informationssäkerhetspolicy.

ISA - Information security awareness.

IVO - Inspektionen för Vård och Omsorg.

SUS - Skånes universitetssjukhus.

MSB - Myndigheten för Samhällsskydd och Beredskap.

PUL - Personuppgiftslagen.

1 Introduktion

1.1 Bakgrund

Informationssäkerhet är en av de största utmaningarna för många organisationer, detta eftersom riskerna kan ha stora konsekvenser inte bara ur det lagliga perspektivet där det kan orsaka monetär skada utan även ur ett trovärdighetsperspektiv (Cavusoglu, Mishra, & Raghunathan 2004). Detta har gjort att säkerhet, speciellt informationssäkerhet, har fått ökad betydelse och hanteras nu direkt av högsta ledningen (Ernst & Young 2008). Tidigare har företag försvarat sig mot säkerhetsrisker genom att endast investera i teknologiska försvarsmekanismer såsom brandväggar, antivirus, mjukvarusäkerhet och kryptering (Siponen, 2005). Vance, Siponen & Pahnila (2012) säger att även då dessa verktyg hjälper till att säkra informationen så är de inte rekommenderat att förlita sig fullständigt (eller allt för mycket) på att dessa verktyg ska eliminera alla risker. Enligt Symantec (2010) finns det empiriska och anekdotiska undersökningar som visar på att antalet incidenter relaterade till informationssäkerhet ökar även hos de företag som har investerat mer i tekniska säkerhetslösningar.

Enligt Ejenäs (2012) är sjukvården en av de mest informationsintensiva branscherna och att utvecklingen av vårdorganisationer kommer att medföra att det behöver göras större eller annorlunda arbete för att hålla information säker och säkerställa sekretessen. Ejenäs (2012) menar också att hantering av säker data inte är någon nytt inom vården men att det kommer att få mer fokus och relevansen kommer öka i takt med att både vården effektiviseras och att kvaliteten och tillgängligheten ökar.

1.2 Problemområde

Organisationer inom vård och omsorg är livsviktiga för dagens samhälle. De är en av stöttepelarna i samhället som tar hand om människor som har ett behov av vård, men för att fungera så är de beroende av att ha tillgång till nödvändig information. Med tiden så har informationshantering för organisationer inom vård och omsorg blivit allt mer komplex och bredare då vårdgivare skaffar sig nya informationssystem som ska integreras med befintliga system och med olika externa tjänster (MSB, 2014). Bara under det senaste årtiondet så beskriver Black et. al. (2011) att många och stora satsningar på digital teknik, e-hälsa och IT skett inom vården.

Black et. al. (2011) forstätter att beskriva att med den stora satsningen så är det viktigt att se till att de nya IT-lösningarna är säkra. MSB, NCSC & BSI (2014) genomförde en fallstudie där de undersökte tre incidenter gällande cybersäkerhet. I slutet av studien pratade de om

vilka lärdomar man kan ta med sig av dessa fallen. En av lärdomarna de beskrev var hur ny teknologi kan skapa nya möjligheter för vårt samhälle, men att de kan även medföra nya risker (MSB, NCSC & BSI, 2014). Vidare beskriver MSB, NCSC & BSI (2014) att nya affärslösningar och teknologier gör att koncentrationen av information i samhället ökar. MSB, NCSC & BSI (2014) hävdar att den ökade koncentrationen av information kan i samband med andra faktorer såsom ökad integration och nya verksamhetsformer, leda till att tekniska fel kan stänga ner ett antal funktioner i samhället under en kort period.

Under 2015 behandlades 390 700 personer av den kommunala hälsosjukvården (Socialstyrelsen, 2016), däremot finns det ingen statistik över hur många som behandlades av privata vårdgivare. För att ta två exempel så används Lunds och Malmös kommun. I Lunds kommun behandlades i genomsnitt cirka nio personer varje dag och cirka 65 personer varje vecka (Socialstyrelsen, 2016). Malmö behandlade i genomsnitt cirka 37 personer varje dag och cirka 263 personer varje vecka (Socialstyrelsen, 2016). Hade någon av dessa kommuner därför upplevt nedsatt förmåga att behandla patienter tack vare tekniska fel så är det rimligt att anta att det hade kunnat få allvarliga konsekvenser för patienterna.

MSB (2014) tog fram en strategi för stärkt informationssäkerhet inom vård och omsorg 2014 där de säger just att bra informationssäkerhet är viktig för att undvika risker med IT-lösningar.

> *"Informationssäkerheten är dessutom en förutsättning för att IT-lösningar ska kunna utnyttjas med full nyttoeffekt utan att det skapar oacceptabla risker."* (MSB, 2014, sid 1)

I MSB (2015) undersökning om uppföljning av informationssäkerhet i vården så uppfattar de dock att informationssäkerhetsarbetet är lågt prioriterat hos de vårdgivare som deltog i undersökningen, även om det fanns undantag. Vidare säger MSB (2015) att vårdgivarnas informationssäkerhetsarbete är mer motiverat av att uppnå lagkrav än att faktiskt generera någon nytta för organisationen. Detta pekar på att den strategi som togs fram 2014 hittills inte varit effektiv i att förbättra informationssäkerheten hos organisationer inom vård och omsorg. Vidare bevis för att informationssäkerheten är bristfällig inom vården är att cyberattacken som benämns som Cloud Hopper, som under flera år lyckades ta del av känslig och sekretessbelagd information utan att upptäckas (MSB, 2017).

Cert-se som är Sveriges "Computer Security Incident Response Team" och jobbar med att hantera och förebygga IT-incidenter rapporterade den femte april 2017 att ett omfattande internationellt cyberangrepp genomförts av hackare baserade i Kina och att Sverige var ett av landen som var påverkade (MSB, 2017). Cyberangreppet som benämns som "Cloud Hopper" siktade in sig på ett antal olika samhällssektorer såsom bl.a. sjukvård och tros ha pågått sedan 2014 (MSB, 2017). Angreppen skedde genom intrång hos olika driftleverantörer för att sedan ta sig vidare till deras kunder och samla in information om dem. Syftet med detta var att kartlägga organisationer och deras anställda noggrant för att sedan lura anställda att öppna infekterade bilagor i email som sprider farlig kod ut i systemet (MSB, 2017; Berger, E. 2017). I en Intervju med SVT berättar Robert Jonsson som är ställföreträdande chef på Cert-se att människan är den svaga länken i detta fallet och att det inte är mailsystemet i sig som är osäkert. (Berger, 2017).

"Vad de gör är att formulera sina brev på ett så skickligt sätt att man luras att öppna det, så egentligen är den svaga länken människan – det skulle inte spela någon roll om systemet var säkrare." (Robert Jonsson i Berger, 2017)

Till BBC (2017) uppger Dr Adrian Nish som är chef för IT-säkerhet hos BEA Systems, som var en av aktörerna ansvariga för att avslöja cyberattacken, att både stora och små organisationer förlitar sig på att driftleverantörer hanterar deras kärnsystem vilket gör att leverantörerna får tillgång till känslig data. Små organisationer har ofta både mindre tid och resurser att lägga på säkerhet (Gupta & Hammond, 2005). Vidare säger Gupta & Hammond (2005) att små organisationer är mer benägna att välja teknologiska lösningar som inte passar in i just deras miljö vilket gör dem utsatta för säkerhetshot. När det gäller stora organisationer istället så påstår Hove et. al. (2014) i sin undersökning om incidenthantering inom informationssäkerhet hos stora organisationer att stora organisationer ofta har processer och planer på plats för att hantera informationssäkerhet men att de inte alltid är väletablerad i hela organisationen. Vidare hävdar Hove et. al. (2014) att utmaningar som stora organisationer stöter på gällande informationssäkerhet gäller anställdas *säkerhetsmedvetande, rapportering, kommunikation, informationsinsamling och spridning samt fördelning av ansvar*.

1.2 Forskningsfråga

Vilka skillnader finns det mellan stora och små vårdorganisationer gällande hantering av Informationssäkerhet?

1.3 Syfte

Läser man om informationssäkerhet inom vård och omsorg idag så ser man att det finns brister inom många områden. Syftet med undersökningen är därför att jämföra om informationssäkerhetsarbetet skiljer sig mellan stora och små vårdorganisationer och hur skillnaderna påverkar slutresultatet av deras informationssäkerhetsarbete.

1.4 Avgränsningar

Denna forskningen har som inriktning att fokusera på organisatoriska säkerhetsaspekter och kommer därför inte ta upp tekniska aspekter såsom kryptering, virusskydd, brandväggar och liknande. Undersökningen tar inte heller hänsyn till om organisationerna tillhör offentlig eller privata sektorn.

I vår undersökning samlar vi bara in data från en större och en mindre organisation. Det gör att resultatet av undersökningen inte kan generaliseras över liknande organisationer i branschen, utan kan som bäst ge en indikation av typiska problem för den större respektive mindre organisationen.

2 Litteraturgenomgång

2.1 Informationssäkerhet

MSB (2015, sid 10) definierar informationssäkerhet som "tillstånd som innebär skydd med avseende på konfidentialitet, riktighet, tillgänglighet och spårbarhet hos information". Vidare förklarar MSB (2015) att informationssäkerhet handlar om att uppfylla krav, normer och mål angående informationens tillgänglighet, konfidentialitet och spårbarhet.

Tillgänglighet: Handlar om att informationen ska vara tillgänglig till den som behöver den inom önskad tid och i förväntad utsträckning (MSB 2015).

Konfidentialitet; Syftar på att informationen inte bryter mot några lagkrav eller överenskommelser och riktlinjer när den görs tillgänglig för någon, att ingen obehörig får tillgång till informationen (MSB 2015).

Riktighet: Är att ingen obehörig kan förändra informationen eller förstöra den (MSB 2015).

Spårbarhet: Handlar om att aktiviteter och händelser i efterhand kan spåras till ett objekt eller en användare för att svara på frågorna vem, vad och när (MSB 2015).

I dagens företagsklimat använder sig företag och organisationer sig alltmer av IS-system (Informationssystem) för att hålla sig konkurrenskraftiga. Där ett bra IS-system kan tillhandahålla ledningen med bättre information så att de kan fatta bättre beslut och utforma bättre affärsstrategier. Den ökade betydelsen av IS-system för företag betyder även att säkerhetsbrister i systemen får en större påverkan, vilket leder till att vikten av Informationssäkerhet ökar. Möjliga konsekvenser av säkerhetsbrister kan vara allt från finansiella förluster till dålig publicitet och tappade konkurrensfördelar (Kankanhalli et. al. 2003).

IS-säkerhet kan säkerställas genom en rad av olika aktiviteter som ledningen kan välja att använda sig av. Bland de vanligaste säkerhetsåtgärder är att ha någon form av "Media back-up", virusskydd och brandväggar. (Whitman, 2003). Hu, Hart & Cooke (2007) påpekar dock att trots att företag lägger allt mer pengar på att utveckla nya teknologier och mjukvaror för att motarbeta säkerhetshot så är det ofta andra faktorer utgör de största hoten, såsom sina egna anställda, befintliga eller obefintliga IS-policys och företagets egna säkerhetskultur.

Litteraturen understryker även vikten av att ledningen involveras och tar informationssäkerhet på allvar (Kankanhalli et. al. 2003; Hu et. al. 2007). Annars finns risken att om ledningen inte tar det på allvar så ökar chansen att deras anställda kommer följa deras exempel och inte heller göra det, vilket gör de anställda till säkerhetshot (Puhakainen & Siponen, 2010). Kankanhalli et. al. (2003) säger att det har upptäckts att organisationer med bra stöd av ledningen använder sig i större utsträckning av förebyggande medel än organisationer där ledningen inte involverar sig lika mycket. vidare påpekar Kankanhalli et. al. (2003) att det är även ledningens ansvar att de krav som ställs på organisationen uppfylls. Kraven som ställs på ledningen

kommer bl.a. i form av lagar och reglerar hur arbetet med sekretessbelagd- och känslig information ska hanteras (SFS: 2008:355. Patientdatalag; SFS 1998:204. Personuppgiftslag; SFS: 2009:400. Offentlighets- och sekretesslag).

2.2 Lagar

Organisationer som bedriver sin verksamhet inom hälso- och sjukvården regleras av en stor mängd lagar, förordningar och föreskrifter (Vårdförbundet, 2017). Då vår uppsats fokuserar på informationssäkerhet fokuserar vi främst på patientdatalagen, personuppgiftslagen och offentlighets- och sekretesslagen.

2.2.1 Patientdatalagen

Patientdatalagen innehåller de regler organisationer inom hälso- och sjukvården måste följa när de behandlar patienters personuppgifter (SFS: 2008:355. Patientdatalag). En av de större delarna som patientdatalagen reglerar är när det är tillåtet för vårdgivare att använda sig av sammanhållen journalföring (SFS: 2008:355. Patientdatalag). Sammanhållen journalföring gör att vårdgivare kan under vissa förutsättningar, få tillgång till personuppgifter som hanteras av andra vårdgivare (Datainspektionen, 2017). Andra delar som lagen reglerar är den inre sekretessen (reglering som sätter krav på åtkomstkontroll och behörighetstilldelning till patienters uppgifter), patientens rätt att spärra tillgång till sina uppgifter i vårdgivarnas journalsystem samt för vårdgivare som använder sig av sammanhållen journalföring och ger vårdgivarna möjligheten att ge patienten direktåtkomst till sin vårddokumentation och dess olika loggar (SFS: 2008:355. Patientdatalag).

2.2.2 Personuppgiftslagen (PuL)

Av organisationer som hanterar personuppgifter kräver PuL att dessa säkerställs och skyddas på ett bra sätt. Det innebär att organisationer skall använda sig av lämpliga organisatoriska och tekniska säkerhetsåtgärder för att säkerställa personuppgifterna. Exempel på organisatoriska åtgärder är instruktioner för de anställda, policyer och rutiner medan tekniska åtgärder kan vara antivirus mjukvara, krypteringsfunktioner och brandväggar. PuL säger även att det som huvudregel krävs godkännande av den registrerade person för att få lagra hens information, dock finns det undantag till denna regel. Särskilda undantag finns gällande myndigheters register av personuppgifter, exempelvis för sjukvården och polisen. Även när behandling av personuppgifterna är nödvändiga för att ett avtal med den berörda personen ska kunna fullgöras, för att skydda den berörda personens vitala intressen eller om behandling av uppgifterna är nödvändiga i samband med någon myndighetsutövning. (SFS 1998:204. Personuppgiftslag)

Enligt PuL finns det vissa begränsningar för hantering av vissa typer av personuppgifter som kan ses som extra känsliga. I lagen räknas uppgifter gällande personens ras/etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i någon fackförening och

deras sexualliv och hälsa som känsliga uppgifter. Det kan även hända att personuppgifter som normalt sett är harmlösa, kan bli känsliga beroende i vilket kontext de förekommer i. Till exempel personuppgifter inom inkasso eller kreditupplysning, uppgifter om vård inom socialtjänsten eller om ekonomisk hjälp, samt personliga uppgifter som hanteras inom bankförsäkringsväsendet ses normalt sett som känsliga uppgifter (SFS 1998:204. Personuppgiftslag.).

Enligt Datainspektionen (Datainspektionen, 2017) finns det även ett antal frågor man bör ställa sig när man ska bedöma hur pass integritetskänsliga uppgifter är. Är svaret ja på någon av frågorna nedan bör personuppgifterna skyddas av mer omfattande säkerhetsåtgärder. Frågorna lyder:

- Omfattas uppgifterna av tystnadsplikt eller sekretess enligt offentlighets- och sekretesslagen eller annan lagstiftning?
- Omfattas behandlingen av någon särlagstiftning, till exempel patientdatalagen eller lagen om behandling av personuppgifter inom socialtjänsten, kriminalvården, med flera?
- Är det uppgifter om lagöverträdelser?
- Är det uppgifter om enskildas personliga förhållanden?

Beroende på hur personuppgifter sparas så gäller olika regler i PuL. Personuppgifterna kan antingen ses som strukturerade eller ostrukturerade och för strukturerad lagring av personuppgifter gäller betydligt fler regler. Sparas uppgifter i något typ av register eller i en databas där man kan söka och sammanställa personuppgifter så anses de vara strukturerade. Medan om uppgifterna finns i en löpande text så anses de vara ostrukturerade (SFS 1998:204. Personuppgiftslag.).

2.2.3 Offentlighets- och sekretesslagen

Offentlighets- och sekretesslagen reglerar myndigheters och andra organs hantering vid registrering, utlämnande och annan hantering av allmänna handlingar. Lagen innehåller även bestämmelser om tystnadsplikt och sekretess vilket är väldigt förekommande inom hälso- och sjukvården (SFS: 2009:400. Offentlighets- och sekretesslag).

Enligt denna lag så gäller sekretessen för alla uppgifter inom hälso- och sjukvården som handlar om en enskild persons hälsotillstånd eller andra personliga förhållanden. Dock så omfattas uppgifterna inte av sekretess om det står klart att uppgifterna kan avslöjas utan att personen uppgifterna handlar om eller någon av dess närstående lider men av detta (SFS: 2009:400. Offentlighets- och sekretesslag.).

Lagen innehåller även regler om sekretess gällande sammanhållen journalföring, Omprövning och tillsyn, patientnämndsverksamhet, omhändertagande av patientjournal, sekretess i förhållande till den vård- eller behandlingsbehövande och anmälningar (SFS: 2009:400. Offentlighets- och sekretesslag.).

2.3 Mindre vs. större vårdorganisationer

Oavsett storlek på sin organisation så behöver alla organisationer följa samma lagar och tackla frågan om IS-säkerhet. Straub (refererad i Kankanhalli et. al. 2003, 143) beskriver att storleken på organisationen ofta avgöra hur mycket resurser man har att lägga på IS-säkerhet. Det gör att det är troligare att större organisationer lyckas skaffa sig rätt kompetens för att skydda sig och använder sig oftare av avskräckande medel jämfört med mindre organisationer (Kankanhalli et. al. 2003). Avskräckande medel är säkerhetslösningar som är designade att minska troligheten att säkerhetsbrister uppstår från första början, alltså sådant som ska förebygga säkerhetsbrister (Straub, 1990). Vidare ger Straub (1990) exempel på avskräckande medel såsom riktlinjer för användning av IS-tillgångar, IS-policys, straffgenomgångar och utbildning av anställda i informationssäkerhet.

Just kompetens är en viktig bit som mindre organisationer ofta saknar (Thong, Yap, & Raman, 1996). Det leder till att det finns en risk att de inte implementerar sina IS-lösningar på bästa sätt, vilket i sin tur leder till både säkerhetsbrister samt att de inte får ut alla fördelar som IS-lösningen skulle kunna bidra med (Thong, Yap, & Raman, 1996). Det ökar också risken för att de väljer helt fel IS-lösning från första början (Gupta & Hammond, 2005). Vidare säger Gupta & Hammond (2005) att även här så spelar resursbrist en stor roll, mindre organisationer väljer lösningar de har råd med även om de inte är den lösning som passar dem bäst.

Brist på kompetens inom informationssäkerhet gör också så att mindre organisationer ofta prioriterar hotbilder fel. I Gupta & Hammonds (2005) studie om informationssäkerhetsproblem i mindre organisationer visar resultatet att mindre organisationer ser virus som det största hotet, medan “insider access abuse” ses som det minsta hotet mot organisationen trots att det är den vanligaste typen av IT attacker. Gupta & Hammonds (2005) resultat visar även att bara runt 40,5% av de små organisationer som undersöktes i studien hade en informationssäkerhetspolicy på plats, jämfört med Hove et. al. (2014) undersökning där alla stora organisationer hade en på plats. Då en informationssäkerhetspolicy är ett viktigt kontrollverktyg för organisationer (Alshaikh, 2016) gör det att organisationer utan en går miste om en möjlighet att förbättra sitt informationssäkerhetsarbete.

2.4 IS-policy

En ISP (Informationssäkerhetspolicy) är ett dokument som används för att informera anställda om vad som är tillåtet och inte tillåtet att göra med informationen som finns i företaget. Whitman et al. (refererad i Bulgurcu et. al. 2010) beskriver att syftet med en ISP är att ge de anställda riktlinjer över hur de kan hålla informationen de arbetar med säker när de jobbar med olika IS-system. Förutom att berätta vad anställda får och inte får göra så bör en ISP även berätta vad som händer om de anställda inte följer dessa regler (Bulgurcu et. al. 2010). Är de anställda medvetna om vad konsekvenserna blir om de bryter mot reglerna så ökar deras foglighet gentemot ISPn (Puhakainen & Siponen, 2010).

ISP:s kan delas upp i två grupper beroende på vilken abstraktionsnivå de utgår ifrån (Baskerville & Siponen, 2002). Vidare förklarar Baskerville, & Siponen (2002) att ISP:s som har en hög abstraktionsnivå behandlar övergripande säkerhetsmål som angår hela organisationen och definierar allmänt vilket ansvar som ledningen och de anställda har. ISP:s som har en låg abstraktionsnivå följer den övergripande policyn och beskriver mer detaljerat vad varje anställd har för ansvar, t.ex. att en anställd måste ändra sitt lösenord var fjärde månad samt att det måste vara minst åtta tecken långt (Baskerville & Siponen, 2002).

Whitman (2003) anser att en säkerhetspolicy är en av det viktigaste delarna i arbetet med informationssäkerhet då den formar organisationens synpunkt på informationssäkerhet och hjälper till att definiera säkerhetskulturen inom organisationen. Dock så visar det sig i Whitmans (2003) undersökning att bara runt 60% av företagen använder sig av en säkerhetspolicy vilket leder till att de andra företagen utsätter sig automatiskt för säkerhetsrisker.

Det går dock inte att ta fram en säkerhetspolicy och anta att anställda kommer följa den automatiskt (Puhakainen & Siponen, 2010). Istället menar Puhakainen & Siponen (2010) att för att säkerställa att policyn följs bör ledningen vara involverad vid framtagningen av den, promota den inom organisationen och föregå med gott exempel för de anställda. Bulgurcu et. al. (2010) påpekar även att belöningar för anställda som följer IS-policyn kan bidra till deras attityd gentemot IS-säkerhet ändras till det bättre. Denna attitydändring är viktig för ledningen att sträva efter för att påverka de anställdas ISP-compliance (Siponen et. al. 2014).

2.5 ISP compliance

ISP compliance beskriver hur villiga de anställda är att följa organisationens ISP samt även hur väl de faktiskt följer ISPn (Bulgurcu et. al. 2010). Skulle de anställda inte följa de framtagna ISP:s så tappar organisationens säkerhetslösningar sin effektivitet, vilket gör att det är viktigt för en organisation att upprätthålla en hög grad av anställdas ISP compliance (Backhouse & Dhillon, 2001).

I litteraturen ses anställda ofta som en svag punkt i IS säkerhet (Warkentin & Willison 2009; Siponen, 2000a; Bulgurcu et. al. 2010; Siponen et. al. 2014), därför är det viktigt för ledningen att veta vilka faktorer som motiverar en anställd att följa ISPn. Följer den anställda organisationens ISP till en hög grad minskar chansen att denna begår säkerhetsbrott (Bulgurcu et. al. 2010). I Bulgurcu m.fl. (2010) undersökning om informationssäkerhetsmedvetande kom de fram till sju faktorer som påverkar en anställds ISP compliance. Faktorerna är *säkerhet, sårbarhet, arbetsbelastning, belöningar, verklig kostnad, verklig fördel och sanktioner/påföljder*. Kan ledningen tillfredsställa dessa faktorer på ett bra sätt ökar de anställdas ISP compliance (Bulgurcu et. al. 2010).

En anställds grad av ISP compliance påverkas även av deras attityd mot informationssäkerhet och deras normer (Bulgurcu et. al. 2010). Därför bör stor vikt läggas på att utbilda de anställda där man går igenom organisationens ISP och tydligt meddelar vilka påföljder brott mot ISPn får (Puhakainen, P & Siponen, M. 2010). Motiverar man inte varför en anställd bör

följa ISPn och vilka konsekvenser det kan få för organisationen så är det inte troligt att deras attityd kommer att ändras till det bättre (Siponen, 2000b). Utöver detta bör det även finnas en kontinuerlig kommunikation mellan ledningen och de anställda för att säkerställa de anställdas ISP compliance (Puhakainen & Siponen, 2010).

När anställda anser att ISP compliance hindrar deras vanliga arbetsuppgifter och därför inte följer den utsatta ISPn, har det visat sig att ISA (information security awareness) kan motarbeta denna åsikt (Bulgurcu et. al., 2010). Vidare påstår Bulgurcu et. al. (2010) att det gör att ISA kan direkt påverka ISP compliance.

2.6 Informationssäkerhetsmedvetande

Informationssäkerhetsmedvetande (ISA) handlar om hur medvetna användare i en organisation är av säkerhetsrisker gällande sin informationshantering (Siponen, 2000b). ISA kan delas upp i två dimensioner, ISP awareness samt allmän ISA (Bulgurcu et. al. 2009). Bulgurcu et. al. (2009) fortsätter med att beskriva att ISP awareness handlar om den anställdas förståelse och kunskap om kraven som finns i organisationens ISP och vad kraven avser att uppnå.

Allmän ISA definieras som en anställds övergripande förståelse och kunskap angående problem som har med informationssäkerhet att göra, samt vilka påföljder dessa problem kan få (Bulgurcu et. al. 2009). Dimensionerna skiljer sig genom att med allmän ISA så kan en anställd förstå att tvånget av att ha ett lösenord är en nödvändig säkerhetslösning, medan ISP awareness gör att den anställda förstår att lösenordet måste ha ett visst antal karaktärer och bytas ut regelbundet (Bulgurcu et. al. 2009).

En bra ISA är viktig då säkerhetslösningar och tekniker kan missuppfattas, missbrukas eller helt enkelt inte användas av användarna vilket gör att lösningarna förlorar sitt värde (Straub, 1990). Det organisationen får ut av en högre grad av ISA är att effektiviteten av säkerhetslösningar och motåtgärder ökar, då användaren inser hur och varför dessa används (Siponen, 2000b).

Målet med att skapa ISA hos sina anställda är att göra de medvetna om riskerna som finns angående informationssäkerhet och att utbilda dem om vilket ansvar och roller de själva har angående dessa risker. ISA gör att de anställda upplever att kraven som ställs på dem genom ISPn uppfattas som rättvisare (Bulgurcu et. al. 2009). Detta får en positiv effekt på deras attityd gentemot ISP compliance, vilket i sin tur minskar antalet säkerhetsbrott som begås av anställda (Bulgurcu et. al. 2010). Siponen (2000b) lyfter dock fram att det inte går att anta att en anställd efter en säkerhetsutbildning kommer börja följa alla riktlinjer i ISPn direkt, utan att det sker gradvis och bör ses som ett långsiktigt mål.

Anställdas ISA kan även påverkas av andra faktorer än utbildningen på jobbet (Bulgurcu et. al. 2009). Deras egna livserfarenheter kan påverka, om en anställd blivit utsatt för virus eller fått någon email hackad i privatlivet kan den erfarenheten bidra till att forma den anställdas

ISA (Bulgurcu et. al. 2009). Sedan kan även externa källor bidra, såsom olika tidningar, journaler och artiklar (Bulgurcu et. al. 2009).

2.7 Riskhantering

Riskhantering är en viktig del av informationssäkerhet (Zhang. et. al. 2010; MSB, 2015). Organisationer i dagens samhälle utsätts alla för olika sorters risker i sin dagliga verksamhet (Blakley, McDermott & Geer, 2002) och måste hantera dessa på ett bra sätt för att hindra att riskerna orsakar finansiella förluster, skador på företagets image, och stöld eller förlust av information (Humphreys, 2008). MSB (2015) säger att det är därför viktigt organisationers informationsstyrning utgår från en generell riskhantering av information samt att man använder sig av riskbaserade kravställningar och uppföljningar av verksamhetskritisk information. För att lyckas med detta är det därför är det viktigt att ledning ser till att det finns processer för riskhantering förankrade och spridda i organisationen, samt att det även finns interna kontroller som stödjer dessa processer (Humphreys, 2008). Vidare förklarar Humphreys (2008) att Riskanalysprocesser är till för att upptäcka och verifiera både tekniska och organisatoriska sårbarheter i olika system så att man sedan kan bestämma åtgärder för att minska riskerna som de sårbarheterna genererar.

För att utvärdera risker bör man identifiera hot, sina tillgångar och vart man som organisation är sårbar. När man identifierat dessa kan man sedan räkna ut sannolikheten att något av de hot man tidigare identifierat utnyttjar organisationens sårbarheter, samt även vilken risknivå riskerna ligger på, alltså hur allvarliga riskerna är (Humphreys, 2008).

Figur 1, Riskhanteringsmodell (Humphreys, 2008, sid 249)

Det finns flera olika ramverk och standarder för riskhantering där ISO/IEC 27001 är den som är mest välkänd internationellt (Disterer, 2013). I ISO/IEC 27001 beskrivs fyra olika lösningar för hur organisationer kan hantera risker som de identifierat (Humphreys, 2008) medan Blakely et. al. (2002) beskriver ytterligare lösningar:

- Undvika risken helt och hållet genom att undvika eller ändra den aktivitet som risken associeras med.
- Överföra risken till försäkringsbolag genom försäkringar eller om man outsourcar aktiviteten som orsakar risken till en tredje part.
- Minskar risken genom att implementera interna kontroller i organisationen.
- Accepterar att risken finns och tar ett aktivt val att inte åtgärda den.
- Att man går samman med flera organisationer och delar kostnaden om risken skulle bli verklighet.

Efter att man har valt hur man ska hantera riskerna så kommer man till nästa fas inom riskhantering, uppföljnings och övervakningsfasen (Humphreys, 2008). Här förekommer det återkommande granskningar av riskerna. Det görs för att omvärlden och organisationen ständigt förändras vilket gör att även riskernas natur kan ändras (Humphreys, 2008). Det kan leda till att riskens risknivå ökas och upptäcks inte det av organisationen så kan de råka illa ut (Humphreys, 2008). Upptäcks det någon ny risk eller en förändring kring någon av de redan upptäckta riskerna kan organisationen då vara tvungen att ta till nya åtgärder eller justera de befintliga åtgärder som organisationen använder sig av (Humphreys, 2008).

2.8 Teoretiskt ramverk

I tabellen nedan visas det teoretiska ramverk som tagits fram och sedan utgåtts från under undersökningen. Ramverket är baserat på de tidigare teorikapitel som finns i uppsatsen och är till för att hjälpa oss att strukturera undersökningen. Under litteraturgenomgången dök ett antal olika teoretiska områden inom informationssäkerhet upp flera gånger vilket ledde till att vi fokuserade på dessa under vår undersökning. I de utvalda teoretiska områdena identifierades elva viktiga punkter som vi valt att basera vår undersökning kring. De viktiga punkterna utgör sedan grunden för de frågor vi försöker svara på i resultatdelen. Ett eget ramverk utvecklades då informationssäkerhet innefattar så många olika områden. Vi behövde därför avgränsa vår undersökning och det teoretiska ramverket användes som ett verktyg för att göra detta.

Tabel 1: Teoretiskt ramverk.

Teori	Litteratur	Viktiga punkter
Mindre vs. Större Vårdorganisationer	Straub, 1986. Straub, 1990. Kankanhalli et. al. 2003. Thong, Yap, & Raman, 1996. Gupta & Hammond, 2005. Hove et. al. 2014. Al-shaikh, 2016.	• Resurser • Kompetens
IS-Policy	Whitman et al. 2001. Whitman, 2003. Puhakainen & Siponen, 2010. Baskerville & Siponen, 2002. Bulgurcu et. al. 2010. Siponen et. al.	• Konsekvenser av regelbrott • Abstraktionsnivå • Involverad ledning
ISP-Compliance	Bulgurcu et. al. 2010. Backhouse & Dhillon, 2001. Warkentin & Willison 2009. Siponen, 2000a. Siponen, 2000b. Puhakainen & Siponen, 2010. Siponen et.	• Anställdas attityd
ISA	Siponen, 2000b. Bulgurcu et. al. 2009. Straub, 1990. Bulgurcu et. al. 2010	• Göra anställda medvetna om risker och ansvar
Riskhantering	Blakley, 2002. Humphreys, 2008. Zhang. et. al. 2010. MSB, 2015. Disterer, 2013	• Standarder och ramverk • Hantering av risker • Uppföljning • Övervakning

3 Metod

3.1 Metodval

För att genomföra vår studie har vi valt att använda oss av en kvalitativ ansats. En kvalitativ ansats lämpar sig när man vill skapa klarhet i vad som ligger bakom ett begrepp eller fenomen (Jacobsen, 2002). Eftersom vi vill samla in detaljerad data som tillåter en djupare diskussion och analys kring de olika teoriområdena som finns i ramverket passar en kvalitativ ansats oss bra. Den låter oss även använda oss utav semi-öppna intervjuer från färre respondenter än om vi hade använt oss av en kvantitativ ansats. Att kunna genomföra semi-öppna intervjuer var viktigt för vår studie då vi vill att studiens resultat ska spegla organisationernas verklighet utan att våra fördomar om dem påverkar resultatet. Med denna typ av intervjustruktur ger vi intervjuobjekten möjligheten att använda sina egna ord och tankar så att de kan beskriva verkligheten ur sina egna perspektiv istället för att tvinga fram det resultat som vi tror att det kommer bli.

Som strategi för att samla in empiri använder vi oss av en deduktiv strategi. Jacobsen (2002) förklarar att deduktiva angreppssätt går ut på att forskarna skaffar sig vissa förväntningar av hur resultatet av studien kommer att se ut och sedan gå ut och samlar på sig empiri som stödjer de förväntningar. Medan det induktiva angreppssättet förespråkar att man ska undersöka situationen helt utan förväntningar, samlar på sig all information som kan vara relevant för studien och sedan kategoriserar den data de samlat in (Jacobsen, 2002). I vårt fall så har vi valt att läsa litteratur om området innan vi samlat in empiri vilket leder automatiskt till att vi skaffar oss vissa förväntningar av resultatet.

3.2 Urval

Hu et. al. (2007) menar att en av utmaningarna när man ska utföra en studie är att hitta organisationer och personer som är villiga att ställa upp och diskutera information som kan vara känslig. Generellt är både organisationer och individer inte väldigt intresserade att berätta om säkerhetsbrister då det i sig är en risk (Hu et. al. 2007). Vidare säger Hu et. al. (2007) att denna information kan både skapa ett dålig anseende och exponera svagheter som kan bli utnyttjande. En organisation vill vanligtvis projicera en positiv bild även om verkligheten inte stämmer (Hu et. al. 2007).

Gupta & Hammond, (2005) säger att ett av problemen när man undersöker organisationer som ska ha en viss storlek, är frågan om hur man ska definiera storleken. Vidare förklarar Gupta & Hammond, (2005) att i sin studie har de valt att definiera små organisationer som

organisationer med mindre än 500 anställda. Hove et. al. (2014) har i sin undersökning kallat organisationer med över 1000 anställda för stora organisationer. Vår undersökning involverar bara två organisationer där den ena har omkring 11 300 anställda och den andra har under 10 anställda. Då ena organisationen är så pass stor gör att vart gränsen sätts mellan stor och liten organisation spelar mindre roll, då majoriteten av alla organisationer ses som liten jämfört med dem. Vi har därför valt att följa Gupta, A & Hammond, R. (2005) och Hove et. al. (2014) definitioner av organisationers storlekar.

Vi tog kontakt med Lunds Universitetssjukhus med tanken att de kunde vara vår stora vårdorganisation i undersökningen. Kontakten togs genom att skicka ett meddelande till Region Skånes Facebook sida där vi frågade hur vi kunde komma i kontakt med någon som ansvarar för informationssäkerheten på SUS, detta pga. av att vi inte kunna hitta någon annan kontaktväg. Vi ville komma i kontakt med någon högre uppsatt chef som ansvarar för informationssäkerhet då vi ansåg att denna person skulle kunna ge oss bäst svar på våra frågor. Som svar på vårt Facebookmeddelande fick vi kontaktinformationen till Jonas Johanssons som jobbar som informationssäkerhetssamordnare på SUS. Vi mailade honom där vi beskrev vår studie och fråga om han kunde ställa upp på en intervju. Han visade sig vara väldigt intresserad men föreslog att vi även skulle kontakta deras informationssäkerhetschef Johan Reuterhäll och skickade med hans kontaktinformation. Vi skickade samma mail till infromationssäkerhetschefen som vi skickade till informationssäkerhetssamordnaren och det visade att även han var intresserad av att ställa upp. På så sätt fick vi två intervjuer med personer på SUS som sköter informationssäkerhet på SUS fast har olika roller.

Då Hu m. fl. (2007) upplyste att det kan vara svårt att hitta intervjuobjekt inom säkerhet kontaktade vi fyra mindre vårdorganisationer för att se om de hade intresse av delta i studien. Tre av dessa mindre vårdorganisationer valde att inte delta. Anledningarna var att de inte hade tid, att de inte tyckte de hade någon som kunde besvara frågorna och där den sista inte hörde av sig tillbaka. Det fjärde företaget som ställde upp var Brahe Vård AB.

Då båda författarna tidigare haft kontakt med Brahe Vård ställde de gärna upp att bli intervjuade. Brahe Vård är en liten vårdorganisation som befinner sig i södra Sverige och inriktar sig på boendestöd och vård av ensamkommande flyktingbarn. Kontakten med Brahe Vård skedde på så sätt att vi mailade Tord Ström, deras föreståndare och frågade om han var intresserad av att ställa upp på vår undersökning vilket han ville. Vi valde att intervjua föreståndaren då vi kände att han kunde ge oss bäst svar på våra frågor då de inte har någon dedikerad informationssäkerhetsanställd.

De tre intervjuerna hoppades vi att de skulle ge insikt i hur större och mindre vårdorganisationer hanterar säkerhetsfrågor. Att både få möjlighet att analysera en mindre och en större vårdorganisation gav oss möjligheten att kunna genomföra vår undersökning på önskat sätt.

Intervjuobjekt:

Johan Reuterhäll
Säkerhetschef, Lunds Universitetssjukhus

Jonas Johansson och Anette Nilsson Brunlid
Informationssäkerhetssamordnare, Lunds Universitetssjukhus

Tord Ström
Föreståndare, Brahe Vård

3.3 Intervjuteknik

Vi ansåg att semi-öppna intervjuer var det som skulle kunna gynna vår undersökning mest. Vi tog även hjälp av stödfrågor då vi inte är vana intervjuare och kände att någon typ av frågor kan vara fördelaktigt att ha med sig in i intervjun för att få den flytande. Även om frågorna är förkonstruerade använde vi inte frågorna ordagrant utan de fungerade mer som stödord för att ringa in alla områden.

Innan en intervju kan påbörjas måste vissa saker vara lösta, hitta intervjuobjekt, komma i kontakt, avtala tid och tiden det tar att ta sig mellan platserna (Jacobsen,2002). Vi satsade på att få intervjun att vara i 45-60 minuter och bokade därför in entimmes möten med våra intervjuobjekt. För att ge intervjuobjekten en chans att förbereda sig för intervjun skickade vi våra intervjufrågor till dem minst tre dagar innan intervjuerna skulle ske. Alla intervjuer skedde på plats hos intervjuobjekten under deras arbetstimmar för att slippa störmoment och göra intervjuobjekten bekväma. För att samla in informationen valde vi att spela in intervjuerna på en mobiltelefon. Vi frågade innan varje intervju startade om det var okej att den spelades in för att ge intervjuobjekten en chans att säga nej. Nu sa alla att det var okej men hade någon sagt nej så hade vi även med en bärbar dator som vi hade använt för att skriva ner anteckningar under intervjun.

De förkonstruerade frågor vi använde oss av togs fram genom att utgå från de viktiga punkter som tagits fram i det teoretiska ramverket. Varje punkt i vårt teoretiska ramverk fungerade som ett ämne och vi utformade frågor så att de skulle både återspegla ramverket och även litteraturen. I slutet av varje intervju frågade vi intervjuobjekten om det fanns möjlighet att kontakta de igen i fall att informationen vi fått inte var tillräcklig och alla som intervjuades uppmuntrade till att kontakta dem igen. I slutet av undersökningen kontaktade vi Brahe Vård en andra gång då informationen gällande några punkter inte blivit så djupgående som vi önskat. Efter att vi samlat in empirin så försöker vi tolka den genom att använda oss av den teoribas vi etablerat i föregående kapitel.

3.4 Analys/Bearbetning av data

När vi transkriberade intervjuerna var vi noga med att skriva ner dess innehåll ordagrant för att ge en rättvis bild av den empiri vi samlat in. De enda undantagen från detta var ord som "öh", "eh" vilket vi valde att inte skriva ner för att underlätta läsandet av intervjuerna. Vid några tillfällen på inspelningen kunde det inte urskiljas vad som sas trots flera tillbakaspolningar och då har vi markerat det med "… (Kan inte urskilja vad som sägs) …".

När vi analyserade informationen vi samlat in så gick vi igenom en intervju i taget och kategoriserade informationen utefter de teoridelar vi valt ut i vårt teoretiska ramverk för att skapa en struktur på informationen. Efter all data blivit kategoriserad enligt ramverket markerade vi de mest väsentliga delarna och använde dem som stödord för att lättare kunna navigera i varje del av vårt teoretiska ramverk. Kategorisering av informationen underlättade svarandet på de frågeställningar vi tagit fram till resultatdelen avsevärt. När vi sedan kategoriserat informationen i alla intervjuer så skapade vi en sammanfattning för varje teoridel utifrån både organisationernas perspektiv som vi sedan applicerade i svaren till frågeställningarna i resultatdelen.

3.5 Undersökningskvalitet

I alla typer av undersökningar där man samlar in någon form av empiri bör empirin uppfylla två krav. Att den är relevant och giltig, samt att den är trovärdig och tillförlitlig (Jacobsen, 2002).

3.5.1 Validitet

Med empirisk validitet syftar man på dess giltighet och relevans. Jacobsen (2002) beskriver både en intern och en extern giltighet och relevans i sin bok. Där den interna giltigheten och relevansen syftar på om man faktiskt mäter det man tror sig mäta. För att garantera att vi gör detta så grundar vi alla våra frågor i den teori vi har redovisat i litteraturgenomgången. Det gör att den empiri vi samlar in är av hög relevans för vår undersökning.

Medan den externa giltigheten och relevansen handlar om till vilken grad empirin i en studie kan generaliseras till att även gälla i andra sammanhang (Jacobsen, 2002). Här kan vi som vi nämnt i våra avgränsningar inte garantera att den empiri vi samlat in representerar alla liknande organisationer, utan den kan som bäst ge en indikation om hur dessa typer av organisationer resonerar angående informationssäkerhet.

3.5.2 Reliabilitet

Reliabilitet syftar på att studien måste gå att lita på, att den genomförts på ett trovärdigt sätt, samt att om man skulle genomföra studien en gång till kort efter det första tillfället så skulle resultatet bli liknande (Jacobsen, 2002). För att få vår studie att hålla en hög reliabilitet så transkriberade vi intervjuerna tillsammans för att säkerställa att informationen blir nedskriven på korrekt sätt. När vi väl transkriberat intervjun så gav vi intervjuobjekten chansen att läsa igenom transkriberingen för att se till att deras tankar blev korrekt nedskrivna. Under vår undersökning var det bara deltagarna vid en intervju som vill se över transkriberingen men hade inga synpunkter på den.

3.5.3 Etik

Då vår studie undersöker informationssäkerhet inom hälso- och sjukvården så kan vissa av de uppgifter vi samlar in från våra intervjuer ses som känsliga. Därför har vi försökt att hantera dessa uppgifter på ett så etiskt korrekt sätt som möjligt. Vetenskapsrådet (2002) beskriver fyra krav som ingår i det grundläggande individskyddskravet. Individskyddskravet säger att "individer får inte heller utsättas för psykisk eller fysisk skada, förödmjukelse eller kränkning." (Vetenskapsrådet, 2002, 5) Medan de fyra krav som ingår i det är informationskravet, samtyckeskravet, konfidentialitets kravet och nyttjandekravet. I vår studie utgick vi från dessa fyra krav för att säkerställa den etiska delen av studien.

Informationskravet är att man ska informera de som berörs av forskningen av forskningens syfte (Vetenskapsrådet, 2002). Detta uppfyller vi genom att innan vi börjar intervjuerna berätta kortfattat om vår studie och vad vi hoppas uppnå. Vi skickade även en kort beskrivning av studien i det mail vi skickade när vi frågade om en intervju.

Samtyckeskravet lyder att alla som deltar i studien har rätt att bestämma över sin egna medverkan (Vetenskapsrådet, 2002). För att möta detta kravet berättade vi muntligt innan vi genomförde intervjun att deras deltagande är helt frivillig och att de kan välja att avsluta intervjun när som helst.

Konfidentialitetskravet säger att uppgifterna vi samlar in till studien ska förvaras så att obehöriga inte kan få tillgång till dem, samt att personer i undersökningen ska ges största möjliga konfidentialitet (Vetenskapsrådet, 2002). För att säkerställa de personer vi intervjuats konfidentialitet så gav vi dem möjligheten att vara anonyma i studien. Detta för att de ska kunna känna sig tryggare att säga det de verkligen tänker, utan att behöva vara oroliga för konsekvenserna. I vår studie var det dock ingen som ville vara anonym i undersökningen. Vi förvarade den insamlade datan från intervjuerna i en google drive map som bara författarna hade tillgång till den. Inspelningen togs även bort från mobilen efter att vi fört över den till datorn för att minska chansen att någon obehörig fick tillgång till den.

Nyttjandekravet säger att de uppgifter vi samlat in om enskilda personer under studiens gång endast får användas till vår studie och inget annat (Vetenskapsrådet, 2002). För att uppfylla

detta krav så försäkrar vi de personer vi intervjuar att uppgifterna som vi får fram under intervjun endast kommer att till vår C-uppsats och inget annat.

Utöver de fyra kraven rekommenderar även Vetenskapsrådet (2002) att man ger personerna som deltar i studien möjlighet att få veta vad resultatet av studien tillslut blev om de är intresserade. Detta tyckte vi var en bra idé som vi därför tog till oss. Därför frågade vi de personer vi intervjuade om de ville ha en sammanställning av studien efter att vi är klara. Här visade det sig att det bara var föreståndaren på Brahe Vård som var intresserad.

3.6 Metodkritik

Våra teoretiska källor är på vissa ställen gamla. Vi anser att de fortfarande är relevanta då de för det mesta handlar om statiska ämnen som vi anser inte har förändrats särskilt mycket genom åren. Vi hade ändå kunnat leta nyare källor om vi hade förbättrat vår sökmetod och satt upp krav från början på hur gamla källorna fick vara men vi insåg detta för sent in i undersökningen.

Vårt genomförande av intervjuerna kunde ha varit bättre då vi ibland kom av spåret vilket ledde till att vi missade att ställa vissa frågor. Det löste sig dock genom att vi kontaktade intervjuobjektet en gång till med följdfrågor. Detta anser vi beror på att vi är ovana intervjuare och har väldigt knappa erfarenheter av att hålla intervjuer. Vi hade kunnat lösa detta genom att lägga mer tid på intervjuguiden och gått igenom intervjuerna innan vi påbörjade nästa intervju.

4 Resultat

I detta kapitel presenteras vår empiriska data från intervjuerna som gjorts. Resultatet presenteras genom att vi använder åtta frågor som täcker in alla punkter i vårt teoretiska ramverk. Detta gör vi för att följa den strukturen som är uppbyggd i uppsatsen och för att underlätta för läsaren. Varje fråga börjar alltid med den stora organisationen, SUS, som sedan följs av den lilla organisationen, Brahe Vård och som till sist följs av en jämförelse. Vi har valt att presentera en sammanfattning av resultatet först för att läsaren ska få en överblick av resultatet innan man kan fördjupa sig i områdena som presenteras i vårt teoretiska ramverk.

Tabellen nedan är gjord för att skapa en förståelse över uppbyggnaden av resultatet.

Tabel 2: Resultatets uppbyggnad.

Frågor	Viktiga punkter
Hur påverkar organisationernas tillgång till kompetens och resurser deras hantering av informationssäkerhet?	• Resurser • Kompetens
Vilka konsekvenser får regelbrott för anställda?	• Konsekvenser av regelbrott
I vilken utsträckning används IS-policys och riktlinjer?	• Abstraktionsnivå
Hur involverad är ledningen i säkerhetsarbetet?	• Involverad ledning
Hur påverkar anställdas attityd deras arbete?	• Anställdas attityd
Hur arbetar organisationer med informationssäkerhetsmedvetande?	• Göra anställda medvetna om risker och ansvar
Används ramverk och standarder?	• Standarder och ramverk
Hur hanterar organisationer risker?	• Hantering av risker
Vilka processer för uppföljning och övervakning finns?	• Uppföljning • Övervakning

4.1 Sammanfattning av resultat

SUS har tillgång till både mer resurser samt högre kompetens inom informationssäkerhet än vad Brahe Vård har. De är även striktare i sin hantering av regelbrott jämfört med Brahe Vård som har en mer avslappnad attityd och hellre hanterar regelbrott internt med varningar och samtal. Båda organisationers ledning saknar intresse för informationssäkerhet, men de inser samtidigt vikten av det. Skillnaden är hur involverad ledningen är i informationssäkerhetsarbetet istället då Brahe Vårds ledning är involverad i allt, medan SUS ledningen försöker hålla sig utanför det så gott det går. Brahe Vårds ledning har även ett annat tillvägagångssätt för att påverka anställdas attityder gentemot säkerhet till det bättre. De försöker fostra fram en mentalitet i sin organisation att de är bättre än sina konkurrenter på allt dem gör, vilket föreståndaren säger sig spegla i de anställdas arbete. Jämförelsevis så satsar SUS på att utbilda sina anställda inom informationssäkerhet istället och på så sätt påverka deras attityd till det bättre.

När de kommer till att påverka anställdas informationssäkerhetsmedvetande så jobbar Brahe Vård mer proaktivt än SUS. De tillhandahåller en utbildning för alla nyanställda men saknar tekniska hjälpmedel för att göra information tillgänglig senare vid behov. SUS satsar istället på att ha lättillgänglig information som sprids med hjälp av olika tekniska hjälpmedel så att anställda kan söka upp information när de behöver den.

Båda organisationerna har någon form av riktlinjer eller policys och båda organisationerna har uttryckt ett intresse av att förbättra dem. I Brahe Vård så har man inte riktlinjerna nedskrivna i något dokument och vill därför skapa ett styrande dokument som kan spridas i organisationen. Medan hos SUS så handlar det om att uppdatera befintliga riktlinjer och den IS-policy som finns i organisationen för att förbättra den systematik som redan finns. Riskhanteringen hos SUS är strukturerad med en uttalad systematik och används ofta som utgångspunkt i deras informationssäkerhetsarbete. Hos Brahe Vård sker riskhanteringen mer situationsanpassat, olika risker kan hanteras på olika sätt. Brahe Vård har heller inga särskilda processer för riskanalyser. De använder sig inte heller av några ramverk eller standarder för att hantera informationssäkerhet jämfört med SUS som har valt att implementera delar av ISO 27000 i sin verksamhet.

Både organisationerna saknar relevanta nyckeltal att basera sin uppföljning på. När det kommer till övervakning så övervakar båda organisationerna sina anställdas användning av system för att säkerställa att anställda följer de sekretesskrav som finns och inte bryter mot några regler.

4.2 Hur påverkar organisationers tillgång till kompetens och resurser deras hantering av informationssäkerhet?

Skånes Universitetssjukhus:

Det finns en solid grundkompetens i organisationen då de har tillräckligt med resurser för att anställa en säkerhetsenhet som uteslutande jobbar med olika organisatoriska säkerhetsfrågor. Av de anställda som jobbar där så finns det dock ingen som jobbar uteslutande med informationssäkerhet. Utan för tillfället finns det två personer som jobbar med informationssäkerhetsfrågor som ett komplement till deras andra arbetsuppgifter. Detta för de ska kunna komplettera varandras brister, då ingen är expert inom eller jobbar heltid med informationssäkerhetsfrågor. Sedan avlastas även alla tekniska säkerhetsproblem som har med brandväggar, virusskydd, och hårdvara att göra på deras IT-avdelning.

Informationssäkerhetschefen påpekar också att det finns en gräns för hur mycket organisationen kan/vill satsa på informationssäkerhet då fokus ligger på att kunna få tillgång till informationen snabbt när man väl behöver den, istället för att säkerställa att informationsflödet i organisationen sker på ett säkert sätt. Detta för att i deras bransch så kan det få väldigt allvarliga konsekvenser för deras patienter om patientens läkare inte får den information de behöver i tid.

Det finns en blandad känsla i organisationen angående resurser. Då Informationssäkerhetschefen anser att det saknas resurser för informationssäkerhetsarbetet medan informationssäkerhetssamordnarna ansåg att de hade tillräckligt med resurser för att kunna utföra sitt arbete. Samordnarna ansåg dock att där det saknas resurser, det är i själva sjukhuset, att det saknas personal. De anser det är en anledning till att deras personal inte har tid till att gå deras informationssäkerhetsutbildning.

> *"Ja det gör det, jo det saknas resurser. Jag jobbar på heltid, hela Region Skåne. Sen har varje förvaltning en informationssäkerhetssamordnare då, som ska arbeta med informationssäkerhetsfrågor, men det har dem, det är ingen heltidstjänst dem har utan dem arbetar med det som en extra uppgift."* (Appendix 1, rad 88–91)

Brahe Vård:

Den som sköter Brahe Vårds informationssäkerhetsarbete är dess föreståndare. Han har en stor mängd olika roller inom organisationen vilket leder till att han har väldigt lite tid att lägga på just informationssäkerhet. Han säger att bara en tredjedel av allt arbete han gör har med föreståndare rollen att göra, och i denna tredjedel handlar det mesta om annat än informationssäkerhet. Rent resursmässigt tycker han dock att de som organisation har tillräckligt för att sköta informationssäkerheten på ett acceptabelt sätt för en organisation av deras storlek. Föreståndaren påpekar också att mer pengar såklart inte hade skadat, och hade kunnat ge dem möjligheten att säkra deras informationssystem ännu mer.

Att föreståndaren har så mycket annat att göra gör att han har svårt att hitta tid att säkerställa att de krav som ställs på organisationen gällande informationssäkerhet följs på ett så bra sätt som möjligt. Även när det kommer nya lagar eller krav så ligger ansvaret på varje organisation att lösningar för dessa implementeras. Vilket föreståndaren antydde var ett problem för dem, då han har så mycket annat att hålla koll på samtidigt.

"Nja det är väl klart att man hade kunnat ha, om man hade varit en större verksamhet så hade man kunnat ha en mer avancerad lokal med mer avancerade lås. Man hade kunnat ha mer avancerade säkerhetssystem på journalsystemet och så vidare. Det finns ju alltid dem möjligheterna om man har tillräckligt med kulor." (Appendix 3, rad 79–82)

Jämförelse mellan organisationerna:

SUS har både mer resurser och kompetens inom informationssäkerhetsarbetet än Brahe Vård vilket är naturligt då de är en mycket större organisation. SUS är även de som anser att de saknar resurser till informationssäkerhetsarbetet, medan Brahe Vård säger att de klarar sig med de resurser de har för tillfället. Både Brahe Vård och SUS fokuserar på olika typer av resurser när vi pratade med dem. SUS diskuterade mer resurser i form av pengar och arbetskraft, medan Brahe Vård la mycket fokus på tid som en resurs.

Att SUS har resurserna att anställa en hel säkerhetsavdelning gör att de besitter en högre kompetensnivå än Brahe Vård som bara har sin föreståndare som jobbar deltid med informationssäkerhet. Föreståndaren har även väldigt lite tid att lägga på informationssäkerhet vilket ökar klyftan mellan de olika organisationerna ännu mer. Dock så saknar SUS någon riktig spetskompetens inom området då deras anställda som har hand om informationssäkerheten både sköter andra uppgifter vid sidan om samt vissa som jobbar med informationssäkerhetsfrågor inte har någon bakgrund inom området.

4.3 Vilka konsekvenser får regelbrott för anställda?

Skånes Universitetssjukhus:

Beroende på vad för regler den anställde bryter mot så får det olika konsekvenser. När regelbrott i organisationen uppdagas så hamnar ärendet hos respektive verksamhets HR avdelning, som sedan tar ställning till hur man bör gå vidare. Kollar en anställd på någons journal som den inte har tillgång till så klassas det som dataintrång vilket i sin tur leder till en polisanmälan. Blir den anställde dessutom funnen skyldig så förlorar den även sin anställning. Är det däremot en incident som riskerar patientsäkerheten så kopplas även IVO in. Det kan i sin tur leda till att IVO förelägger SUS med olika saker, utöver de konsekvenser som den anställde råkar ut för.

"Jodå det är ingen hemlighet med det utan, om vi har en anställd till exempel som tittar på en journal utan att ha rätt till det så kan de ju bli, ja dem kan, dem blir väl oftast anmälda då för olaga dataintrång. Så det kan ju leda till att de blir av med sin anställning." (Appendix 1, rad 308–310).

Brahe Vård:

Konsekvenserna för anställda som bryter mot regler beror på allvaret i vad de har gjort. För det mesta så försöker man att lösa saker internt inom organisationen, där varningar och tillrättavisningar ofta är de första konsekvenserna anställda får utstå om de bryter mot regler. Sker det upprepade regelbrott och oacceptabelt beteende så kan det leda till att man förlorar sin anställning. Än så länge har de dock aldrig behövt agera arbetsrättsligt mot någon anställd.

"Det beror ju på allvaret i vad de har gjort men ibland får man ju tillrättavisa och förmana och ibland skärpa tonen ordentligt men vi har ännu inte gått så långt att vi behöver agera arbetsrättsligt." (Appendix 3, rad 135–137)

Jämförelse mellan organisationerna:

Konsekvenserna hos båda organisationerna beror på allvaret i regelbrottet. När vi diskuterade konsekvenser med de olika organisationerna var Brahe Vård mer angelägna om att lösa problemen internt och inte blanda in utomstående utredningsorgan som polisen eller IVO. Medan SUS sköter regelbrott mer formellt och har tydliga processer för hur regelbrott hanteras. Överlag har Brahe Vård få regelbrott och har aldrig behövt ta till arbetsrättsliga åtgärder mot någon anställd. Föreståndaren påpekar även att anställda uppmanas att komma till honom och berätta om de klantat sig eller gjort något fel, vilket också kan spela in i deras mildare behandling.

4.4 I vilken utsträckning används IS-policys och riktlinjer?

Skånes Universitetssjukhus:

SUS använder sig av en gammal säkerhetspolicy som informationssäkerhetschefen anser är alltför utdaterad. Det har lett till att de har börjat att arbeta om policyn för att anpassa den bättre till dagens verksamhet. Policyn i sig handlar dock inte specifikt om informationssäkerhet utan det är mera allmän säkerhet där informationssäkerhet får ett eget parti. Policyn ligger på en väldigt övergripande nivå och det är kommunfullmäktige som fattar beslut om den. Policyn ska rama in krav som ställs på alla verksamheter inom Region Skåne, vilket bidrar till att den är väldigt generell.

I dagsläget arbetar regionstyrelsen även på att ta fram en ny riktlinje. Riktlinjen kommer att delas upp i flera kapitel som behandlar alla Region Skånes verksamheter. Kapitlet för informationssäkerhet kommer att innehålla mer detaljerad information om hur informationssäkerheten ska hanteras. I riktlinjen kommer det att finnas regionövergripande instruktioner samt

att det specificeras vilket ansvar och roller olika delar av organisationen har i informationssäkerhetsarbetet. Ett av syftena med den nya riktlinjen är att göra arbetet med informationssäkerhet mer uppföljningsbart. Då de i dagsläget har svårt att få fram någon vettig information tack vare att de saknar mätbara nyckeltal och liknande.

Varje enskild förvaltning kan sedan ta instruktionerna som finns i riktlinjen och välja själva hur de praktiskt vill implementera dem i sin verksamhet utefter sina egna förutsättningar. Det gör att varje enskild förvaltning kan skapa sina egna rutiner och dela ut ansvar och roller på det sätt som bäst passar dem själva. Det enda kravet uppifrån är att deras egna instruktioner inte får avvika från de övergripande instruktionerna som finns i riktlinjen.

"Nä, överst är då säkerhetspolicyn då och de är fullmäktige som fattar beslut, det är ju högsta beslutande organet [...] och de kommer också fatta beslut om de övergripande målen som är på en väldigt molnfri höjd så att säga. Och nivån under är regionstyrelsen och dem kommer fatta beslut om riktlinjer och den blir ju ganska detaljerad utan att gå ner i detalj så talar den om vad som ska göras och det är hyfsat detaljerat" (Appendix 1, rad 480–484)

Brahe Vård:

I Brahe Vård så har ledningen tagit fram flera separata riktlinjer som behandlar olika områden. Riktlinjerna är inte nedskrivna någonstans för tillfället men det är något de siktar på att göra. I dagsläget behandlar riktlinjerna mestadels sekretess som rör deras klienterna och fokuserar mindre på känsliga data som berör organisationen. Föreståndaren berättade att de är en nystartad organisation och fram tills nu har de fokuserat mer på operativa frågor och lagt mindre tid på att ta fram interna dokument och rutiner. Brahe Vård har dock insett att detta behövs och har därför börjat planera för att ta fram olika rutiner och interna dokument.

Jämförelse mellan organisationerna:

SUS använder sig av en väldigt övergripande IS-policy som passar in i alla deras verksamheter. Sedan finns det även en riktlinje som berättar hur SUS ska arbeta med informationssäkerhet mera detaljerat. Brahe Vård däremot använder sig inte av någon policy utan de har olika riktlinjer där en fokuserar på sekretessbelagd information angående deras klienter. Riktlinjen innehåller mer regler än instruktioner över hur anställda ska jobba med känslig- och sekretessbelagd information. Båda organisationerna tycker att deras policys och riktlinjer inte är tillräckligt uppdaterade eller väl utformade vilket tyder på att organisationerna inte har prioriterat denna del av informationssäkerhetsarbetet.

4.5 Hur involverad är ledningen i säkerhetsarbetet?

Skånes Universitetssjukhus:

Informationssäkerhet är inte högt prioriterat hos ledningen i organisationen. Ledningen tycker fortfarande att det är viktigt men intresset finns bara inte där. För ett och ett halvt år sedan gjordes en satsning för att öka intresset och medvetenheten om informationssäkerhet hos verksamhetscheferna. Då gick alla verksamhetschefer en halvdagsutbildning i informationssäkerhet, men efter det så har intresset svalnat igen. Det låga intresset leder till att ledningen inte är lika involverad som de hade kunnat vara.

"InfoSek är väl i nuläget inte högt prioriterat. Vi gjorde en satsning för 1,5 år sedan, då gick hela ledningen, alla verksamhetschefer, en halvdagsutbildning i informationssäkerhet. Då tog man lite tag i det. Nu är det väl sisådär." (Appendix 2, rad 182–184)

Informationssäkerhetschefen säger dock att han inte möter något stort motstånd när han försöker driva igenom saker, utan det är när han börjar diskutera saker i detalj med ledningen som de börjar skruva på sig. Särskilt känsligt är det när pengar och krav börjar diskuteras, han förklarar att de skriver hellre bara på saker än att sätta sig in i dem ordentligt. Informationssäkerhetssamordnarna säger samma sak, att de inte har några problem att driva igenom saker om de tar egna initiativ.

"De tycker att det är viktigt och jag möter väl inte på något jättestort motstånd men när man börjar på att gå ner mer i detalj och man vill att regionstyrelsen ska fatta beslut och riktlinjer som är ganska detaljerade då kommer de skruva på sig, det tror jag iallafall. För då börjar det komma närmare och då kommer det ställas krav och då kommer det kosta pengar och så kanske det försenar saker och ting som man tänk sig." (Appendix 1, rad 411–417)

Brahe Vård:

Allting som har med informationssäkerhet att göra drivs av Brahe Vårds ledning då de inte har några speciella IT eller säkerhetsanställda. Det gör att ledningen är väldigt involverad i hur deras organisation hanterar informationssäkerhet. Föreståndaren ser informationssäkerhet som intressant till den mån att de lyckas säkerställa deras informations säkerhet i organisationen. Ledningen sköter allt från att ta fram riktlinjer och välja säkerhetslösningar till deras system, till att även se till att de följs av de anställda.

"Vi utvecklar ju hela arbetet här. [...] Personalen jobbar i princip bara med vård av elever [...] Men det är ju inte dem som jobbar med driftsfrågor alltså säkerhetsriktlinjer och sånt." (Appendix 3, rad 146–149)

Jämförelse mellan organisationerna:

Ledningens intresse för informationssäkerhet är inte stort hos någon av organisationerna. Ledningarna tycker dock fortfarande att det är ett viktigt område av deras verksamhet men det prioriteras bara inte. Den stora skillnaden mellan organisationerna är hur involverad ledningen är i informationssäkerhetsarbetet. Då i Brahe Vård är föreståndaren involverad i allt som har med informationssäkerhet att göra. Medan i SUS så säger informationssäkerhetschefen att ledningen vill mest bara skriva under saker och låta andra utföra själva arbetet. Han lägger dock till att han inte stöter på något större motstånd när han försöker driva igenom saker vilket visar att ledningen ändå inser vikten av informationssäkerhet.

4.6 Hur påverkar anställdas attityd deras arbete?

Skånes Universitetssjukhus:

Informationssäkerhetschefen anser att en blandning av anställdas okunskap och att de tror att de vet bättre själva är en bidragande faktor när en anställd väl bryter mot regler. Att de anställda letar efter genvägar för att de tycker att vissa regler gäller inte just dem. Dock så hade han inga konkreta fall utan det var hans åsikt som växt fram under tiden. Informationssäkerhetschefen menar att utbildningen är viktig i detta sammanhang, att man tränar anställda så att de förstår att det är fel att göra på vissa sätt.

"Alltså ibland vet dem inte, ibland vet dem fast dem går runt det eller kanske inte tycker att det är så viktigt. Så det är nog en blandning, men jag har inga konkreta såna fall. Men det är ofta en blandning av okunskap och att man tycker att det här kanske inte gäller mig, så man tar en genväg eller någonting." (Appendix 1, rad 295–298)

Informationssäkerhetssamordnarna berättar att när de pratar informationssäkerhet med anställda så uppfattas det ofta som något som är tråkigt vilket de anser kan vara ett hinder i deras säkerhetsarbete. Informationssäkerhetssamordnarna poängterar dock att de oftast just är ordet "informationssäkerhet" som gör att de anställda tycker att det är tråkigt. Pratar man med anställda och använder ord som integritet eller patientuppgifter istället så får de bättre respons av de anställda. Informationssäkerhetssamordnarna anser att anställda vill göra rätt och tänka på säkerhet, så när anställda inte inser att de pratar om informationssäkerhet så går informationssäkerhetsarbetet bättre, vilket Informationssäkerhetssamordnarna tycker är ett av dilemmat med att jobba med informationssäkerhet.

"Alltså allting går i ett, menar, problemet med informationssäkerhet det är att det egentligen spänner så otroligt mycket, och ja om man frågar folk hur kul man tycker det är med informationssäkerhet så säger dem att det är tråkigt" (Appendix 2, rad 192–194)

Brahe Vård:

Föreståndaren för Brahe Vård trycker på att i deras organisation har det växt fram en mentalitet att Brahe Vård är bättre än andra liknande organisationer på det dem gör, vilket han säger speglar sig i deras anställdas beteende. Anställda som jobbar hos Brahe Vård avlönas i snitt bättre än hos andra organisationer i samma bransch, vilket föreståndaren anser att de anställda är stolta över och gör att de vill fortsätta leverera högkvalitativ vård till deras klienter. En annan förmån som de anställda hos Brahe Vård har är möjligheten för dem att jobba hemifrån och skriva sina journalinlägg. Hade inte anställda skött det på ett bra sätt så hade lösningen varit att de hade varit tvungen att åka in till huvudkontoret och skriva sina journalinlägg. Föreståndaren menar att dessa förmåner och den mentalitet som vuxit fram hos Brahe Vård påverkar deras anställdas attityd till det bättre när det kommer till deras arbetsinsats, att de faktiskt anstränger sig för att göra allt på ett så korrekt sätt som möjligt.

"Vi tycker att vi är bättre än andra och det tycker vår personal också [..] Vi avlönar dem efter det och att vi ställer krav på dem helt enkelt efter det. Och det tycker jag att de vill att vi ska göra. De vill att vi ska ha den höga kvalitén som vi påstår att vi har. Det ska vara en förmån att få jobba hos oss." (Appendix 3, rad 158–162)

Den största biten av informationssäkerhetsarbetet som de anställda hos Brahe Vård kommer i kontakt med är sekretessbiten, att klienters personliga uppgifter och journaler ska hållas hemliga för obehöriga. En faktor som föreståndaren lyfter fram som bidrar till att den sköts så pass bra hos dem är att många av deras behandlingsassistenter har varit i samma eller i liknande sitsar som de klienter som de behandlar. Det gör dem mer motiverade att sköta sitt jobb på ett så bra sätt som möjligt, både behandlings- och administrationsdelen av sitt arbete.

"Vår förste anställde tog jag med mig från där jag jobbade innan för att han är marockan och de första eleverna vi fick var marockaner förutom en svensk tjej. Och han är väldigt motiverad av att hjälpa sina landsmän till ett bra liv i Sverige." (Appendix 3, rad 177–180)

Jämförelse mellan organisationerna:

Informationssäkerhetssamordnarna på SUS och föreståndaren på Brahe Vård pratar både om att i grunden vill de anställda verkligen göra rätt för sig. På SUS pratas det dock om att anställda ser informationssäkerhet som något som är tråkigt och hindrar deras arbete. Informationssäkerhetssamordnarna säger sig få bättre respons av anställda om de inte använder ordet informationssäkerhet och istället använder sig av ord som kan placeras under kategorin informationssäkerhet, som integritet, sekretess och liknande. Informationssäkerhetschefen går även så långt att påstå att anställda ibland kan tro sig veta bättre än de som sätter upp reglerna, vilket kan leda till regelbrott. Föreståndaren hos Brahe Vård pratar istället om att anställda hos dem tas om hand på ett så bra sätt med olika förmåner att det påverkar deras anställdas attityd till det bättre gentemot hur väl man genomför sina arbetsuppgifter. De säger sig även ha framgångsrikt fostrat fram en mentalitet hos sina anställda som bidrar till de anställdas arbetsflit.

SUS anser att utbildning av anställda är viktigt i det här sammanhanget, att man genom utbildning kan påverka anställdas attityd till det bättre. Vilket skiljer sig från Brahe Vårds angreppssätt som fokuserar på att fostra en kultur inom organisationen som tar informationssäkerhetsarbete på stort allvar.

4.7 Hur arbetar organisationer med informationssäkerhetsmedvetande?

Skånes Universitetssjukhus:

I dagsläget finns det en informationssäkerhetsutbildning på deras intranät som är till för att göra anställda mer medvetna om risker och verksamhetens olika riktlinjer och policys men då den inte är obligatorisk är det ett lågt antal anställda som faktiskt går utbildningen. En informationssäkerhetssamordnare förklarade att målet gällande antalet anställda som ska gå utbildningen inte längre följdes upp då förutsättningarna för att anställda ska kunna utföra sitt arbete samt ha tid att gå utbildningen inte finns. Den intervjuade menade att det inte var möjligt att få anställda på avdelningar som redan har ett underskott på tid att sitta och göra utbildningar som inte är obligatoriska vilket leder till att ett lågt antal anställda går utbildningen.

"Nä utan vi har en E-utbildning i informationssäkerhet som vi tagit fram [...] Men den är inte obligatorisk, och innan den blir det och att man följer upp den så är det inte så många som kommer att gå den heller." (Appendix 1, rad 103–108)

Beslut och förändringar gällande informationssäkerhet kommuniceras ut neråt i organisationen till berörda avdelningar som informerar ut till sina anställda. Anställda kan sen ta del av informationen via dokument på intranätet eller uppdaterad e-utbildning. Intranätet förklarades dock av både av informationssäkerhetschefen och informationssäkerhetssamordnarna som ett svart hål och att de själva har svårt att hitta även om de ansvarar för informationen som publiceras där.

"Ofta ligger informationen på något intranät. Om man lyckas hitta det för det är [...] ett svart hål… Men annars så… hittar de inte det där så kommer de ju… ställer de frågan till… uppåt då så att säga och till slut så... ja, ibland landar den ju hos mig eller hos juristerna." (Appendix 1, rad 502–506)

Avslutningsvis gick informationssäkerhetschefen igenom vikten av att skicka rätt information till rätt mottagare i organisationen gällande informationssäkerhet. Balansgången att ge tillräckligt med information för att de ska sköta sitt arbete utan incidenter men att inte kasta så mycket information på dem att det inte kan behandla allt eller att det blir ointressant är en utmaning.

Brahe Vård:

Då vissa av de anställda har gått en socionomutbildning som innehållit kurser gällande bland annat personuppgiftslagen och sekretesslagen anser föreståndaren att de har en god bas när det kommer till informationssäkerhetsmedvetande. Deltids och timanställda är ofta inte insatta i lagarna kring informationssäkerhet och behöver därför mer utbildning för öka medvetenheten.

"Ja alltså, jo om man har en socionomutbildning som vissa av oss har så ingår det ju i utbildningen. Annars, alltså sekretesslagen och kunna den. Annars så har vi internutbildat till det." (Appendix 3, rad 47–49)

Organisationen saknar tekniskt stöd såsom intranät för att kunna publicera rutiner och instruktioner. Istället finns de på en lokal dator och i pappersform på huvudkontoret vilket gör att information inte blir lättillgänglig. Det finns inte heller något utbildningsmaterial gällande informationssäkerhet utan utbildningen görs muntligt. Föreståndaren menar att genom att ha personal i organisationen som har en djup förståelse för lagarna kan de både besvara frågor och vidareutbilda kollegor.

Vid nya lagar eller rutinförändringar kommuniceras detta ut på veckomötena.

Jämförelse mellan organisationerna:

SUS stora utmaning gällande att göra anställda medvetna om informationssäkerhet är att nå ut med information till så många som möjligt och prioriterar därför tekniska hjälpmedel. Brahe Vård har däremot inte några problem med att nå ut till alla anställda då de är så få. Brahe Vård använder sig dock inte av några tekniska hjälpmedel utöver mail utan sprider information direkt mellan varandra på bl.a. sina måndagsmöten. SUS publicerar informationen på intranät och erbjuder e-utbildning för att öka anställdas informationssäkerhetsmedvetande samt deras kunskaper inom området. Informationssäkerhetssamordnarna benämner dock deras intranät som ett svart hål, att det är svårt att hitta den information man söker. SUS informationssäkerhetsutbildning är inte obligatorisk vilket gör att den har en låg deltagarnivå. De har satt upp mål för hur många anställda de vill ska genomgå utbildningen men har inget sätt att följa upp hur många som faktiskt går den. Brahe Vård har också en utbildning gällande hur man hanterar känslig och sekretessbelagd information och varför det är viktigt. Deras utbildning är tillskillnad från SUS individuell och genomförs en gång med de nyanställda för att bidra till ett ökat informationssäkerhetsmedvetande hos den anställde.

4.8 Används ramverk & standarder?

Skånes Universitetssjukhus:

Organisationen använder sig av en del ramverk och ISO-standards genom hela organisationen. Inom informationssäkerhet har de valt att inte certifiera sig utan använder istället de bitar ur ISO 27000 som lämpar sig.

Brahe Vård:

Brahe Vård använder inga ramverk eller standarder gällande informationssäkerhet då behovet ansågs som väldigt litet.

Jämförelse mellan organisationerna:

SUS använder sig av en del bitar ur ISO 27000 till deras informationssäkerhetsarbete medan Brahe Vård har valt att inte implementera några, ramverk eller standarder för att hantera informationssäkerhet.

4.9 Hur hanterar organisationen risker?

Skånes Universitetssjukhus:

För att hantera risker så arbetar SUS med riskanalyser i både förebyggande och proaktivt syfte. Informationssäkerhetssamordnarna säger att riskanalyser utgör ofta organisationens utgångspunkt i deras informationssäkerhetsarbete och har som mål att identifierar risker och se hur de ska lösas.

"Och då kan du använda riskanalyser som ett utgångsläge, man gör riskanalyser ... och den är ofta i ett utgångsläge och den är ofta utgångspunkten i allt informationssäkerhetsarbete."
(Appendix 2, 551–553)

När SUS tar fram en ny e-tjänst eller liknande så ingår en riskanalys i det projektet. I riskanalysen undersöker man vilka krav på informationssäkerhet som finns, både från verksamheten och olika lagkrav. Det görs för att sedan identifiera hur man ska möta kraven på ett så informationssäkert och ekonomiskt hållbart sätt som möjligt. Det är så informationssäkerhetschefen beskriver att riskanalysarbetet ska fungera, men säger att verkligheten är att det inte alltid fungerar på det sättet.

Informationssäkerhetschefen säger att det största problemet när de gör sina riskanalyser är att man inte får till den rätta systematiken i riskanalysprocesserna vilket kan leda till att de missar att vidta nödvändiga säkerhetsåtgärder. Förutom att fokusera på att få till rätt systematik så lyfter han även fram att det är viktigt att det inte går för snabbt fram när man gör sin riskanalys då det kan bidra till att den slutliga kvalitén av tjänsten sänks och dessutom riskera patientsäkerheten.

"Det största hotet ja, det största hotet är att alltså om man inte får till den här systematiken så vi gör våra riskanalyser och att man missar och vidtar säkerhetsåtergärder som gör att patientinformation kommer ut." (Appendix 1, rad 39–41)

Riskanalyser görs även reaktivt och kan startas av att någon brist i befintliga processer upptäcks eller om en avvikelse rapporteras in och måste hanteras. Proaktiva riskanalyser görs oftast för att hitta förbättringsmöjligheter i redan befintliga processer, från ett informationssäkerhetsperspektiv. När en riskanalys är genomförd så skickas resultatet vidare till en relevant förvaltningsgrupp som sedan fattar beslut utefter den information de fått.

Brahe Vård:

Hos Brahe Vård hanteras risker situationsanpassat, det finns ingen utsatt systematik för hur risker ska hanteras. Föreståndare nämner att de risker som redan identifierats är att sekretessbelagda dokument kan förvaras på osäkra ställen, att man glömmer eller tappar bort dokument samt att någon obehörig får tillträde till deras journalsystem. För att motarbeta de risker som identifierats så förlitar sig Brahe Vård en rad regler och rutiner. Föreståndaren säger även att när det väl sker möten där allvarlig sekretessbelagd information utbytes eller förflyttas så är han med i 95% av fallen, vilket gör att han kan övervaka hanteringen.

Brahe Vård har inga särskilda processer för riskanalyser. Istället litar de på att sina anställda kommer till dem och berättar om de upptäcker några brister eller risker i hur de arbetar för tillfället. Det kan i sin tur leda till en utredning där man undersöker vad man kan göra åt saken.

"Ja alltså dem risker som finns är ju att, ja dels eftersom att vi ibland måste ha kontoret på fickan, att man skulle glömma sin portfölj någonstans med något sekretesspapper i någonstans, och det är inte bra." (Appendix 3, rad 23–25)

Jämförelse mellan organisationerna:

SUS har en mer strukturerad riskhanteringsprocess, alla projekt och förändringar ska ha riskanalyserats enligt rutinerna. Riskanalyserna används sedan som utgångspunkt i informationssäkerhetsarbetet. Brahe Vård använder sig av ett mer situations anpassat tillvägagångssätt och har inga särskilda rutiner eller verktyg för att hantera risker. Brahe Vård fokuserar också på att ha en öppen och snabb kommunikation gällande risker där de litar på att anställda kommer och berättar om de upptäcker några risker eller problem i deras arbetsuppgifter.

Hos Brahe Vård finns det ingen systematik i hur riskhanteringen går till medan hos SUS så har de arbetat fram en teoretisk systematik som de ska följa i sin riskhantering. Informationssäkerhetschefen på SUS säger dock att den inte alltid följs i praktiken då det finns andra faktorer som gör att det inte alltid är optimalt att använda den systematik som arbetats fram.

4.10 Vilka processer för uppföljning & övervakning finns?

Skånes Universitetssjukhus:

Informationssäkerhetschefen berättade att verksamheten inte hade något automatiskt stöd vid varken uppföljning eller övervakning. Detta pga. att organisationen har mängder med olika system som inte kan integrera med varandra eller producera statistik. Arbetet får därför göras manuellt vilket är en tidskrävande process och det anses inte som något som är värt att investera i tills en ny IT-lösning ska ta över. Därför har man valt att främst fokusera på två delar. Alla större incidenter hanteras manuellt och följs upp om det anses behov av det. Den andra delen är att följa upp att anställda inte tar del av information som de inte har rätt till som till exempel patientuppgifter eller patientjournaler. Detta följs upp genom att 10% av organisationens anställda granskas i månaden och anställda väljs ut helt slumpmässigt.

"Men det nuvarande stora journalsystemet, den databasen är inte byggd på ett sätt som gör att det är enkelt att göra de här avancerade analyser, utan det är manuellt, tar mycket tid. Men det är det vi gör gällande patientuppgifter. Sen alltså övrigt, övrigt så har vi inga sådana beslutande åtgärder, att man ska göra granskningar eller så. Det är om det inträffar incidenter, då får man titta närmare på det." (Appendix 1, rad 159–163)

Efter att träffat informationssäkerhetssamordnarna fick vi ytterligare insikt i hur svårt uppföljning för tillfället är pga. det bristande IT-stödet. Detta styr organisationen till att jobba mer med brandsläckning och enstaka förebyggande åtgärder. De mål som en gång har satts upp, till exempel deltagarantal i informationssäkerhetsutbildningen, jobbas det knappt för att uppnå då det manuella arbetet är för stort.

De förklarar också att när en "känd" person, vilket inte behöver vara känd från media utan kan var en känd anställd från avdelningen eller sjukhuset, kommer in så räknas detta som en högrisks person och därför kontrolleras det så att ingen obehörig har läst journaluppgifterna. Alla incidenter som sker i organisationen rapporteras dock i ett avvikelsesystem där varje avdelning hanterar de incidenter som är relaterade till deras område. Detta fungerar inte optimalt då avvikelser och incidenter ofta kategoriseras fel av anmälaren vilket leder till att ärendet hamnar på fel avdelning där den "försvinner" istället för att de skickas till rätt avdelning.

Men det finns klara visioner om bättre uppföljning och övervakning. Informationssäkerhetschefen jobbar för tillfället med upphandling av ett nytt journalsystem ska ersätta flera av organisationens befintliga system och detta ska ge organisationen det stöd de behöver för att kunna ta fram nyckeltal mm.

"Nä precis, inga nyckeltal. Det finns inga krav, liksom inte ska-krav att följa upp verksamheterna mot. Hade vi haft det hade jag kunnat ställa frågor på alla de här, har ni gjort det här? Har ni gjort det här? Har ni gjort det här? Kunna samla in och ta fram statistik och visa för ledningen men det finns inte idag." (Appendix 1, rad 387–390)

Brahe Vård:

Både uppföljningen och övervakning inom informationssäkerhet är lågt prioriterat och data såsom nyckeltal inte finns för att följa upp. De anställdas aktivitet i journalsystemet loggas så att i fall att det skulle behöva utredas kan man kolla upp vilken personal som begärt tillgång till vilken information. Dock har detta aldrig behövt användas då alla anställda har en viss insikt i alla elevers patientuppgifter. Föreståndaren påpekade att i en liten organisation där anställda kan behöva jobba med klienter som de inte har ansvar för finns ett behov att veta grundläggande information om klienterna. Dock poängterades det också att all information om klienterna inte skulle besittas av alla och att klienternas journalföring inte får tas del av om det inte fanns ett syfte. Incidenter tas upp veckovis i den mån de inträffar och hanteras därefter.

"Det säkerhetsarbete dem ska hantera är ju dels journalsystemet och dels att hålla flabben stängd när de pratar med andra människor än folk i företaget. Och det senare är väldigt svårt att kontrollera och det första är ju ganska lätta att kontrollera." (Appendix 3, rad 202–204)

Jämförelse mellan organisationerna:

Både uppföljning och övervakning har låg prioritet i båda organisationerna. Ingen av organisationerna har några nyckeltal alls inom informationssäkerhet. På SUS har man dock identifierat ett behov av att följa upp vissa processer för att kunna mäta och agera korrekt utifrån den data man kan samla in. Brahe Vård ser dock inget behov att administrera uppföljning och övervakning mer än man redan gör. Båda organisationerna anser att det behövs mer tekniska resurser för att kunna sköta övervakning, uppföljning, och att kontrollera vart resurser behövs för att optimera informationssäkerhetsarbetet. Både anser också att även om de kan undersöka de anställdas aktivitet då de är på kontoret/arbetsplatsen så är det mycket svårare att kontrollera att de följer sekretessen när de inte är på arbetsplatsen eller talar med sin familj och vänner.

5 Diskussion

Diskussionen är strukturerad utefter de viktiga punkter som tagits fram i det teoretiska ramverket för att göra den enklare att följa. Under diskussionens gång kopplar vi även de olika punkterna med varandra och jämför med vad teorin säger. Till sist lägger vi till egna tankar och resonemang kring varför och hur saker ser ut.

5.1 Resurser och kompetens:

Informationssäkerhet är ett viktigt verktyg för organisationer av alla storlekar i deras mål att hålla dem säkra mot hot, både interna och externa. En av de största skillnaderna i vår undersökning var tillgången till resurser och kompetens vilket vi redan innan uppsatsen startade trodde skulle vara fallet. Gupta & Hammond (2005) säger att resursbrist hos mindre organisationer leder till att de väljer säkerhetslösningar de har råd med, även om lösningarna inte är lämpade för just deras organisation. Hos Brahe Vård märktes det att resurser inte prioriterades till informationssäkerhet. Istället för att lägga resurser på uppföljning, riskanalyser och tekniska säkerhetslösningar så lägger de hellre resurser på att skapa bra löneförmåner till sina anställda vilket stärker Gupta & Hammond (2005) slutsats. När vi diskuterade resurser med Brahe Vård tyckte vi det var intressant att de fokuserade mycket på tid som en resurs istället för pengar och arbetskraft. Vi fick känslan av att föreståndaren verkade tro att bara han hade mer tid på sig till informationssäkerhet så hade han kunnat förbättra informationssäkerhetsarbetet. Eftersom Brahe Vård är en liten organisation med begränsade resurser så har de inte råd att anställa en säkerhetsanställd till skillnad från SUS vilket gör att förändringar tar längre tid då kompetensen är lägre. Det kan förklara varför Brahe Vård fokuserar så mycket på just tid som en resurs.

Hos SUS säger deras informationssäkerhetschef att det saknas resurser i form av pengar och arbetskraft till informationssäkerhet medan föreståndaren hos Brahe Vård upplever att de befintliga resurser som läggs på informationssäkerhet räcker, förutom att tid saknas. Det leder in oss på nästa punkt, att Brahe Vård gärna inte gör mer än vad som behövs gällande informationssäkerhet medan SUS vill genom informationssäkerhet bidra med något av värde till hela organisationen. MSB (2015) säger att vårdgivarnas informationssäkerhetsarbete är mer motiverat av att uppnå lagkrav än att faktiskt generera någon nytta för organisationen vilket stämmer överens med Brahe Vård, men hos SUS har det börjat ske en förändring. SUS informationssäkerhetschef blev anställd runt den tiden som MSB (2015) undersökning släpptes vilket vi ser som ett intressant sammanträffande. Nu vet vi inte om hans anställning påverkades av MSBs (2015) undersökning, men det är möjligt att SUS insåg att något behövdes göras och skaffade sig ny kompetens.

Kompetens och resurser har ett starkt samband mellan varandra. Kankanhalli et. al. (2003) säger att organisationer med större tillgång till resurser har en bättre chans att lyckas skaffa sig rätt kompetens för att skydda sig. SUS har resurserna att anställa en hel säkerhetsavdelning

där två anställda jobbar just med informationssäkerhet. Informationssäkerhetssamordnarna säger att anledningen till att de är två som jobbar med informationssäkerhet är att de ska komplettera varandras brister. Från början när vi bokade en intervju med Jonas (informationssäkerhetssamordnare nr 1) så var tanken att vi bara skulle prata med honom, men sedan dök även Anette (informationssäkerhetssamordnare nr 2) upp på intervjun för att även här komplettera varandras kunskapsluckor. Vi blev positivt överraskade av att Anette också dök upp då vi tycker att det påvisar att det finns ett bra samarbete mellan informationssäkerhetssamordnarna och att de har en form av självinsikt. Att de inser att trots deras resurser så har de inte den bästa kompetensen inom området men tar steg för att överkomma det kunskapsgapet.

5.2 Konsekvenser av regelbrott:

Även om SUS och Brahe Vård har samma tankesätt gällande regelbrott av sina anställda så sköter de inte det på samma sätt. Detta beror enligt oss på att de är olika stora. Brahe Vård har en större lojalitet gentemot sina anställda och kopplade brister i informationssäkerheten till slarv istället för en avsiktlig handling och önskar hantera det internt med utbildning och varningar. Detta beror på att de är en mindre organisation där de anställda har en närmre relation med ledningen/föreståndaren. SUS har ett mer objektivt tillvägagångssätt där man har en utarbetad rutin hur det ska hanteras. En informationssäkersamordnare på SUS berättade att de har flera ärenden per år där de har skett brott mot sekretessen. Detta förklarar varför SUS har ett utarbetat arbetssätt att hantera dessa frågor. Även då SUS har ett mer utarbetat tillvägagångsätt och på grund av sin storlek även har ett större antal incidenter mot informationssäkerheten skulle detta kunna diskuteras att deras anställda har en större medvetenhet av konsekvenser. Puhakainen & Siponen (2010) menar att om en anställd är medveten om vad koneskvenserna blir om de bryter mot reglerna så ökar deras foglighet gentemot ISPn. Vi menar att detta inte har samma betydelse i den mindre organisationen då det finns många andra faktorer som verkar spela en väsentligt större roll så som *personligt engagemang och professionalitet i arbetet.*

5.3 Abstraktionsnivå:

Hos SUS finns det policys och riktlinjer med olika abstraktionsnivåer som appliceras genomgående i hela organisationen ända ner till varje enskild förvaltning. Brahe Vård däremot kan liknas till en av SUS förvaltningar, de har bara riktlinjer med väldigt låg abstraktionsnivå. Då Brahe Vård saknar något styrande dokument med en hög abstraktionsnivå så saknar de övergripande säkerhetsmål som angår hela organisationen och definierar allmänt vilket ansvar som ledningen och de anställda har (Baskerville, R. & Siponen, M (2002) vilket märks tydligt när man pratar med dem. De pratar om att det finns riktlinjer och regler men att dem inte finns nedskrivna någonstans utan är mer outtalade regler. Det gör att vi fick känslan av att de inte finns någon struktur på deras informationssäkerhetsarbete, utan de mest hittar på nya regler när det dyker upp något nytt som de inser bör regleras. Detta stämmer bra överens med både Gupta & Hammonds (2005)

och Hove et. al. (2014) slutsatser. Gupta och Hammonds (2005) visade att bara 40% av alla mindre organisationer de undersökte hade en konkret informationssäkerhetspolicy medan Hove et. al. (2014) bevisade att alla större organisationen de undersökte hade en informationssäkerhetspolicy på plats.

5.4 Involverad ledning:

Litteraturen understryker hur viktigt det är att ledningen involveras i informationssäkerhetsarbetet och tar det på allvar (Kankanhalli et. al. 2003; Hu et. al. 2007). I vår undersökning visade det sig att ledning är mer involverad i informationssäkerhetsarbetet i Brahe Vård än hos SUS. Det borde ha lett till att Brahe Vård använder sig mer av förebyggande säkerhetsåtgärder än vad SUS gör enligt Kankanhalli et. al. (2003). Detta visade sig inte stämma utan i vårt fall var det tvärtom. Det är möjligt att det stämmer i andra fall men vi anser att även andra faktorer spelar roll, såsom storleken på organisationen och tillgång till resurser.

Att ledningen hos Brahe Vård är så pass involverad i det dagliga arbetet och känner de anställda på ett mer personligt plan gör att de vet vad som motiverar sina anställda till att följa de regler och riktlinjer som finns i organisationen. Bulgurcu et. al. (2010) hävdar att anställda som följer organisationens riktlinjer till en hög grad är mindre trolig att begå regelbrott vilket man i Brahe Vårds fall kan se då de säger sig ytterst sällan vara tvungen att hantera regelbrott. Det är värt att ha i åtanke att bara för att de säger en sak så behöver det inte vara sant, utan påståendet kan påverkas av att de vill framstå som pålitliga i undersökningens ögon.

5.5 Anställdas attityd:

I båda organisationerna upplevs det som att anställda verkligen vill göra rätt för sig men av olika anledningar så får de olika resultat. Vi tyckte det var intressant att informationssamordnarna på SUS nästan fick lura anställda till att prata om informationssäkerhet då de upplevde att deras anställda såg informationssäkerhet som något tråkigt och var motvilliga att diskutera det. Det borde inte behöva gå till på det sättet men det uppfattades som att informationssamordnarna inte visste hur de annars skulle få fram sitt budskap till de anställda, vilket kan skapa problem. Informationssäkerhetschefens åsikt var även att anställda ofta tror att de vet bättre själva vilket kan leda till att dem tar genvägar i säkerhetsarbetet. Tar anställda genvägar och inte följer organisationens uppsatta regler och ISP så leder det till att organisationens säkerhetslösningar tappar sin effektivitet (Backhouse & Dhillon, 2001). För att ändra på anställdas attityder så trycker SUS på att utbildning är en viktig del av lösningen. Siponen et. al. (2014) belyser hur viktig denna ändring är för att påverka anställdas foglighet mot organisationens ISP. Det känns som att SUS är medvetna om problemet och har en lösning i åtanke men sen är det bara lösningens genomförande som lämnar mer att önska.

Brahe Vård har ett annat angreppssätt för att påverka anställdas attityd till det bättre. De satsar på en långsiktig lösning som tar tid innan den är fullständigt implementerad. Brahe Vård vill

fostra fram en mentalitet inom organisation, att de är bättre än sina konkurrenter och att anställda bör känna en stolthet över att jobba hos dem. Tanken är att deras arbetsinsats sedan ska spegla den mentaliteten och göra att regler och riktlinjer följs. Vi tycker det är en mogen lösning som vi inte förväntade oss av en så pass ung och liten organisation som Brahe Vård. Gupta & Hammond (2005) påstår att små organisationer kan ha svårt att välja vettiga lösningar men i detta fallet tycker vi inte att det stämmer.

5.6 Göra anställda medvetna om risker och ansvar:

När det gäller att göra sina anställda i organisationen medvetna om riskerna har Brahe Vård lagt mer fokus än SUS gjort. Det finns flera källor som hävdar att just de anställda är en svag punkt, om inte den svagaste punkten i informationssäkerhet (Warkentin & Willison 2009; Siponen, 2000a; Bulgurcu et. al. 2010). Även om alla intervjuobjekten ansåg att den anställda förmodligen är den svagaste punkten i deras informationssäkerhetsarbete så var det bara Brahe Vård som hade en obligatorisk utbildning gällande informationssäkerhet. Siponen (2000b) hävdar att få sina anställda informationssäkerhetsmedvetna är en lång process där bara en initial utbildning inte är tillräcklig. Lösningen på detta hade för Brahe Vård varit att deras anställda behövt gå uppföljningsutbildning med jämna mellanrum för att förnya kunskapen. SUS informationssäkerhetssamordnare anser att det är omöjligt att få deras anställda att ta sig tid till att gå deras informationssäkerhetsutbildning då det helt enkelt saknas anställda och tid. SUS har många teoretiskt bra lösningar på problem men i praktiken så fungerar de inte alls så som de tänkt. Tittar man bara på deras intranät som har som syfte att sprida information ut genom organisationen så beskriver deras egna anställda det som ett svart hål där man måste veta vart man ska leta om man faktiskt vill hitta något av värde. Fortsättningsvis så har SUS satt upp mål för deltagarantal på deras utbildning men varken arbetar för att nå målet eller följa upp det.

Till skillnad från SUS så använder inte Brahe Vård sig av några teknologiska hjälpmedel, till exempel intranät, för att sprida information vilket gör att det är svårt att ta del av information vid behov. Istället så måste anställda kontakta föreståndaren eller kunnigare kollegor vilket gör att informationen inte alltid är tillgänglig när man behöver den. SUS trots alla sina teknologiska hjälpmedel jobbar likt Brahe Vård i detta sammanhanget. Informationssäkerhetschefen säger att det är vanligt att anställda frågar sina chefer om de är osäkra om någonting, vilket i sin tur kan leda till att de frågar sina chefer. Det kan tolkas som att medvetenheten och kunskapen om informationssäkerhet är generellt lägre hos SUS anställda.

5.7 Hantering av risker:

När det kommer till identifiering och hantering av risker jobbar SUS mer systematiskt än Brahe Vård gör vilket vi anser är direkt kopplat till kompetens. Brahe Vård som saknar en lika djupgående kompetens som SUS arbetar istället mer situations anpassat. Thong, Yap & Raman (1996) menar att mindre organisationer pga. detta har större sannolikhet att missa att identifiera risker och vidta rätt säkerhetsrisker. Detta anser vi stämmer delvis i vårt fall då det finns andra variabler som spelar roll. Informationssäkerhetschefen på SUS menar att ofta påskyndas säkerhetsarbetet vilket medför en överhängande risk att alla risker inte identifieras. I Brahe Vård anser man inte att informationssäkerhetsarbetet påskyndas undan får ta den tid det tar istället. Humphreys (2008) anser att det är viktigt för en organisation att just förankra sitt säkerhetsarbete i organisationen vilket tyder på att SUS är en mognare organisation. Gupta & Hammonds (2005) menar även att ett annat tecken på mognad vid informationssäkerhet är vilken typ av hot man identifierar som det största hotet. Gupta & Hammonds (2005) fortsätter att förklara att små organisationer ofta identifierar yttre hot som det största medan större organisationer vet att statistiskt sett är det största hotet inifrån. I vår intervju med informationssäkerhetssamordnarna på SUS så tog de upp Cloud Hopper attacken och berättade att de börjar se allvarligare på externa hot vilket vi tyckte var intressant. Att de anpassar sig efter dagens verklighet istället för att utgå från gamla rankningar av hot.

I vår undersökning ser vi en mognad hos den mindre organisationen som precis som den större ser inre hot som det största hotet och arbetar mer med dessa precis som SUS. Detta kan förklaras genom att Gupta & Hammonds (2005) undersökning är en äldre undersökning och att resultatet inte hade varit samma idag då mindre organisationen har gått igenom en mognadsfas gällande informationssäkerhet.

5.8 Standarder och ramverk:

Det var svårt att tolka resultatet från denna punkt då ingen av organisationerna arbetar djupgående med något ramverk eller standard. SUS informationssäkerhetschef berättade att de använder ISO 27000 i vissa situationer men att det inte är genomgående genom hela organisationen vilket tyder att SUS ändå är intresserade och medvetna om vad ISO 27000 är för något. Det känns som att resursbrist spelar roll här då en full certifiering inom ISO 27000 hade kostat mer än vad SUS kanske anser att det är värt. Informationssäkerhetssamordnarna som är på steget under informationschefen hade däremot väldigt lite insikt varken vad ISO 27000 var för något samt att de inte visste att det ens användes vilket tyder på precis som informationssäkerhetschefen säger att det inte appliceras i alla lager av organisationen. Hos Brahe Vård anser vi dock att det är förståeligt att inga ramverk eller standarder används då de inte ens har sina riktlinjer nedskrivna än. När vi pratade med föreståndaren om ramverk så visste han att det fanns en ISO-standard för informationssäkerhet men han hade ingen tanke att införliva den i verksamheten inom den närmsta framtiden. Då deras organisation är så pass liten så är det förståeligt att de väljer att lägga sina resurser på annat och kan återbesöka ramverk och standarder när deras verksamhet har växt till sig.

5.9 Uppföljning och övervakning:

Alla fyra intervjuobjekten bekräftade att följa upp att informationen faktiskt hanteras säkert är en av de svåraste bitarna i informationssäkerhetsarbetet. Under intervjuerna uppdagades att båda organisationerna hade svårt att precisera vilka aktiviteter som skulle vara intressanta att mäta och därför valt att prioritera uppföljning lägre. SUS har kommit steget längre då de identifierat vissa områden i verksamheten som är värda att möta men saknar nyckeltal för att mäta. MSB (2015) slutsats att vårdgivarna är mer motiverade till att uppnå lagkraven än att faktiskt generera någon nytta för organisationen tycker vi stämmer bra. Då ingen av organisationerna har resurser i överflöd fokuserar man mindre på uppföljning och övervakning då dessa bitarna inte är något faktiskt lagkrav utan är till för att effektivisera organisationen ge indikationer på hur arbetet går. Istället väljer man att lägga resurserna på proaktiv riskhantering.

6 Slutsats

Frågeställning i vår undersökning är:

Vilka skillnader finns det mellan stora och små vårdorganisationer gällande hantering av Informationssäkerhet?

Vi kom fram till att det finns flera skillnader mellan organisationerna, att Brahe Vård sköter sitt informationssäkerhetsarbete mer spontant och hanterar problem när de väl dyker upp. Medan SUS har fler utarbetade processer för sin hantering av informationssäkerhet, dock så märkte vi att dessa processer inte alltid fungerade i praktiken. Tack vare att SUS har tillgång till mer resurser så leder det till att de kan täcka flera områden av informationssäkerheten även om detta inte alltid görs på ett bra sätt.

En annan intressant skillnad är att organisationerna fokuserade på olika saker när de diskuterade bristande resurser. Brahe Vård la mycket fokus på tid som en resurs, att de med mer tid hade kunnat förbättra sitt informationssäkerhetsarbete. Medan SUS pratade mer om avsaknaden av pengar och arbetskraft. Tid uppfattas som viktigt för Brahe Vård då de inte har någon IT eller säkerhetsanställd vilket leder till att alla förändringar inom deras informationssäkerhetsarbete tar längre tid att genomföra.

Det finns även ett antal punkter som organisationerna gör olika bra. Brahe Vårds ledning är väldigt engagerad i allt som sker i organisationen och känner sina anställda på ett personligt plan. Det leder till att ledningen vet vad som motiverar anställda till att utföra ett bra jobb och följa de riktlinjer och regler som finns. Detta är möjligt tack vare att organisationen är så pass liten och är omöjligt i en större organisation som SUS vilket vi upptäckte att så var fallet. SUS har istället ett mer strukturerat och teoretiskt korrekt informationssäkerhetsarbete där de jobbar i högre grad med IS-policys, riktlinjer, riskhantering, övervakning och uppföljning. Dessa skillnader gör att SUS informationssäkerhetsarbete är mer proaktivt än Brahe Vårds där man jobbar mer reaktivt. Det Brahe Vård dock gör proaktivt är att de tvingar alla nyanställda att gå en internutbildning där de lär sig om hur utför sina arbetsuppgifter på ett informationssäkert sätt.

Undersökningen visar att den större organisationen har fler verktyg och processer dedikerade till informationssäkerhet och har en djupare förståelse av vikten av informationssäkerhet. Det resulterar i att de på pappret har ett bra informationssäkerhetsarbete men i praktiken så kan den framtagna systematiken fallera och inte fungera så som det var tänkt. Resultatet visar även att den mindre organisationen är mer fokuserade på att bara uppnå de krav som ställs och hanterar informationssäkerhet på ett mer reaktivt sätt. Medan stora organisationer har svårare at förankra delar av informationssäkerheten i organisationen.

6.1 Förslag på vidare forskning:

En liknande undersökning men på en större skala hade kunnat ge mer generaliserbar data som hade kunnat spegla branschen på ett korrekt sätt.

7 Bilagor

7.1 Intervju med Informationssäkerhetschefen (SUS)

M = Markus, D = David, J = Johan

M: Vill du berätta lite om dig själv?
J: Ja vem är jag, jag är informationssäkerhets chef på region skåne. Jag heter Johan Reuterhäll, jobbat här i, va blir det, snart 2,5 år. Så jag är inte så gammal här. Kommer från Länsstyrelsen, Skåne där jag var tidigare, jobbade med säkerhet. Ja vad jag gör, jag ansvarar för vårt ledningssystem för informationssäkerhet och ser till att region skåne har effektiva processer för att arbeta med informationssäkerhet och ställer rätt krav vid upphandlingar, anställningar. Ja det är egentligen hela ISO27000 då som det omfattar. Och ja det är ett ganska stort jobb med tanke på att det är en rätt stor organisation. Vi är på rätt väg i alla fall men det återstår mycket, man blir aldrig klar med det så att säga. Men det är det min uppgift är att ansvara för ledningssystemet.
M: Sen är du med och utformar, eller är du med och sätta det i kraft också? Eller gör du både och?
J: Det är både och. Jag fram styrande dokument på övergripande nivå. Jag ska jobba strategiskt som det heter, när jag blev anställd. Men det låter ju jättefint men i praktiken så behöver man liksom vara med faktiskt och göra någonting operativt också, och det har inga problem med, utan det är faktiskt väldigt viktigt att vara med och, innan man gör riskanalyser och sådär också, och testar det man tar fram naturligtvis. Så att det är både och.
M: okej, så att när man ser till just informationssäkerhet, för att jag förmodar att du gör hur mycket som helt med säkerhet, både patientsäkerhet och, eller du har hela…?
J: Ja det är hela, så att det är klart att mycket fokuserar kring patienteruppgifter, eller det heter ju personuppgifter inom hälso- sjukvården. Men det är klart att kanske, 80% av all information rör ju det, och det är ju oftast där det blir mest att göra. Men vi har även skånetrafiken, dem tillhör också region skåne. Sen har vi kulturskåne och sådär men det är lite mindre. Men så annars så är det ju dem här tre, dem här vårdförvaltningarna SUS, KRYS SUND. Vilken var det mer, jag har glömt den andra bara för det. Sen har medicinsk service som har nej hade, hand om IT, men det handlar om medicinsk teknik och labb. Sen har vi regionservice som har hand transporter och byggnader, drift av vatten och kyl och allting sånt där. Men det är klart det är vården och den informationen inom vården som tar mest tid. Men det andra är precis lika viktigt.
M: Det är såklart alla bitar, men är det så att ni behöver lägga mer tid på säkerhetsinformationen inom vården jämfört med dem andra delarna? Jag tänker skånetrafiken kanske inte är riktigt samma…
J: Nä det mesta tiden behöver nog läggas i vården för det är mest patienter och mest sekretess. Alltså det är mest personal inblandad i den verksamheten. Så det är där fokus ligger just nu, men det är ju så att inom skånetrafiken finns det också information som ska vara riktig och konfidentiell och tillgänglig. Men dem, dem får komma lite senare, just nu är fokus på vården.

D: Om man kollar på vården, vad ser ni som organisation som det största ah liksom, som det största problem eller hot mot informationssäkerheten? just patienternas då
J: Det största hotet ja, det största hotet är att alltså om man inte får till den här systematiken så vi gör våra riskanalyser och att man missar och vidtar säkerhetsåtergärder som gör att patient-information kommer ut. Vi ska ju lansera massa e-tjänster nu, strategin för det är hälsostrategi, ska ta fram massa e-tjänser, vi ska digitalisera våran verksamhet. Och gör vi inte rätt där och har hög kvalité så är det klart att då riskerar vi patienternas, alltså journaler och sånt. Och det är det värsta som kan hända, det är ett stort hot. Alltså att det går så snabbt att vi inte hinner göra ett jobb med hög kvalité. Men det är klart att omvärlden förändras ju också, ja ni vet ju själva vad som hände senast förra veckan, civildrabbade, det är ju saker att när vi upphandlar tjänster och vilka krav ställer vi där, det hör ju ihop med det jag sa, att vi ska ställa krav på våra leverantörer och utbilda vår personal och hantera informationen korrekt.
D: Riskanalysen du pratade om, hur ser den processen ut när ni arbetar där? Hur startar ni upp det?
J: Ja i den bästa av världar om jag säger så, och ibland så, det börjar fungera, vilket är en av det största sakerna jag jobbar med, så ska ju det här vara en del av beslutet att införa ny (slut-tjänst?) i ett system. Då ska man börja fundera över vilka krav på informationssäkerhet som finns. Det är både lagkrav och verksamhetens krav. Sen ska det vara en del i hela den processen då, bli en del av en upphandling eller ett utvecklingsarbete, att vi får ett system som håller rätt nivå. Men det är som sagt den bästa av världar och ibland funkar det, det funkar bättre och bättre. Och det är det jag håller på och bygger upp, den processen, och det är ju inte bara nya system utan det är när vi anställer folk till exempel, anställer ny personal så ska ju det vara med, med informationssäkerhetsaspekten och det. Och dem avtalen vi redan har idag, hur ser dem ut. Säkerställer vi att informationen hanteras korrekt, ja det här GDP som är på väg, dataskyddsdirektivet som också kommer ställa massa krav på informationshantering av person-uppgifter. Ah, så att nä det är mening att det ska vara en systematik i det.
M: Får ni, jag förmodar kanske att om det inte funkat så bra så beror det på att säkerhetsbiten inte har fått sin del i projekten, alltså att tycka till tillräckligt mycket, är det nu, blir det bättre, det är det du försöker att säga?
J: jaja visst, jo så är det. Nä men det är så att fokus kanske inte har legat så mycket på det här med säkerhet
M: Nej, ja jo av min egna arbetslivserfarenhet så vet jag att den biten kan vara så att dem som inte jobbar med det tycker att, varför.
J: Nä precis, hade man jobbat i försvarsindustrin eller någon myndighet där man har, där det är en annan typ av kompetens som jobbar. Som kanske jobbar i försvaret eller andra säkerhetsmedvetna myndigheter, då är det ett annat fokus på dem här frågorna. Då vet man ju vilka, oftast vilka risker som finns, och vilka andra som vill komma över ens information. Men så är det inte här, utan här man tittar väldigt mycket på att verksamheten ska vara effektiv och det ska vara enkelt, man ska åtkomst till all information, det är oftast det. För att annars är det patientosäkert, och så gör man avkall, man liksom springer förbi dem här säkerhetsfrågorna och tror att informationssäkerhet bara är ett hinder, alltså att det handlar om att sätta stop för personal att få åtkomst till information. Men det är ju en missuppfattning, för det är inte alls det det handlar om, det är precis tvärt om. Meningen med det här är ju att de ska ha tillgång till den information de behöver. Men det är liksom en pedagogisk grej att lösa alltså

en utbildningsfråga. Det är ju ingen teknikfråga utan det är liksom, det är mycket parallelt här, det är mycket teknik och (processutbildning?) och liksom få det där att, det tar tid i en sån här jätteorganisation. Sen har det inte funnits, det finns fortfarande inte speciellt mycket resurser. Det saknas ju resurser i egenskap…
M: Gäller det generellt även i dem interna avdelningarna?
J: jaja visst
M: För det har man hört mycket om alltså på avdelningarna på sjukhuset men det är samma?
J: ja det gör det, jo det saknas resurser. Jag jobbar på heltid, hela region skåne. Sen har varje förvaltning en informationssäkerhetssamordnare då, som ska arbeta med informationssäkerhetsfrågor, men det har dem, det är ingen heltidstjänst dem har utan dem arbetar med det som en extra uppgift. Vid sidan om av andra uppgifter de har fått på sig då.
M: Är de säkerhetsanställda, eller dem är något annat som jobbar med säkerhet också?
J: Lite blandat, några av dem jobbar ju på säkerhetsenheten. SUS till exempel där sitter ju, har ju två säkerhetssamordnare som jobbar på att säkra säkerheten. Men det är ju för vissa förvaltningar så ibland jobbar de i staden och ibland sitter de någon annanstans och det liksom funkar, det är varierande. Även utbildningen varierar, hur mycket tid de får lägga på det så här. Och då blir det ju eftersatt. Väldigt IT styrt har det varit också och är fortfarande. Det är mycket att man litar på att IT ska fixa det här med IT-säkerheten så glömmer man det här lite bredare.
D: Du nämnde förut det om, det är viktigt med utbildningsdelen av personal också. Är det någonting som ni erbjuder här också, eller förlitar ni er på att dem får den utbildningen i sin tidigare utbildning? När dem utbildar sig till läkare eller sjuksköterska.
J: Nä utan vi har en E-utbildning i informationssäkerhet som vi tagit fram. Den är inte obligatorisk. Nu ska vi, vi håller på att ta fram mål för informationssäkerhet och där kommer ett av målen vara att alla anställda ska gå den här grundläggande utbildningen och att det ska följas upp, och att nyanställda ska gå den inom en månad och ska repeteras var tredje år. Men den är inte obligatorisk, och innan den blir det och att man följer upp den så är det inte så många som kommer att gå den heller.
M: Men då, den utbildningen gäller informationssäkerhet? Inte patient, nu tänker jag dem andra delarna med behandling och så vidare
J: Nä det är bara informationssäkerhet, man hanterar sekretess, ja ofta sekretessbelaggd information, vad man ska tänka på. Både fysisk säkerhet och hantering av handlingar.
M: Har ni ett system till alla era, typ ett journalsystem där ni har det mesta som är sekretess?
J: Nä vi har hur många system som helst.
M: som alla andra organisationer.
J: Ja ja visst. Men jag vet inte om det är en mardröm eller himmelriket. Men det är ju väldigt många system, som sällan pratar med varandra.
M: Och där det finns, som innehåller uppgifter som är skyddade?
J: Ja det är i princip bara journaluppgifter. det är labbprover, det är även andra uppgifter som handlar i de här, röntgenbilder…
M: Ja juste det är dem grejerna som vi inte riktigt tänker på.
J: Ja så att det finns jättemånga olika system. Nu håller vi på att upphandlar ett nytt system som ska ersätta väldigt mycket av det gamla, så vi får ju se om det blir bättre då.

M: Är det något som kommer fler i närheten, för det har, är det inte att alla sjukhus har olika system också eller är det samma?
J: ja det har varit, sen slogs de ihop. Så det är en central IT organisation, meningen är ju att ett system ska köpas in och ska vara centralt.
M: Ja okej. Är det region skåne eller hela sverige?
J: Ja det är region skåne.
M: Så att skåne har samma, sen så sköter dem andra sig själva
J: Ja nä precis, det är olika system.
M: så klart, varför göra det lätt.
J: Nej precis. Nej utan det är, det finns ju ett visst samarbete, vi samarbetar inom informationssäkerhetsområdet. Men det här med att samverka, att samarbeta och upphandla ett gemensamt system, för flera landsting, tillsammans, det har ju inte funkat.
M: Har man försökt?
J: Ja ja. Den upphandlingen vi håller på med nu började som en gemensam upphandling med stockholm och västra götaland men det sprack ju vart efter och vi klev ju ut ur det för något år sedan och gjort en egen upphandling. Så att det, det är ju lite synd men det är så det är.
M: Har det någonting med att kraven är olika? från olika…..
J: Nej det har att göra med att, tror jag, framförallt att vi har kommit olika långt. Stockholm har kanske inte kommit lika långt som vi har när det gäller att konsolidera olika system och många olika instanser av ett system, då de har flera olika bolag inom sitt landsting. Västra götaland vet jag inte varför det inte fungerade, det kanske var någonting annat som inte funkade. Det är nog en blandning av teknik och relationer, jag vet inte. Men det har inte gått, och nu upphandlar vi ett eget.
D: Om vi återgår lite till det där med utbildningen, finns det något sätt för er att fullfölja att era anställda verkligen följer dem här reglerna ni sätter upp också?
M: Stickprov och, alltså hur ni säkerställer att inte folk springer runt och bryter mot, jag förmodar att till exempel att skriva ut journaler och ta hem inte är okej liksom.
J: Ja vi har ju stickprov, vi ska ju, vi har en anvisning som säger att 10% av personalen ska granskas per månad under ett dygn. Det är ganska mycket, det är 34 000, nu är inte alla vårdanställda men det är väldigt många personer då som ska kollas upp. Det som kontrolleras då är vilken åtkomst, alltså vilka patientjournaler ,vilka patientuppgifter dem har tittat på. Så det är ju den stickproven som ska göras, som beslutat. Det är ju helt slumpmässigt så att säga, så det är ganska stor risk att man inte upptäcker någonting.
M: så det är stickprov…
J: ja så alltså det är stickprov, vi har inget automatiserat som liksom tittar på olika händelser, men det är någonting vi skulle vilja ha, så att säga. Men det nuvarande stora journalsystemet, den databasen är inte byggd på ett sätt som gör att det är enkelt att göra de här avancerade analyser, utan det är manuellt, tar mycket tid. Men det är det vi gör gällande patientuppgifter. Sen alltså övrigt, övrigt så har vi inga sådana beslutande åtgärder, att man ska göra granskningar eller så. Det är om det inträffar incidenter, då får man titta närmare på det. Det finns ju regler för det här med att ta hem journaler också, det ska man ju inte göra om man inte kan säkerställa att dem skyddas mot obehöriga, och det är ju jättesvårt, så det finns inget förbud men arbetsplatsen ska ju vara så säker så att andra i familjen inte ser, det är ju helt oacceptabelt. Och det gör det väldigt svårt att arbeta hemma.

M: Ja vi har faktiskt just det, alltså hur är det att arbeta, har ni att man jobba på plats bara? Eller kan man jobba remote?
J: Nej man kan jobba hemma.
M: Men det gäller kanske inte för, eller är det för läkarna kanske?
J: nej jag tror det är upp till, det är upp till den chefen då alltså, som får besluta om en anställd får ta med arbetsuppgifter och sitta hemma och jobba.
D: Ligger det på den chefens ansvar då att det görs säkert liksom?
J: Ja, dem är ju ansvariga för sin verksamhet så att, även den informationen de hanterar. Så det ska ju ske säkert och det finns en anvisning om det där, där det står om just det här att säkerställa att obehöriga inte kommer åt.
M: Då är det något beslut som ska tas det här med att jobba hemifrån? det är inte bara vem som helst som bara, nu kan jag jobba hemifrån.
J: Nej men det är ju oftast, ibland är det från chef till chef och beroende på vad man jobbar med. De flesta har ju inte möjligheten att sitta hemma. Utan det är ju vissa som har det. Men jag tror att det förekommer, men det är svårt just på grund av det här med sekretessen. Sen slarvas med allting förmodligen, det tas säkert hem såna uppgifter och sådär, men det är ju absolut inte meningen att det ska gå till på det sättet isåfall.
M: ni har ingen sådan speciell, typ Citrix eller remote säkerhet?
J: Jo jo, vi har vpn som man kopplar upp sig.
M: Så då måste man egentligen, för att jobba hemifrån, få vpn uppsatt, det är inte bara att tuta och köra?
J: Nej dem som jobbar hemma kopplar också upp sig, dem kopplar nog oftast upp sig via vpn. Jag vet inte exakt den personal i vården som tar med sig, är det medicinska sekreterare vilka som är det som skriver ut journaler, diktatamen och så vidare. Men jag tror inte det är så jättevanligt. Men det flesta gör det nog på jobbet alltså. Svårt att se det alltså
M: Slipper ta med det hemåt så det kan vara skönt.
J: Ja och vi som jobbar med annat, administration alltså, vi ska ju inte ha kontakt med journaluppgifter. Jag har aldrig det, så dem flesta har ju inte det. Det kanske är möjligt att dem som jobbar med uppföljning och sånt där, men det är inte meningen att dem ska gå ner i enskilda patienter och se den typer av uppgifter, det ska hållas till ett minimum liksom.
M: Och ni håller bara på med intern sekretess, alltså era affärshemligheter och så vidare?
J: Ja, riskanalyser och sånt där, det är ju inga patientuppgifter, det är annan typ av sekretess.
D: Ivo, det är dem som kontrollerar er också
J: Nja de är en tillsynsmyndighet
D: Ja precis, men hur fungerar det sammarbetet?
J: Det är inget sammarbete, utan dem är tillsyn, de har hand om tillsynen så att om det inträffar en händelse så är ju vi skyldiga att anmäla det till IVO och så kan dem göra en granskning, alltså en utredning av det.
M: Är dem kravställare också då, eller är dem bara granskare?
J: Nej dem är en tillsynsmyndighet så att, som landstinget följer gällande lagar och föreskrifter. Händer det någon incident gällande information eller utrustning eller något annat som riskerar patientsäkerheten exempelvis så kan ju IVO göra en utredning så att dem kan förelägga oss med olika saker.

M: är det någonting som, har ni någon kontakt med IVO i jämna mellanrum eller är det väldigt väldigt sällan?
J: Det är dem ärenden i så fall, då gör ju dem en utredning. Så är ni intresserade av sånt så kan ni ju begära ut dem handlingarna ifrån oss ju. Det va en incident förra, vad var det, förrförra året det va ju nätverket i Kristianstad som blev överbelastat vid en uppgradering av en programvara. Så där va ju IVO och gjorde en tillsyn då, eller granskning, tillsyn får man nog kalla det. Och den håller dem på att följa upp just nu faktiskt. Men jag vet inte något mer om det.
M: Är det, va sa du, tvåtusen….
J: Ja 2015 tror jag det inträffade, våren 2015
M: så det är långa processer?
J: Ja det tar jättelång tid innan dem kom till skott, dem kom och granskade förra året tror jag om förra våren, och vi hade möten här då, och nu håller dem på att följa upp det underlaget och vad vi har gjort egentligen. Men det ligger på IT och redovisningar.
D: Gör dem så här, kommer dem oanmälda inspektioner på något sätt eller är det bara vid anmälningar?
J: Det vet jag inte, det tror jag inte. Jag tror inte dem har sådana, vad ska jag säga, dem kommer inte bara hux flux. Jag tror, ni får kolla på deras sida, men jag tror att det är anmälningar som kommer antingen från oss eller från allmänheten då.
M: Det verkar som att dem har mycket att göra ändå.
J: Ja dem har tillräckligt ändå, utan att initiera egna, men dem kan säkert initiera egna också men jag vet inte i vilken utsträckning dem gör det, det vet jag faktiskt inte.
M: Du nämnde innan ISO, att ni följer….
J: Ja, 27000
M: 27000, är det det som, det är det ni valde att, är ni certifierade inom det?
J: Nej.
M: Ni följer det bara?
J: Ja det är det vi använder för informationssäkerheten.
M: och ni har ingen annan typ av ramverk eller certifiering?
J: Nej
M: ITIL…
J: Jo IT använder ju ITIL för att få en effektiv förvaltning av systemen så att säga, det finns en förvaltningsmodel som baserar sig på ITIL, det gör vi ju.
M: Ni är inte certifierade där heller?
J: Nej, nej.
M: ni har valt er egna inriktning?
J: ja en egen, en egen variant.
M: Ja det brukar vara att man gör det, det är nästan vanligare.
J: jo men det tror jag, en egen variant
M: Ja det blir så mycket man ska följa
J: och den där PN3, är också en till sån. Så man blandar ihop allt möjligt då så att det ska passa.
D: En go blandning

J: Ja både på gott och ont, det blir ju liksom inte riktigt, kanske alltid det bästa, naturligtvis om man håller på att plocka det man tycker är bästa utan då, det blir liksom varken eller.
M: Det brukar vara en god tanke, är det ofta att man ska
J: Ja, man kanske inte får alla fördelar som det. Men nu har dem förmodligen tänkt igenom det där. Men det blir som sagt, det är deras, dem kör ju ITIL och jag försöker trycka ihop det som har med informationssäkerhet i deras processer då också då. Så det är också det jag håller på med.
D: Okej.
J: för det saknas nämligen en del modeller idag, informationssäkerhets, det systematiska informationssäkerhets arbetet finns inte med i det utan det är mer förvaltning av drift. Alltså av system, systemdrift, systemförvaltning. Jätteviktigt.
M: den här incidenten som du nämnde, det va ju den här jättestora med IT-driften i Kristianstad. Är det, har ni mindre, den absolut största säkerhetsboven i våra ögon är den anställde i sig. För det är dem som kan göra fel, en dator gör ofta inte fel om man satt upp den rätt. Men den anställde kan ju göra lite som dem vill och känner, och skita i vissa policys som dem inte tycker är så viktiga. Har ni problem med det? Eller det kanske inte har hand om som sitter högt upp?
J: Anställda?
M: Ja
J: Jo det är klart att det, det är klart att det finns problem med det också. Och det är därför vi behöver utbilda dem så att dem gör rätt. Men det är så att, det är ju inte alltid att dem känner till alla regler, och det kan vara nya som inte vet ska göra och, ja menar även om dem gör rätt så kan det bli fel ändå. Råka skriva ut saker på fel skrivare, eller det kan vara så att de råkar glömma någonting eller att dem, alltså det är mycket som kan gå fel i såna stora organisationer.
M: Kommer IVO och granskar även i såna lägen?
J: Ja det kan dem göra om det kommer en anmälan på det ju, så kan dem granska det. Det tror jag ingår i deras uppdrag.
M: Ja jag tänkte bara på i vilken utsträckning som..
J: Nej, nej det är inte alltid att jag får reda på sånt, jag vet inte men det kan ni bara begära ut från diariet här. Alltså alla ärenden som kommit in från IVO det senaste året. Sen vet inte jag, begär ut det bara.
M: Ligger det här, kontaktar man dem här på plats alltså?
J: Ja det finns nog på Skane.se, eller så kan ni åka till diariet och tror diariet att Skane.se ha, men det står kontaktuppgifter. Då kan ni begära ut alla anmälningar som har skett tidigare, det senaste halv-året eller, så får man en lista på det. Det kan ni ju börja att kolla med
M: Ja det skulle man kunna göra
J: Då får ni lite mera hum om vad det är som händer i samband med anmälningar och se vad resultatet blir av det
M: Men till dem anställda, känner du att det ofta är okunskap eller om det ofta är att dem tror att dem vet bättre? Eller du har inte riktigt..
J: Nej men jag tror att, i min erfarenhet så är det väl en blandning. Alltså ibland vet dem inte, ibland vet dem fast dem går runt det eller kanske inte tycker att det är så viktigt. Så det är nog en blandning, men jag har inga konkreta såna fall. Men det är ofta en blandning av okunskap

och att man tycker att det här kanske inte gäller mig, så man tar en genväg eller någonting. Men det är, det är lite så det är ju. Det är därför utbildningen är viktig också, att man inte ska göra så. Då får man hitta på tekniska lösningar som innebär att det inte går att göra fel, men det är jättesvårt, det är i princip omöjligt.
M: Och det ställer ofta till problem för dem som då väl sköter sig?
J: Ja jo precis, jo det gäller att hitta den här avvägningen, ja mellan liksom åtgärder och utbildning, så är det ju.
D: Får det några konsekvenser för anställda om man upptäcker att de inte följer reglerna?
J: Ja det kan det få.
D: Eller det kanske ni inte kan prata om?
J: Jodå det är ingen hemlighet med det utan, om vi har en anställd till exempel som tittar på en journal utan att ha rätt till det så kan de ju bli, ja dem kan, dem blir väl oftast anmälda då för olaga dataintrång. Så det kan ju leda till att de blir av med sin anställning.
M: Men det har inte med det här Lex Maria och det här att göra? Det är mer patientvården eller?
J: Ja det där är ju mer dataintrång.
M: Då är det riktiga IT, alltså vanliga…
J: Ja då tittar dem, och det kan vara pappersjournaler också. Men oftast så upptäcker man ju det när det är ett IT system, alltså att dem har tittat på uppgifter dem inte får, i granskningarna då. Att dem tittar på släktingar eller en känd person som ligger inne till exempel. Så det kan ju få jättestora konsekvenser, om man gör något sånt.
M: Sköter ni det internt, eller är det också något som går över på IVO om det är dataintrång?
J: Nej det blir en polisanmälan på det
M: Så då är IVO inte med i den biten?
J: Nej inte när det gäller det, då tror jag inte att det hamlar hos IVO. Utan det är om det handlar om patient, dem har hand om det om det blir en risk eller fara för patienter. Dem gör säkerhetsfrågor, om det hade kunnat inträffa, om hade kunnat hända eller leda till någon patient, eller om det har gjort det, alltså både och. Alltså både händelser och incidenter. Men just det där med dataintrång det hamnar inte hos IVO, det tror jag inte, det blir en polisutredning då.
M: Då är det ni som lägger en polisanmälan?
J: Ja precis.
D: Är det även samma för sammanhållen journalföring? Jag har läst att man måste uppfylla vissa krav för att kunna få tillgång till det, men om uppfyller alla krav, men känner att de verkligen måste ha tillgång till den här informationen, men dem fortfarande inte får det, ah så kommer ni på det på något sätt…
J: Du tänker att om en vårdgivare då, eller ah, ni vet vad sammanhållen journalföring är?
D: Ja typ, att man delar med sig…
J: Ja det är att man ska kunna titta i en annan vårdgivares journal, under vissa förutsättningar. Jo men det är det här med att olika vårdgivare ska kunna dela journaler. Alltså att vi ska kunna titta i Stockholms journaler. Om vi får en patient så kanske vi vill, vi har inga uppgifter om patienten så kollar vi liksom i, vi har något som kallas nationellpatientöversikt. Då kan vi kolla om det är någon annan vårdgivare som har information om den här patienten, och ja, då kanske det visar sig att det finns i Stockholm, dem har uppgifterna, och då väljer man då att

titta. Ja och då finns det två, antingen är det nödöppning eller samtycke från patienten. Nödöppning är om patienten inte kan samtycka om den är medvetslös eller något. Och samtycke är, aha okej det är okej att vi tittar. Och då kan man gå in och kika, då ser man då vilka, vid vilka vårdenheter det finns uppgifter så kan man gå in och titta då, vad det är för uppgifter. Så det är en flerstegsraket i det här att det aktiva valet finns. Men det är samma sak där alltså, tittar man på en patientuppgift, även om det är i Stockholm eller är i ett annat landsting utan att, har du inte samtycke och det inte är nödöppning då är det ju dataintrång.
D: Det var jag lite oklart innan, Vårdgivare, då är det själva institutionen och inte en läkare?
J: Nä, vårdgivare är region Skåne, det är en vårdgivare. Så det är ingen person. Det är själva vårdorganisation. Alleris är en vårdgivare, Stockholm läns landsting. Jag vet inte hur Stockholm har i och för sig, det är uppdelat i olika nämnder. Hon oss är ju region Skåne, jag är lite osäker där. Om det är. Vad heter det, nämnden. Hälso- och sjukvårdsnämnden, tror jag företräder vårdgivare i region Skåne. Men det är vårdgivare och sen är det vårdgivare och vårdenhet enligt patientdatalagen. I vårdgivaren finns ett antal vårdenheter, och det är det allting baserar sig på. Det här med inre och ytter sekretess, spärr av journaluppgifter. Kan man spärra både mellan vårdenheter och vårdgivare. Så det är en hel uppsättning olika regler beroende på vilket syfte man ska titta på uppgifterna så är det olika saker som gäller. Så det är rätt snårigt innan man har…
D: Det låter rätt avancerat…
J: Ja, men det där ska ju sjukvårdpersonalen känna till och verktygen ska vara utformade på ett sätt som gör att det här bara sker av misstag utan dem ska ju svara, så får de upp en ruta. Har du samtycke eller är det nödöppning och sen får de ju välja. Och det där loggas ju.
M: Okej. Och det förmodar sker inte lika ofta som man tittar på sina egna journaler så det är väl någon högre kontroll på dem också? Det kan väl inte vara ofta?
J: Nä, det ska ju ingå också. Det är ju i loggen och det är ju ganska så…så ja.
M: Du var nyanställd i 2,5år och ni har massa nya projekt, är det någon lite extra satsning på säkerhet från ledningen eller va det en försättning…
J: Du tänkte att jag anställdes?
M: Ja, det brukar vara så. Ni skulle jobba med det och att ni inte riktigt var där?
J: Jaja, Nänä men såhär då. Min företrädare gick i pension ju och det va därför jag började här och tidigare har man fokuserar mycket på patientintegritet. Det fanns en del… Här sa man att man hade ett ledningssystem för informationssäkerhet. Men det bestod egentligen bara av en hög med anvisningar om hur vi ska hantera patientuppgifter och sekretess, såhär gör du, såhär gör du. Men det fanns liksom ingen process, det fanns liksom ingen ordentlig grund att stå på, att så här jobbar vi i informationssäkerhet, riskhantering, informationsklassificering, ingen modell för det här. Det saknades liksom det här grunden och det är de jag håller på att bygger upp nu. Mycket av de här grundgrejerna finns när det gäller just sekretess i sjukvård, logghantering, skyddade personuppgifter och det här. Men det finns systematiska ????(33:17) och det är det jag jobbar med och det som sker just nu att vi bygger upp den här grundstommen, plattan att stå på, den här grundläggande, styrande dokument, lite större riktlinjer för informationssäkerhet, mål för informationssäkerhetsarbeten för att komma ifrån de här brandkårsutryckningarna och relaterade arbeten som har varit. Att det blir mål fokuserat, att de får resurser till det här. Så har det inte riktigt varit och det är det jag håller på med. Stockholm ligger

före oss, de har hållit på i flera år. Och det är nu de har börjat med att följa upp säkerhetsarbetet. Det kan ju inte vi. Jag har ingenting att följa upp.
M: Inga nyckeltal eller…
J: Nä precis, inga nyckeltal. Det finns inga krav, liksom inte ska-krav att följa upp verksamheterna mot. Hade vi haft det hade jag kunnat ställa frågor på alla de här, har ni gjort det här? Har ni gjort det här? Har ni gjort det här? Kunna samla in och ta fram statistik och visa för ledningen men det finns inte idag.
M: Är det ett nytt krav att ha detta eller är det något själva känner att det hade varit bra för oss?
J: Nja, jaa. Behovet har funnits hela tiden. Men det har ju blivit ett större fokus på det nu tror jag. Jag försöker ju sätta fokus på det och sen är det ju den här digitaliseringsstrategin vi har och det händer ju jättemycket i omvärlden nu också det senaste året. Det är ju nästan i tidningen varje vecka om incidenter gällande informationssäkerhet. Så liksom ögonen öppnas ju upp då det kommer mer lagstiftning i området. Så man måste jobba med det och gör vi inte det då riskerar vi ju det här vi bygger upp nu att det blir osäkra tjänster som allmänheten inte vill använda. Jag menar ni vill ju inte använda en app från region Skåne om det visar sig att den läcker era patientuppgifter.
M: Nejnej, det är klart.
J: Nä det är klart ni inte vill och då har ju region Skåne misslyckats med målet liksom ju. Vi vill ju att medborgarna ska använda apparna ju. Det effektiviserar, vi vill ju helst inte att de ska komma till oss för det blir bara jobb. Att man kan svara på frågor redan innan att de inte ska behöva ringa eller behöva komma att man kanske får svar på sina frågor ändå, på ett säkert sätt då. Men det misslyckas ju då om man inte lyckas få så säkra appar då så att patienterna vill använda dem. Så därför är det ju jätteviktigt det här jag försöker föra fram då men det tar lång tid, det är trögt, folk som ska övertygas och det finns de som ser det som ett hinder.
M: Har du stöd från ledningen eller är säkerhet inte så prioriterat?
J: Nä, det är det inte. Nä, just nu kan jag väl säga att det inte finns sådär jättemycket. De tycker att det är viktigt och jag möter väl inte på något jättestort motstånd men när man börjar på att gå ner mer i detalj och man vill att regionstyrelsen ska fatta beslut och riktlinjer som är ganska detaljerade då kommer de skruva på sig, det tror jag iallafall. För då börjar det komma närmare och då kommer det ställas krav och då kommer det kosta pengar och så kanske det försenar saker och ting som man tänk sig.
D: Så de är inte jätteinvolverade i själva arbetet utan mest och de skriver på någonting om det skulle behövas?
J: Ja, jo men det är lite så. De har ju rätt många andra frågor också att stå i så att. Men de är ju ansvariga för informationssäkerheten så de måste ju sättas in i det här. Så vi får väl se nu när det går vidare med det här och hur det kommer att gå, reaktionen bli, de är spännande.
D: Den nya dataskyddsreformen som kommer om något år. Har ni börjat planera inför den någonting eller startat arbetet?
J: Ja, vi har tagit fram en handlingsplan för anpassning till det här dataskyddsdirektivet, det börjar gälla i maj nästa år.
D: Nästa år, okej.

J: Maj 2018, ja det är lite drygt ett år. Så det kommer ju bli jättemycket jobb att hantera alla personuppgifter i hela region Skåne.
D: Det kan jag tänka mig.
J: Ja men det är ju lite jobb.
M: Den betyder då att ni ska gå igenom alla, allt ni ligger inne på eller? Har ni allting i elektronisk form eller ni sitter på…
J: Nä, det här gäller ju bara elektroniska system. Automatisk databehandling eller vad det står i den här, patientuppgiftslagen. Så det är ju inte papper, utan allting är ju elektroniskt. Nästan alltid är elektroniskt.
M: Så ni har lyckats konvertera allt till…
J: Nä, men det är ju väldigt mycket, det mest är. Vi har pappersarkiv också men det scannas ju in. Det finns ju jättemycket uppgifter. Så allting ska ju gås igenom så det är ett jättejobb ju. Inventera allting och kolla vilket syfte vi hanterar det här då. Patienter, det är dem som personuppgifterna då handlar om, är de informerade på korrekt sätt och vilket syfte, så det är ett jättejobb. Så det håller vi på att startar upp det personuppgiftsombudet som håller i det, som är projektledare. Jag är väl lite delaktig men jag försöker hålla mig lite på sidan av kan jag väl säga, det är rätt mycket med det där.
D: Ja, det kan jag tänka mig.
J: Men det är ju en jättebra dragkraft till informationssäkerheten.
M: Du kan trycka in mycket annat…
J: …samtidigt ja! När ändå alla personuppgifter ska inventeras så kommer det behövas gå igenom alla system och allting och titta vad som finns och när man ändå håller på med det så kan man göra annat samtidigt. Så då blir en dragkraft till mig också så att säga, jag kan ju göra andra saker också, andra saker samtidigt och sen är det ju informationssäkerhet det handlar om faktiskt. Det är ju personuppgifter men det ställs ju krav hantering av personuppgifter. Men det finns ju andra krav förutom dataskyddsförordningen som ställer krav på hanteringen av personuppgifter och sekretessbelagd information.
M: Vilka tänker du på då?
J: Patientdatalagen t.ex. offentlighets- och sekretesslagen ställer krav på information. Så man kan ju göra flera sker samtidigt. Så det här är bara en del men eftersom det är ny lag och nu är det tight med tid tyvärr men då kan man göra annat på en gång så det blir en bra skjuts för hela informationssäkerhetsarbetet tror jag, så det är bra.
M: Innan du blev anställd som så hade ni inte grunden men ni hade, va var det, policys som ni hade en hel del som låg…
J: Policys har inte funnits, det har funnits en säkerhetspolicy som är oerhört gammal och den håller vi på att arbeta om just nu. Det kommer inte stå så mycket specifikt om just informationssäkerhet utan det är säkerhet i största allmänhet. Sen kommer det bli en säkerhetsstrategi och där kommer det stå lite grann om hur vi ska, vilken strategi vi ska ha när vi jobbar med säkerhet. Men det som är viktigt för mig är den här riktlinjen för informationssäkerhet för där kommer vi slå fast hur…vilket ansvar vilka delar av organisationen har i informationssäkerhetsarbetet. Det kommer stå… Vi kommer specca vilka roller och ansvar de har. Vi kommer att utefter standarden sätta de här SKA-kraven har jag tänkt. Det här ska göras och det här ska göras så vi får någon att följa upp emot då den här riktlinjen blir jätteviktig, då den är en del av den här grundplattan. Och sen kommer ett antal med instruktioner då slängas upp för beslut

hos regiondirektören, det är på olika nivåer som det här beslutas då men som liksom talar om mer hur det hör ska göras då för att nå det här och komma ut i hela organisationen jobbar på samma sätt. Men det saknas idag, massa lösa grejer som ligger som inte innebär någon systematik, men det är det de här nya instruktionerna och riktlinjerna kommer göra och då blir det systematik. Att vi börjar göra riskanalyser, börjar göra vår informationsklassificering, att vi börjar ställa krav på våra system och våra leverantörer och sådär.

D: Riktlinjerna du pratade om, kommer dem, är de mer övergripande då och liksom gäller avdelningar övergripande eller kommer dem… kommer varje avdelning ha sina egna riktlinjer fast mer detaljerat?

J: Nä, överst är då säkerhetspolicyn då och de är fullmäktige som fattar beslut, det är ju högsta beslutande organet. Så dem har policyn och det är ju… och de kommer också fatta beslut om de övergripande målen som är på en väldigt molnfri höjd så att säga. Och nivån under är regionstyrelsen och dem kommer fatta beslut om riktlinjer och den blir ju ganska detaljerad utan att gå ner i detalj så talar den om vad som ska göras och det är hyfsat detaljerat. Men det är ju för att få något att följa upp mot, asså det ska ju helst vara uppföljningsbart. Och där kommer även de kortsiktiga målen att landa som blir lite mer detaljerade då. Nivån under hamnar nog på regiondirektören och det är han som liksom styr verksamheten så han få de här instruktionerna och det är mera hur saker och ting ska göras och de är regionövergripande dem jag tar fram så det kan liksom inte en förvaltning välja att inte följa. De ska följa den. Men den är också mer eller mindre övergripande så. Sen har ju dem möjlighet att ta fram egna instruktioner då på rutiner, vet jag inte vad de kommer kallas, på en förvaltningsnivå som konkretiserar instruktionerna ovanifrån. Såhär göra vi och vem gör de och planera in det i sin verksamhetsplanering och sådär.

D: Ja, det va det där jag…

J: Och det är det jag följer upp sen, så instruktionerna talar typ om ”Här har ni modellen och såhär ska ni göra er klassificering och såhär ska ni tänka och dokumentera”. Sen hur dem praktiskt väljer att genomföra det i förvaltningen de får ju dem själva bestämma lite kring. Skånetrafiken har ju en helt annan verksamhet än SUS t.ex. Så de får anpassa det efter sina förutsättningarför att kunna följa upp sådära.

M: Så då om en anställd på sjukhuset då skulle behöva kolla upp… är osäker gällande någon säkerhetsbestämmelse, hur gå dem tillväga för att få reda på informationen? Intranät eller…

J: Ja, ja, ja. Ofta ligger informationen på något intranät. Om man lyckas hitta det för det är inte…

M: Ja det är det vanliga problemet som finns.

J: Ett svart hål… Men annars så… hittar de inte det där så kommer de ju… ställer de frågan till… uppåt då så att säga och till slut så... ja, ibland landar den ju hos mig eller hos juristerna.

M: Men meningen är dem ska hitta den själv.

J: Meningen är att de ska hitta eller att de ska eller att de ska få den har e-utbildningen till exempel.

M: Ja just de.

J: Där har vi tänkt att den som finns idag, den är ganska bred och övergripande men att vi tar fram mer e-utbildningar som är mer nischade. Att vi har en för sjukhuspersonal, en för konsulter, en för administrativ personal och en kanske för IT som kanske är lite olika inriktningar

på så de får svar på sina frågor. Sen kan de naturligtvis inte svara allihopa men att de blir lite mer nischade. Det är så planen ser ut iallafall.
M: Och de här riktlinjerna som dem kommer läsa är det då mer specifika saker som förvaltarna har tryckt ner eller är det ett steg under förvaltarna till? För förvaltningen är väl, Sjukhuset blir en förvaltning, SUS?
J: Ja, SUS är ju en förvaltning. Det är ju sjukhuset i Malmö och Lund här och det är största förvaltningen.
M: Ah, okej. Så de dem, de anställda inom SUS, har samma krav? Det är aldrig några specifika enheter inom vissa avdelningar?
J: Nä, utan dem ska ju följa såhär, säkerhetspolicyn, riktlinjer. De ska följa de här regionövergripande instruktionerna. Sen kan ju förvaltningen då ta fram egna då förvaltningsvisa styrande dokument om vi kan kalla det för det. Som dem inom SUS måste följa men de får ju inte avvika från de här övergripande som jag tar fram.
M: Nä. Och det du tar fram täcker allting. Det är inte så att du lämnar ute något som ”Ja, det är specifikt för er”.
J: Nä asså, det jag tar fram det bara sånt som gäller regionövergripande, alla förvaltningar inklusive Skånetrafiken.
M: Mhm okej. Och då skiljer de sig inte…
J: Ja dem har ju… Nejnej de skiljer sig inte. De är samma för alla. Det är så att i mina instruktioner så står det sällan någon om patientuppgifter och så utan det handlar om informations klassificeras och sådär. Sen beror det ju på vilken information man har och så får anpassa det. Asså håller man på med tåg och sånt så kanske de har andra typer av lagarstiftning som de får titta på och klassa. Och vården har. Så får man bedöma det, en liten gemensam skala så att säga som gäller alla men man får ju försöka passa in sin information.
M: Okej, så det har också ett arbete att göra när de väl får de där…
J: Jaja visst. Sen hjälper ju, vi hjälper ju dem att ta fram exempel. Att patientuppgifter i stor mängd eller patienter med skyddad identitet t.ex. har ju en högre klassning än dem som inte har det. Att de ska skyddas på ett särskilt sätt t.ex. när det gäller konfidentialitet. Så det hjälper vi ju dem med så att alla tänker likadant. Men instruktionerna, de här regionövergripande är inte skrivet så att man pekar på just en specifik förvaltning. Det är sällan, ibland är det så t.ex. jag tog fram en instruktion för några månader sen, veckor sen i och för sig som gäller behörighets… tilldelning av behörighet… åtkomst till personuppgifter inom hälso- och sjukvården, hur det ska gå till. Den riktar sig inte till Skånetrafiken utan specifikt till vårdförvaltningarna bara.
M: Men det är ändå du som ska göra den även om du… skulle det inte egentligen legat på förvaltningen eller?
J: Nä, nä. Det är en övergripande. Det är koncernkontoret då som jag sitter på. De glömde. jag säga också, förvaltningen koncernkontoret.
M: Okej, och det är här där vi befinner oss och alla interna avdelningar?
J: Nä, ja. I det här huset sitter koncernkontoret och medicinsk service, IT. Dock här nere är det i princip bara koncernkontoret personal. I Kristianstad också där på Kårhuset sitter ju, sen har du ju SUS som ligger i Malmö det är ju där huvuddelen av förvaltningens personal sitter. Men man kan säga koncernkontoret är administrativa förvaltningen liksom som tar fram sånna här

gemensamma riktlinjer och instruktioner sköter administrativa koncern???(54:58) och koncerninköp, alla sånna centrala funktioner sitter på koncernkontoret, så vi tar fram sånt.
D: Dem här riktlinjerna sen då, hur tänker ni sprida dem i organisationen? Ni tar fram dem och lägger dem på intranätet och sen blir det lite ”Ni får kolla själva” eller finns det någon…?
J: Nä men riktlinjen är uppdelad i flera kapitel. Vissa kapitel kanske rör framförallt HR, ett kapitel rör ju kanske främst IT, de här med drift och leverantörer, leverantörsrelationer och sånt där och nästa kapitel kanske rör koncerninköp och ställa krav på leverantörer. Man kommer naturligtvis att gå igenom det här med varje sån… och jag har möte imorgon med HR tror jag fram att liksom kratta ?????(50:02) inför att det här kommer vill jag gå igenom de här kraven med dem. Men sen får man ju liksom gå igenom dem igen när de är beslutade. Liksom, nu är det här beslutat och nu ska vi då arbeta vidare med det här. Så det blir ju liksom att man… får bli en utbildning.
D: Ah, det blir lite åt det hållet istället…
J: Jaja, det blir det ju naturligtvis och sen kommer ju de här informationssäkerhetssamordnarna, som finns i varje förvaltning, de kommer ju behöva gå igenom det här i sin förvaltning. Jag är kanske med och get det med ledningen, kanske. Men sen få samordnarna lägga upp arbetet i sin egen förvaltning hur de ska nå ut med…
D: Delegera ut arbetet lite?
J: Jaja de måste… de måste ju göra det i sin egen förvaltning, det gör ju inte jag.M: Då säger de ”Okej, det här är stort nog för att kräva en utbildning eller vi kanske bara ska ta det på ett morgonmöte för det är en liten…”
J: Ja, precis. ???????(50:54) kanske tar upp på en sån här arbetsplatsträff t.ex. Man går igenom det här, okej nu är det beslutat, när är de det här som gäller. Nu tror jag inte just det kommer bli så mycket när det gäller riktlinjer och det är ganska övergripande nivå. Det är liksom systematik och sånt där. Det kan ju finnas andra instruktioner som man liksom behöver nå ut med till t.ex. enskilda sjuksköterskor att nu är det de här som gäller, det här ska du tänka på. Då tas det ju upp på…
M: Och då är det administratören eller förvaltarna som sköter det? Det är ofta inte du som är ibland i…
J: Nänä, det är förvaltningen och informationssäkerhetsförordnanden som går ut till sin organisation och skickar ut det via… de har ju chefsläkare som skickar ut till sina läkare och så kommer det ner. Det är verksamhetschefer och sånt, det är olika strukturer och sånt där som ner. Det är ju en jätteorganisation så man kan inte göra på något annat sätt men sen når det inte ut till alla, och så är det ju. Det är ju massvis med människor då som aldrig kommer ha någon aning om det här och aldrig kommer att bry sig och sen finns det de här som inte ens vet om att de finns en förvaltning som heter koncernkontoret. Jobbar mani vården som undersköterska och sjuksköterska på SUS, varför ska man bry sig om det? Det är inte det man tycker är viktigt, de är intresserade av sitt jobb och gör ett jättebra jobb men de bryr sig inte riktigt om de här hela administrativa överbyggnaden med allt vad det för. Det har fullt upp med de håller på med. Men så är det viktigt att det kommer ut APTerna det som är viktigt för dem och sen får man skydda dem från allt det andra för varför ska dem tyngas med det? Det är lite så man får tänka.

M: Är det någonting som är svårare än alla de andra grejerna som vi har diskuterat nu? Asså är det det här får ner informationen till absolut lägsta ledet eller är det hantera ledningen eller är de de nya kraven eller…?
J: Det är nog alltihopa. Alltså allting är, vad ska man säga, en utmaning. Dels att nå fram till ledningen och informera dem så de är med på banan. Det är en utmaning med att gå ut med information, det är en utmaning med resurser och få pengar och personal att göra det här. Det ska ju fungera sen också, jag menar bara att sitta och ta fram en massa dokument. Ja, det är en utmaning att får styrande dokument beslutande, det tar också jättelång tid beroende på vad det är och få dem implementerade då så det funkar och det ska följas upp och det ska bli en systematik. Jag menar allt allting är det rätt mycket jobb med, det är liksom ingenting som är enkelt utan… det är mycket… de är ju många som tycker allt möjligt om det här, vissa tycker det är bra, vissa tycker det är skit och motarbetar och har egna agendor, de är jätte… det är så i en sån här jätteorganisation, har man en liten organisation på bara några hundra anställda där man liksom träffar alla dagligen i matsalen och de är lätt att springa bort och prata då är det ju lite skillnad. Men jag menar denna organisationen är en av Sveriges största så det att… de i sig gör att det inte blir lättare.
M: Du känner det är en stor utmaning, just att det är stort…
J: Ja, det är klart.
M: Var hade du jobbat innan?
J: Länsstyrelsen.
M: Är den mindre eller?
J: Ja, det är bara 450–500 anställda.
M: Och då kände du att du hade en helt annan…
J: Det va mycket lättare att nå ledningen där ju. Det var ju landshövdingen och landsdirektören som var ledningen och de satt i samma hus så det var bara gå upp två våningsplan och knacka på dörren men det liksom går ju inte här. Jag kan ju ringa regiondirektören och… visst kan jag göra det är svårare. Det krävs mycket mer för att göra det. Det är inte lika enkelt, det tycker jag inte.
D: Det kanske känns bra det här.
J: Har ni fått svar på era frågor?
D: Ja, det tycker jag.
M: Ja, det hoppas jag. Det har varit lite upp, ner, fram och tillbaka.
J: Ja, det blir lite svårt annars.
M: Ja, man kommer lätt in på något och sås säger någon någonting

7.2 Intervju med Informationssäkerhetssamordnarna (SUS)

D = David, M = Markus, J = Jonas, A = Anette

D: Om ni vill börja med att beskriva er själva lite kort, och er roll liksom.
J: Jag är informationssäkerhetssamordnare här på SUS, va fasen gör jag, ja vi ska liksom leda och hålla samman InfoSek arbetet vi gör här, på förvaltningen. Det kan vara utbildning, det kan vara information, det kan vara att man går in i speciella projekt och ska bedöma dem ur informationssäkerhetperspektiv, inte projekt utan det blir då mycket systemutveckling, eller man vill ha nya tjänster, man vill använda någon ny tjänst som finns någonstans, så ska man bedömas ur ett informationssäkerhets perspektiv. Man håller på på akuten med ett, vad fan heter det, positionellt projekt, där man har sändare på patienter, personal och prylar.
M: Aha för att se vad…
J: Inom akuten, var dem rör sig och hur, rörelsemönster och vad saker och ting finns någonstans. Det är ett forskningsprojekt, så ska det bedömas ur ett InfoSek perspektiv. Det var någon verksamhet som ville ha bilder och, ja det va skitsmidigt tyckte man, men sen så var jaha, var lagras dem bilderna någonstans? Ja, det var någonstans i molnet och… (Kan inte urskilja vad som sägs)… eller vem äger bilderna? Det är mycket sånt ja.
A: Jag jobbar med lite blandade säkerhetsfrågor, men jag har också börjat introducerats i informationssäkerhet, det arbetet som pågår här för att, det är lite så, vi är ett antal som jobbar på säkerhetsenheten här va men, är man bara själv så är det rätt så sårbart, så därför så är vi flera stycken som, så vi överlappar varandras område så att vi kan ge bästa tjänster till sjukhuset och våra patienter.
M: Vad var det du fokuserade främst på? Innan du nu, gick in i informationssäkerhet
A: Jag har jobbat med brandskyddsfrågor framförallt.
J: Ja vi tillhör då, staben för verksamhetsutveckling, och enheten heter Enhet för säkerhet och katastrofmedicin. Katastrofmedicin är ett eget litet spår så att säga.
M: sitter hela internavdelningen för säkerhet här i Malmö?
J: Ja
M: Men ni har ändå hand om Lund, Malmö och…
A: Ja, vi har arbetsplatser i Lund också så att vi…
M: Ja Johan satt ju i Lund när vi träffade honom igår
J: Ja
A: Ja precis
M: Okej, så att det är lite mer huvud…
A: Man kan själv välja här… (Kan inte urskilja vad som sägs)… så att säga, men
J: Just vår stab är placerad här
A: Precis, men vi har arbetsplatser där också, så att det beror lite på vart man bor, vad man har för uppdrag, om man har möten på olika, tanken är ju att man ska liksom kunna vara tillgänglig för båda för båda sjukhusen

J: Du det sa du jävligt fel, ”båda sjukhusen”, vi är ETT sjukhus
A: Ja men om man säger båda sjukhusbyggnaderna
J: Ja båda lokalerna
A: Ja det var så jag menade
M: Har det varit tidigare två eller?
J & A: Ja det har varit två sjukhus
A: Nu är vi två sjukhusområden
M: Väldigt politiskt korrekt
A: Ja precis
D: Och om någon av er skulle vilja vara anonym så är det helt okej också
J & A: Nej det är bra
A: Det är rätt svårt när man jobbar i en offentlig verksamhet, så är det rätt svårt att vara anonym, alltså dem flesta har namnskyltar, ID-kort och sådana grejer
D: Om vi hoppar in i frågorna lite, börjar vi med att, vad ser ni som det största problemet eller hot mot er verksamhet när det gäller informationssäkerhet? Varför det skulle kunna vara ett problem
J: Ni får inte svar på största, för det kan vi inte värdera vilket som är störst. Men däremot finns det andra hot så att säga. Och det är väl helt enkelt att någon kommer åt våra patientuppgifter.
D: Med ”någon”, menar du utifrån?
J: utifrån. I större skala, eller större volym, det är väl lite sånt. Generell risk så att säga. Sen informationssäker är ju att uppgifterna ska vara riktiga. Det kan vara, och en sak är att dem ska vara konfidentiella och…
A: I rätt tid och dem ska
J & A: tillgängliga
J: Och är det någonstans det brister så är det ju allvarligt ju. Sen är det svårt att värdera vad som är allvarligast eller, eller om någon helt enkelt hackar. Sen har vi lite mer reella hot som inträffar så att säga, risker som inträffar så att säga. Det kan vara misstänkta dataintrång, att någon läser någon annans journal helt enkelt. Och det kan vara väldigt allvarligt för den individen.
M: Ja, hur är det med dem här aktiva hoten utifrån jämfört med dem interna hoten?
J: Vi vet väldigt lite om hot utifrån. Och det kanske är en risk att vi är okunniga på det, eller om vi är naiva, jag vet inte riktigt. Nu när man pratade om Cloudhopper förra veckan så var det nästan första gången man pratade om sjukvården som ett mål för sådana här aktiviteter.
D: När man tänker säkerhetsåtgärder då mot dem externa hoten, är det mera teknologiska lösningar eller fokuserar ni på lite mer interna, som policys eller utbildning av personal.
J: Det är både och. Vi håller på med den administrativa delen av informationssäkerhet sen all det här tekniska håller vi inte alls på med egentligen. Utan det är ju, vad heter dem, E-hälsa och digitalisering, dem ligger under vår IT avdelning inom region Skåne och tillhör något som heter Koncern kontoret. Nytt sen någon månad. Och dem står för allt det här med hårdvara, brandväggar, ja virusskydd och det är inte vi, så att säga, alls inblandade i. Däremot om dem gör en bedömning kring, ja det här potioneringsprojektet på akuten, ja då gör vi bedömningen tillsammans så att säga. Dem ur sitt perspektiv och vi ur vårt perspektiv. Ja sen som

risk, risken är ju att vi läcker uppgifter någonstans, till någon som inte ska ha. Om jag bara ska förtydliga mig så kan det gälla i relationer där det förekommer hot och våld.
M: Dem här externa hoten som ni inte är så insatta i, det är ingenting som händer heller jätteofta? Alltså jämfört med dem här att när någon person går in och kollar en journal som dem inte borde och skriver ut i fel skrivare och alla sådana här
J: inte vad vi vet
A: Nej precis, inte vad vi vet. Det är vanligare i så fall, alltså det förekommer nog oftare att det är interna hot så att säga. … (Kan inte urskilja vad som sägs)… sig tillgång till information som dem inte ska ha.
J: Men nu vet vi nu förra veckan, vi har ju… (Kan inte urskilja vad som sägs)… som driftar alla våra grejer, och dem skulle titta på om vi blivit utsatta för någonting i den här Cloudhopp till exempel. Så det är mer IT-avdelningen som hanterar dem sakerna.
D: så ni fokuserar mer på dem organisationella delarna?
J: Ja precis
A: Så att det finns regler och rutiner för alla, att de ska känna till att det är så här som det är, hur vi arbetar med säkerhet
D: Riktlinjerna ni får, ovanifrån antar jag, hur kommunicerar ni ut dem i er avdelning?
M: Hur fungerar arbetet när ni får nya riktlinjer? Som ni behöver informera ner till anställda på alla avdelningar
J: det dras i olika arbetsgrupper där man, vad heter det, dem som arbetar med journalsystem och dem bitarna dem kan tala om kring behörighet, vi har någonting, man drar det i olika nätverk helt enkelt. Sådana saker som gäller kortinloggning, där finns det ett nätverk för det som den personen kan återkomma. Styrning och behörighet, (två dokument till?), kan dras i det nätverket men det haltar lite, det kan bli mycket bättre. Det kommer att komma nya instruktioner som visar hur, ja hur man ska jobba regionalt på förvaltning och på verksamhetsnivå och det kommer att komma efter sommaren, vet inte om Johan pratade om dem.
M: Han talade om någon ny utbildning som skulle ske för anställda, som skulle…
J: Har ni något annat, … (Kan inte urskilja vad som sägs)… det är instruktioner som regiondirektören ska fatta beslut om, och där det står vad man ska göra, det ska finnas kontaktpersoner på varje verksamhetsnivå. Verksamhet kan vara akutkliniken, den är akut, … (Kan inte urskilja vad som sägs)…. Det kan vara hud, det kan vara kvinnosjukvård, det kan vara ortopeden. Det är verksamheter
A: och då går det oftast via chefslinjen, alltså att det går uppifrån från förvaltningschefen då så, sprids det ut via cheferna ner på eget sätt
M: vilka är målgrupper för er? Kan man säga, för oss är det väldigt mycket, tänker man sjukhus så tänker man sjuksystrar, undersköterskor, läkare. Är det några mer roller som ni kommunicerar ut till? Interna avdelningar eller, hur
J: Det är alla som på något sätt hanterar personuppgifter
A: Så det är både administrativ personal och då, sjukvårdspersonal.
M: okej, så det är alla som är inblandade i er organisation, håller i princip på med känsliga uppgifter, i någon grad?
J: Nej inte alla, men det är klart att det är framförallt vårdpersonalen
M: det är framförallt dem som ni, när det kommer ett nytt direktiv så
J: Det är framförallt vårdpersonalen som kommer i kontakt med dem här

A: Men alla ska ju känna till att det finns regler och rutiner så att
M: Så ni måste ändå kommunicera ut till alla, även dem interna, borde göras
J: Borde göras, inte tillräckligt väl men det är på gång det också, vi har tagit tag i det här med loggar och sånt där, logguppföljning. Det håller på att bli bättre, kan vi säga.
A: Informationen finns ju tillgänglig på vårt intranät, så att alla kan gå in och titta, så att den
J: Det finns ju ett ledningssystem för informationssäkerhet och där ligger det massa sådana här grejer. Dokument, riktlinjer, anvisningar och allt vad det heter, instruktioner. Men det kan vara svårt för den oinvigda att, på något sätt måste man fokusera på vad var och en ska tänka på så att säga. När det gäller en vårdpersonal så handlar det om att ta del av, ni får ta del av den, där ni har en vårdrelation. Låna inte ut ditt kort eller inloggning, sådana saker, prata in om patienter i andra sammanhang. Det är liksom deras, det räcker nästan.
D: Ni sa att det ligger ute på ert intranät, vi fick igår att ni har väldigt många olika system. Men det är ändå ett och samma intranät som alla använder, i hela verksamheten?
J: Alla använder samma intranät ja, VGI
A: Vårt Gemensamma Intranät. Men informationen som kommer liksom, den, mycket av den informationssäkerheten som ligger ute, alltså information kring det, det ligger liksom regionalt och då är det liksom kommunicerat ut till alla. Det är tekniskt styrt, så man jobbar inom då, SUS som vi gör, så har vi liksom, en anpassad framsida. För SUS gäller detta liksom. Och sen kan man då, om man byter profil, så kan man om man nu jobbar i Helsingborg så tar man ju SUND då, och då får man en liten annorlunda, som ser likadan ut men där är annorlunda information som är mer relevant för en. Men informationssäkerheten som ligger mer regionalt, den är samma för alla.
M: Det lät som, KRY och dem här, det är också sjukhus och dem utför samma arbete som ni då?
J: Ja
M: Har ni mycket samarbete med dem? Eftersom, jag tänker att arbetet är väldigt liknande
J: Vi har väl samarbete med, samarbete men, det finns ett regionalt informationssäkerhetsråd som Johan leder. Vi träffas, vi fungerar väl och det, vi träffas en gång i månaden ungefär. Och jag tycker det funkar väl ihop med KRY.
D: Är det i det rådet, där ni diskuterar hur ni ska följa upp ert säkerhetsarbete också?
J: Ja bland annat. Vi ska följa upp, vad är det man ska rapportera till regionen, ja olika aktuella frågeställningar. Om det kommer nya dokument så får vi (remissrundor?) på dem, synpunkter och sådant.
D: Hur följer ni faktiskt upp ert arbete? Att anställda följer dem riktlinjer och regler som finns. Har ni några särskilda processer för det?
J: Nej, det man följer upp är loggkontroller, att man kontrollerar vad man tittat på. Det ska ske slumpmässigt varje månad, x antal. Det görs, borde göras i större utsträckning sen följer man upp även om man haft, patienter kan även begära att få ut loggkontroller också till exempel, om man misstänkt att, om man haft en kändis inne så, och en kändis behöver inte vara någon kändis på stan, utan det kan vara en chef här, en kollega, och då kan man göra riktad loggkontroller så att ingen varit inne och titta på just den personen. På så sätt följer man upp det, vi försöker följa upp i bästa möjliga mån, man ska göra avvikelser, eller … (Kan inte urskilja vad som sägs)… , InfoSek också.

M: dem här, ni jobbar i grupper SUS, KRYS och dem här. Hur ser ert, ni får mycket från Johan, men har ni mycket egna arbeten också som ni inte fått från Johan eller är det, ni har inte så mycket egna projekt, ni jobbar mycket uppifrån, vad ni får från toppen?
J: Alltså det vi får uppifrån det är mer dem här styrande dokument och sådana saker, riktlinjer att förhålla oss till och sådant. Sen om det är något vi, jag va inne på det här med tjänster, och dem ska riskanalyseras till exempel jag menar, då är det på vårt egna initiativ, eller om vi får reda på via IT avdelningen och sådant, då gör vi det själva. Vi kan själva ta initiativ till att göra, som förra året riskanalyserade delar av (1177?), tjänsterna på webben så att säga. Och nu har vi ett annat område på gång, så att säga. Så det är vilket som.
M: Då när ni gör era egna…
J: Och sen följer upp även, det är inte vi som håller på med det va, men man följer upp E-tjänstekorten, var dem finns någonstans om dem lämnas tillbaka och sådana saker.
M: okej lite mer praktiska. När ni gör era egna projekt eller vad man ska kalla det, hur är det med stödet uppe från ledningen? Känner ni att man har det alltid eller är säkerhet lågt prioriterat, eller högt prioriterat?
J: InfoSek är väl i nuläget inte högt prioriterat. Vi gjorde en satsning för 1,5 år sedan, då gick hela ledningen, alla verksamhetschefer, en halvdagsutbildning i informationssäkerhet. Då tog man lite tag i det. Nu är det väl sisådär. Fast vi har inga problem, tar vi initiativ och tar det med vår chef har han inga som helst problem att han tar det med sin, så att det kommer upp i ledningsgruppen.
A: Vi behöver aldrig kämpa för att få igenom något. Såklart det är ju förvaltningsledningen, intresserade av att ha ett så säkert sjukhus som möjligt, det gäller inte bara informationssäkerhet utan även andra säkerhetsfrågor också liksom, så att
M: Men det är ofta kanske mer just sjukhus känns som det borde, eller är mer fokus på patientsäkerhet med vårdperspektiv
J: Alltså allting går i ett, menar, problemet med informationssäkerhet det är att det egentligen spänner så otroligt mycket, och ja om man frågar folk hur kul man tycker det är med informationssäkerhet så säger dem att det är tråkigt. Men däremot kan man vara angelägna om att patientuppgifterna är skyddade och är du angelägen då intresserar informationssäkerhet också, nu att kvoten ska fungera, behörighet och sådana saker. Då pratar du kort och sådana saker, men då pratar du hela tiden informationssäkerhet också. Pratar vi integritet kring det här med postionering och sådana saker, ja då pratar du också informationssäkerhet, men du vet inte om att du pratar InfoSek. Det är liksom InfoSeks dilemma lite. Man pratar logguppföljning i nätverken kring journalsystemen och sådana saker. Ja då pratar dem, dem pratar gärna och är intresserade och aktiva men dem tänker inte på att dem pratar om InfoSek. InfoSek ses liksom på något sätt, man klagar och gnäller över om, med all rätt, om journalsystemen ligger nere, det är inte tillgängligt, det påverkar vården väldigt mycket. Det är inte alls bra. Det är också en InfoSek fråga men man tänker inte det, då är det en IT fråga så att säga. Det är väl lite dilemmat med InfoSek.
D: Du nämnde att IT säkerhet, eller informationssäkerhet, ofta benämns som tråkigt
J: ”Uppfattas”
D: Ja uppfattas, tror ni det är något som kan påverka hur allvarligt folk tar på den biten av sina dagliga uppgifter liksom?

A: Det är väl som Jonas säger att dem vet inte om att dem arbetar med det va, men om man säger informationssäkerhet, så bara ”Åh, säkert bara policys och tråkiga riktlinjer som man måste läsa igenom, åh va tråkigt”. Men dem arbetar ju med det praktiskt liksom, så vi kanske ”schh” mer liksom
J: Komma bort från order informationssäkerhet
M: Säkerhet överlag är egentligen någonting som brukar va rätt tråkigt
J: Ja på något sätt är det ett hinder, men å andra sidan vill ju människor verkligen göra rätt och man vill ju, man tänker på integritet, man tänker på säkerhet och skydda sådana saker. Det är bara just begreppet informationssäkerhet
D: Nu när ni har er E-utbildning för informationssäkerhet, hur motiverar ni era anställda att verkligen ta den? Eller finns det någon sådan, liksom plan?
J: Nej det finns, det finns ett mål på en enhet att si och så många ska gått den här utbildning men liksom en plan för hur man ska nå dit vet jag inte. Problemet är att om du går in på nätet så har vi massa E-utbildningar på region skånes utbildningssida. Och då ska man få personal att ta sig och gå på det. Det finns säkerhetsutbildningar, det är brandutbildningar det är liksom ett enormt utbud av utbildningar. Och var har vi den tiden, det fattas personal, det har vi inte.
D: Är det någonting som ni tror hade kunnat säkra informationen på ett bättre sätt? om ni hade fått alla anställda verkligen gå utbildningen, och ta det på allvar
J: alltså man tar det på allvar, absolut, det gör man. Man tar InfoSek på allvar eller sina, det gör man
A: Vård styrs ju av så många olika lagar, det är sekretesslagen, det är ju att man inte får yppa något om patienten och att man bara får lov att gå och titta i journalsystemet på den patienten som man har, som man vårdar liksom. Så där är informationssäkerhet också så jag tror att, i och med att det är så många, det är så mycket andra, både lagar och regler och liknande som också innehåller informationssäkerhet, så jobbar man med det utifrån det. Men det är inget som säger att man inte kan bli bättre.
J: Absolut inte. Men jag vet inte hur man motiverar eller får personal till att ta sig tiden helt enkelt till att, du har möjligheten för att, i vården har inte var och en sin egen dator. Var ska dem gå och sätta sig och göra dem? Vi har flera datorer än personal men man samsas ju med datorerna, ena stunden står du på den datorn, andra står du på den datorn och tredje står du på den datorn, man jobbar ju så aktivt och rörligt där så att säga
M: gemensamma inloggningar och sånt, är det ett…
J: Nej det är påväg ut
M: Ni har något, eller det är
J: Nej jag ska inte svara, det har funnits gemensam inloggning på datorn men sen in på respektive system så finns det inga gemensamma inloggningar, men där har alla individuella inloggningar.
M: Där dem, ni sa att ni hade mål att ni ville att x antal skulle gå utbildningen, hur går det med det målet? Klarar ni att hålla upp det, att så många som ni sagt ska gå eller…
J: Nej det tror jag inte att vi gör, vi jobbar inte för att vi ska nå det heller riktigt
M: Tror ni att det hade varit givande att göra den obligatorisk eller? Eller det hade blivit att ni hade så många så det hade, varför skulle den vara obligatorisk jämfört med brandsäkerhet eller, alla är ju viktiga
A: Precis så brandutbildningen är ju obligatorisk

M: Ja okej den är det?
A: Ja men, vi har lite olika system, vi har sådana här stora brandutbildningar som man går då, vart femte år, all personal och den är teoretisk och praktisk. Men vi har också som komplement för att liksom fräscha upp så där va, så man har egentligen inga krav på sig att göra brandutbildningen i E-form så att säga. utan det är mest som ett komplement för att friska upp sina sådana, men ja jag vet inte om det finns något. Det är lite som det här som Jonas säger att det är väldigt lite tid för sådana här grejer ute, och vi saknar ju vår personal.
M: är det lite tid…
J: Sen tror jag det är viktigare, jag vet inte, har ni sett utbildningen?
M & D: Nej
J: Jag tror att det är viktigare att man, var som då är kontaktperson för … (Kan inte urskilja vad som sägs)…, att man vill om, journalsystemet, att man i sådana grupper pratar om vilka rättigheter man har att ta del av patientinformationen, att man loggas, att man ska göra sina (klick?) och sådana där saker för att komma, det är där InfoSekarbetet, det … (Kan inte urskilja vad som sägs)… man har störst … (Kan inte urskilja vad som sägs)… där så att säga. Sen går det ju ut ibland, bara tänker även ibland kommer ut på nätet, intranätet, att det kommer upp sådana spammail man inte ska klicka på. Det är en sådan risk också, men då går det ut information emellanåt.
M: Har ni bra samarbete, för jag förmodar att det är IT avdelningen som sköter när det kommer spam och har som ansvar för att stoppa upp det, fungerar samarbete med dem bra? Eller ni har inte så mycket samarbete?
J: Vi har inte så mycket samarbete så det kan vi inte säga
M: Det är mer när det väl sker någonting så kanske det finns någon kommunikation mellan er
J: Ja Johan har lite mer kontakt med IT än vad vi har. Vi har inte mycket speciell kontakt, det kan vara i speciella uppgifter i så fall.
D: Om vi hoppar tillbaka lite till IS-policys och riktlinjer
J: Och? Va sa du, IS-policys och?
D: Riktlinjer. Är det mera generella riktlinjer eller är det liksom specifika för varje avdelningen i organisationen?
J: Det är mer specifika
D: Det är det okej. Så då finns det massa olika policys och riktlinjer?
J: Nja, policys finns det bara några. Det finns något sånt här dokumenthierarki som jag aldrig lär mig. Policys får det inte finnas för många. Absolut inte. Det finns någon säkerhetspolicy vi håller på att utarbetar.
A: Ja, det gör det.
J: Och då finns det en policy som innefattar väldigt många olika områden.
A: Den finns det en informationssäkerhetspolicy.
J: Ja, fast ingår inte den i säkerhetspolicyn?
A: Ja, de gör den ja.
J: Och sen kommer nog instruktionerna från regiondirektören och sen finns det anvisningar och det är Johan som tar fram dem. Jag tror det heter det. Och sen får vi förhålla oss i respektive förvaltning.
D: Så det är inget ni är med i att ta fram liksom?

J: Jo, vi är delaktiga via informationssäkerhetsrådet. Johan leder arbetar men vi får gärna lämna synpunkter och har tar ofta hänsyn till synpunkterna också.
D: Är det ett kontinuerligt arbete med de riktlinjerna? Ni tar fram dem och sen så är det klart för ett bra tag framöver.
J: Asså man tar fram en riktlinje och sen håller den ett tag och så jobbar man med en annan riktlinje. Men man kan ha riktlinjer för tilldelning av behörigheter är en ny vi har. Och det är behörigheter till journalsystem och alla andra system. Det är en riktlinje och när vi är klara med den så får den finnas och gälla. Och sen är t.ex. hur man gör logguppföljning i säkerhetssystem och säkerhetssystem är då inte journalen och de grejerna utan passersystem, kameraövervakning och sånt där. Och så kommer där fram en ny instruktion och så får den gälla. Det är ett kontinuerligt arbete men de nya instruktionerna.
M: När era nyanställa t.ex. börjar jobba här så förmodar jag att i deras läkar- eller sjuksysterutbildning så ingår inte jättemycket om informationssäkerhet. Hur, när de ska sätta sig in i informationssäkerheten vad som krävs för att uppfylla de kraven som ställs? Hur kommunicerar man ut det och vilka dokument behöver de läsa? Och vilken utbildning får de av sina kollegor osv?
J: Man får gå en Mellior-utbildning om du ska in i journalsystem.
A: Och du skriver på en sekretessförbindelse och då har väl den sekretess ingen?
M: Då står de har då i enklare ord. För de här rikt dokument och så är ofta rätt tunga att läsa igenom. Lite svårt att se…
A: Där står framförallt bara om sekretess och jag tror jag inte nämner informationssäkerhet där. Men nu är informationssäkerhet en väldigt stor del att synt inte får yppas.
J: Sen har man introduktionsutbildning också och där förnyas…nämner man informationssäkerhet i några minuter säkert.
M: Är det sekretess som är den stora biten för era operativa anställda när det gäller just informationssäkerhet.
A: Ja, det måste det väl vara.
J: Ja, det är det väl.
D: Om en anställd skulle ha behov att jobba hemifrån av någon anledning, hur ser den processen ut? För jag tänker då måste de ju säkerhetsställa sin uppkoppling kanske…
M: … och behörigheter?
A: Vi har ju inloggning med kort och autentisering så det finns absolut möjlighet att jobba på distans.
J: Det finns en RSVPN heter det. Region Skåne VPN-lösning.
D: Okej.
J: Och den betraktas då som säker.
M: Kommer man åt alla systemen då eller det finns skillnad på vad man kommer åt hemifrån och vad man kommer åt härifrån?
J: Jag tror du kommer åt allt.
A: Ja, precis men du måste ändå autentisera dig längre in sen.
M: För att logga in i varje system?
A: Ja, det tror jag.
J: Det är precis som att sitta här. Jag tror man kommer åt samma saker. Jag ska låta det vara lite osagt. Det är nog IT-avdelningen som kan svara på det.

M: Men ni har inte… ni godkänner inte förfrågningar eller så? Alla har tillgång till att jobba hemifrån eller är det något man måste ansöka om?
J: Du måste ansöka. Asså, du kan ju sitta hemma och skriva på ett papper, det kan vem som helst. Men måste du jobba hemma via dator måste du sitta med en RSVPN och den måste man ansöka om och få godkänt av sin chef.
M: Och det är inte något som…
J: Det är en liten kostnad. Nä, det ät inte alla som får det.
M: Så det är lite restriktivt om vilka som får det?
J: Ja, det måste finnas ett behov.
M: Arbetstelefoner och sånt? Där har ni mail och sånt?
J: Ja, det har vi.
M: Men ni kommer inte åt dokument?
A: Nä, då tror jag vi måste koppla upp oss. Vi kan ju via mailen titta på dokument såklart.
M: Du menar bifogade filer?
A: Ja, precis.
J: Nä, vi kommer inte åt intranätet… nä inte på telefonen.
A: Nä. Då måste vi logga in.
M: Och ni skickar inte jättemycket sekretessbelagda uppgifter över mail?
A: Nä, man får inte lov.
M: Ah, man får inte lov?
A: Nä.
J: Eller jo du får om du skickar med säker e-post.
A: Det är alltså att du krypterar det men absolut inte med den vanliga e-posten.
J: Nä, det är tydligt. Ska du skicka personaluppgifter är det säker e-post och krypterar och signerar du meddelandet.
M: Ah, okej.
J: Och det fungerar internt inom region Skåne.
D: Det är någonting som vem som helst kan göra då antar jag? Kryptera sin epost?
J: Ja, du ska in och göra en lite inställning i outlooken. Det finns anvisningar på nätet hur man gör.
D: Jag tänker det här…är det någon…blir det någon sorts…går tillbaka lite till det här jobba hemifrån. Blir det någon sorts övervakning? Kollar man igenom vad en anställd gör hemifrån eller liksom så fort den kopplar upp sig antar man det är säkert?
A: Det är ett förtroende liksom. En överenskommelse man har med sin chef om man arbetar hemifrån är det ju liksom så att man…. Ja, det är ett förtroende liksom som anställd har jag skyldigheter mot min arbetsgivare.
M: Men det loggas precis som om man skulle vara…
J: Ja, asså du kan inte göra andra saker hemifrån än vad du gör… Jag menar sitter du hemma och går in i Mellior…. Ja, då syns det också. Du kan inte göra saker hemma som inte syns. Det är mer fråga om förtroende som du säger. Hur man disponerar sin arbetstid och vad har man för arbetsuppgifter med mera.
M: Vi var inne på det lite innan med uppföljning också. Nyckeltal, det har ni inte så mycket att plocka fram?
J: Nä.

M: Johan sa att ni höll på att titta på nya, det kanske inte är något som tittat på nytt system helt för hela organisationen. Att det skulle bli något gemensam…
D: …upphandling.
J: Nä, då pratade han nog om riskhanteringsverktyg.
M: Jaha okej. Det är inte själva…
D: …journalsystem?
J: Jo, det är ett som heter… det heter… det har bytt namn, vafan heter det. Framtidens vårdinformation digitala informationssystem. Jo, det är ett arbete som ska ersätta journalsystemen, vi har flera stycken ju plus massa andra system också.
M: Flera stycken? Ett för psykiatri…. Eller har ni flera….
J: Asså Mellior som är journalsystemet är för all sluten vård, det är på sjukhus. Det är psykiatri och sånt. Öppen vård är vårdcentral och de har ett annat journalsystem. Jag är inte involverad i det, Johan är engagerad i det. Så det ska väl bli ett system och även andra system. Asså funktioner ska möta systemet.
A: Och andra sjukhus i Sverige kan ju ha andra journalsystem, det är inte bara så att det är ett.
D: Det kanske är en liten för teknisk, jag tänker om två olika system vill… om man vill hämta information från ett annat system som man inte själv arbetar med, hur går det till?
J: Hur menar du?
D: Som det exemplet du gav med öppen vård om öppen vård vill hämta information från system som sluten vård använder, hur skulle det gå till?
J: Då kan du ha en behörighet och så kan du logga in i det andra systemet.
D: Ah, då loggar man in direkt i det andra systemet liksom?
J: Ja, om man har en behörighet.
D: Mmm, ah.
J: Det är inte alla som har det. Det är ett litet problem att primärvården har sitt och slutenvården har sitt.
M: Är det så att man brukar en på varje avdelning som tillgång till det andra systemet?
J: Det vet jag inte.
M: Är det mer på chefsnivå som man ger de behörigheterna?
J: Ja, utifrån en behovsnivå så att säga om man behöver ta del av andras.
A: Akuten och så när man kommer in på… när patienterna kommer in med ambulans och sånna grejer kan det vara bra att ha någon sjukdomshistoria så att säga. Jag låter också det vara osagt hur det funkar men klar, har man ett behov av det ska man ha tillgång till det.
D: Det med upphandlingen av det här systemet, är det något ni är delaktiga i eller låter det vara?
J: Nä, inte alls. Det sköter de på regional nivå.
M: Sen när det väl ska implementeras osv. kommer ni bli inblandade då arbetet någonting?
J: Nä, det tror jag inte. Det finns ju en enhet här på staben också som heter e-hälsa tror jag den heter. Det är väl de människorna där som är inblandade. Vi kanske blir lite inblandade också. Inte i nuläget i alla fall.
M: Okej. Det är vi talade om innan om att ni följer upp om det bli någonting. Om de anställda skulle bryta mot någon av de här… kolla på någon kändis journal eller liksom som man inte har… och ni skulle komma på det. Vad blir konsekvenserna, hur ser arbetet ut runt det?
J: Jag kan inte det riktigt för de frågorna utreds av respektive verksamhets HR.

M: Ah, okej. Är det ni som uppmärksammar det eller det går inte via er alls? Asså nä, det går inte via oss utan de är väl om verksamheten har haft kändisar så göra man… kan verksamhetschefen… då gör vi en kontroll på denna person om någon har varit inne och kollat och då kan man se någonting. Och då ska det utredas av verksamheten med hjälp av HR. Det finns rutiner för hur man ska hantera sån här misstänkt…. Då är det mycket vad som händer. Jag vet inte om man kan få någon varning och är det riktigt mycket fuffens kan man få bli uppsagd och sånna saker och ibland om det är extremt kan man lämna till polisen.
D: Okej, är det vanligare att man löser det internt tror ni eller blir det oftast polisanmälan ni av…
A: Jag kan inte svara på det. Det är HR mest som….
J: Kan inte svara. Jag vet att förra året utredde man fem dataintrång från HR sida så att säga, misstankar om ska jag säga för det kanske inte var ett enda. Vi vet inte och det visst inte HR heller när jag pratade med dem.
D: Finns det om man tänker lite mer allmänt arbete, finns det någon särskilda standarder som ni följer eller ramverk, jag tänker typ…
J: Ja det finns ju de där Si-standard, vad heter det…
M: ISO?
J: Ja, precis. ISO 31000, jag vet inte riktigt. De finns.
D: Ah, okej
M: Men det är lite över er också dem? Eller ni jobbar inte så mycket med det eller ni har…
J: Jo, vi jobbar med det, vi försöker… det ligger på regional nivå, det är inget SUS bestämmer, det är Johan som bestämmer. Vi är ju inte certifierade och vi har ingen ambition att bli det men vi följer ju dem i mångt och mycket ändå så att säga.
D: Blir det att man tar de delarna som passar ens egen verksamhet lite.
J: Ja, det får man göra lite.
A: Det är en kostnad också att certifiera sig och sånt. Det kan säker också spela in. Men grunden är att man jobbar med de delarna som man tycker passar.

D: Är det, om vi går in på kostnader, saknas det resurser eller har ni tillräckligt resurser jobba effektivt känner ni…
J: För vår del som infosäkerhetsförordnande så tycker jag vi har tillräckligt med resurser, ja.
M: Det är mer resurserna då på få de anställda hitta tid som är ett problem till era utbildningar
J: Det är ett generellt problem, det är patient… det är alla områden. Det finns patienter som är sjuka och de ska botas och opereras. Det finns en brist på personal. Det är klart att sånt här är… en patient kan inte sätta sig och göra en e-uppgift. Men på vår nivå tycker jag det är bra med resurser, absolut.
D: Om ni skulle beskriva er avdelning lite tänkte ja. Hur många jobbar liksom i just er avdelning.
A: Nio och en halv, eller hur?
J: Jag skulle vela säga 9.
A: Men är det inte på katastrofmedicinsk?
J: Men är vi inte fler än 9 då? Vi är ju säkerhet och vi är katastrofmedicin och de är väl fyra och en halv?
A: Är dem det? Är de inte tre och en halv?

J: JA jag vette fan, cirka 4. Och vad är vi? Är vi nio? Cirka?
A: Sex är vi väl? Sju med Patrik?
J: En, två, tre, fyra, fem, sex… ja något sånt. Sex – sju.
A: Okej.
M: Katastrofavdelningen, vad va det de hanterade?
J: Katastrofmedicin. Dem förbereder sjukhuset på stora olyckor och katastrofer.
M: Ja, okej.
J: När det kommer in ett stort antal skadade.
A: Som nu i fredags när terrordådet gick till i Stockholm. Då gick ju alla sjukhusen upp där i olika katastroflägen och vissa förstärkningslägen och det är den processen som dem jobbar med lite liksom så vi kan hantera de här situationerna.
M: Men det är bara själva vården? Inte om det skulle börja brinna i en byggnad och sånna katastrofer.
A: Det kan ju innebära en katastrof, asså det finns ju interna katastrofer och utom ligga hot. Men blir det en…
J: Men tar man att det brinner så drabbas såklart patienter med rökskada. Det har faktiskt inträffat någon gång för länge sen på ortopeden. Annars är det som sagt yttre.
A: Och det är kriterierna att man får ett visst antal skadade liksom som inte är normalt- Asså det är ett icke normalt läge där man ska behålla kapaciteten för att kunna driva en normal vård så vi får en bra vård så finns det olika lägen.
J: Men de är lite för sig själva så att säga. Sen är det hot och våld, vanlig säkerhet, låsa dörrar och sånt där. Brand, infosäk, kontinuitetsplanering…
A: Riskhantering.
J: Mycket riskhantering, ja. Riskanalyser i olika sammanhang. Något mer? Nej.
A: Nä, det är egentligen säkerhetsrelaterade saker.
J: Sen finns det en annan enhet som jobbar med patientsäkerhet. Den går lite hand i hand med vissa saker.
M: Och då är det mer vårdrelaterade…
J: Ja, precis.
A: Kan vara vårdrelaterad saka till exempel som utreds.
M: IVO, har ni någon kontakt mot dem eller är det de här som har hand om patientsäkerheten?
J: Det är framför allt patientsäkerheten, absolut. Men gjorde inte IVO någon revision kring kontinuitetsplaneringen nyligen som William uppe i?
A: Jag känner inte igen det. Det vet jag faktiskt inte.
J: Men i så fall är det att IVO tar något initiativ där de ska titta på, eller ganska eller göra någon revision eller något sånt.
M: Okej, men det är inte att ni skickar ärenden till IVO eller något likande?
J: Nej, det gör vi inte.
M: Om det skulle ske något sånt här sekretess… då går det via… ni sa HR och sen polisen direkt. Det har inte heller någonting med *IVO att göra?
J: Nä. Vi har ett infosäkerhetsärende vi har dragit till IVO. Då gör man sån här Lex Maria-anmälan och det var en hårddisk som skickades och försvann i transporten. Den skickades från en verksamhet till förtaget för support och den försvann i posthanteringen någonstans så den

innehöll ultraljudsbilder på patienter. Och då har ju patientsäkerheten brustigt kan man väl lugnt säga. Och då blev det en Lex Maria-anmälan, nu va det absolut inga jobbiga bilder. Det va ultraljudsbilder så det var inte så farligt. Med det är fel, det får ju inte inträffa. Och då blir det Lex Maria och då är det allvarligt när vi gör en Lex Maria, annars nä.
M: Hur tar man beslutet att det ska gå då via Lex Maria som i det här fallet eller om det ska…
J: Det är chefsläkaren. Alltid chefsläkaren som anmäler till IVO.
M: Okej okej, så det är lite besluts… situations anpassat vad chefläkaren…
J: Asså de bedömer det när det inträffar om det ska anmälas eller inte.
D: När IVO granskar informationssäkerhet blir ni involverade på något sätt? Kommer dem och…
J: IVO har granskat… IVO är ju en utbrytare ur socialstyrelsen, socialstyrelsen en granskning för några år sen. Jag vet inte om IVO har gjort det… Socialstyrelsen har granskat oss och hur vi hanterar behörighet till journalsystem och sånna saker.
M: Vilka krav har ni på er? Eller vem ställer kraven som ni behöver hantera det här med att man inte får kolla på någon annans patient och så vidare… De kommer från…
J: Det kommer från patientdatalagen och finns ju andra lagarstiftningar också. Sen har vi ju Socialstyrelsen föreskrifter som då ger ett tydliggörande av patientdatalagen.
D: Jag tänker personuppgiftslagen också, när används den och när används patientdatalagen, är det… Tar patientdatalagen över personuppgiftslagen roll lite eller blir det... eller används de i olika sammanhang?
M: Eller kompletterar de varandra?
J: De kompletterar väl varandra kan man säga.
A: Ja kan inte riktigt svara på det.
J: Nä, jag är inte helt säker på den.
A: Det kan man kolla med en jurist. Vi har ju en jurist också som jobbar inom…
J: Ja, han jobbar mycket med oss också. Nä, jag kan inte det riktig, jag låter det vara osagt. Men han är PUR-företrädare för Region Skåne. Så fort det blir lite juridiskt och man blir osäker så får han svara.
D: Härligt. Om man hoppar till riskanalys lite som du var väldigt inriktad på. Hur ser den processen ut när man ska starta upp en ny riskanalys om någonting? Kommer det in ärenden man får?
J: Det är olika. Det vi gjorde förra året var utifrån en rapporterad avvikelse och ett samtal med den läkaren som rapporterat avvikelsen. Det kan ju vara lite, asså där man märker det finns ett behov. Och pratar vi om att titta på en annan process ur ett infosäkerhetsperspektiv för vi tycker att… asså, det finns förbättringsmöjligheter om vi säger som så. Och då kan du använda riskanalyser som ett utgångsläge, man gör riskanalyser som… och den är ofta i ett utgångsläge och den är ofta utgångspunkten i allt informationssäkerhetsarbete. Man identifierar risker, vilka risker finns och hur hanterar vi dem och hur löser vi dem. Och hittar vi någon som brister så kan vi välja… Då får vi hitta en uppdragsgivare som kanske får ansvara för systemen.
M: När ni väl har identifierar risken, gjort riskanalysen, tar ni upp det då i det här rådet… samrådet…
J: Det tas upp i olika sammanhang, som riskanalysen kan man använda på många olika ställen. Den vi gjorde förra året så… Den drogs lite i Infosäkerhetsrådet, men får ju hitta vilken…

var ska man dra den vidare så att säga. För det är vår divisionschef och verksamhetschef som är uppdragsgivare. Vad är bäst att dra nästa steg? Ja då drog vi dem med regionala chefsläkare gruppen och sen har de då lagt det regionalt så det gå vidare så att säga. Det är resultatet. Sen om man tittar på något IT-system, ja då får man sånna här styrgrupper, förvaltningsgrupp heter det väl, för olika IT-tjänstesystem. Så då får dra det där så att de kan fatta beslut om det är något man ska åtgärda.
M: De här avvikelserna. Är det ni som tar emot alla dem från hela organisationen eller var landar dem?
J: Nä, verksamheter skriver avvikelser i ett verktyg och sen kan de grupperas utifrån vad de handlar om. Och alla dem som man sätter säkerhet på går till vår avdelning så har vi någon kollega som går igenom dem och sen kollar vi den någon gång i veckan, varannan vecka. Sen kan det ju finnas många gånger att en informationssäkerhetsrisk ligger någon annanstans. Precis det jag varit inne på innan, du tänker inte informationssäkerhet. Det kan vara en patientrisk, det kan vara något med IT-stödet. Så ibland får vi leta fram sånna här klassificeringar bland patientavvikelser till exempel eller bland IT-avvikelser. De kan ligga där också så att säga och då får vi mer aktivt söka i systemet om dem då inte är satta som säkerhet för då får vi dem direkt.
D: Finns det några risker som man hanterar kontinuerligt eller kanske interaktivt istället om man känner att det kan vara en pågående säkerhetsrisk men just nu så är det lugnt men det kan bli i framtiden.
J: Nä, det gör vi nog inte.
M: Vilken är den vanligaste typen av incidentärenden som når er?
J: De är så få så det kan jag inte svara på.
M: Va bra.
J: Problemet är att de nog ligger fler under patientavvikelser och där hittar vi dem inte. Det är svårt att hitta dem där. Det jag mest kommit i kontakt med är väl att fel person har fått information den inte ska ta del av. Det är väl det vanliga.
A: Och det behöver ju inte vara avsiktligt heller…
J: Det är ju så att den vanligaste incident får vi inte del av och det är ju så enkelt som att det är driftstopp i systemet. Då är inte datan tillgänglig och då brister infosäkerhetsarbetet så det är ju den absolut… men den går ju i ett IT-spår så att säga. Oplanerade avbrott i systemet, det är väl det stora? Ah, det är de stora! Men som sagt det kommer inte till oss.
D: Ska vi börja avrunda lite?
M: Ja.
D: Ja, vi är jättenöjda.
M: JA, vi är jättetacksamma. Om det skulle… vi har några intervjuer till. Vi ska träffa några mindre företag och så, skulle vi… om det skulle vara något vi kommer på. Kan vi höra av oss till er, maila eller slå en signal.
J: Ja absolut.
A: Ja.
M: Finns det något annat som ni känner att det här skulle vi vela lägga till eller någonting som ”Det här är väldigt intressant” som ni känner att ni arbetar med.
A: Nä, det känns som vi har gått igenom det mesta.
M: Ja, vi har hoppat lite fram och tillbaka.

J: Det var någon fråga här på slutet, Vad skillnaden är på små och stora företag.
D: Nä, det blir lite spekulativt.
J: Ja, precis.
M: Ja, det är väldigt spekulativt.
J: Ja, jag hade bara ställt massa motfrågor då.
A: Jag tänkte det kunde vara bra om ni hade mitt namn också
M: Absolut.
A: Anette Nilsson Brunlid, Anette med ett n.
D: Efter att vi har transkriberat det här skulle vi velat kolla igenom det?
J: Ja absolut.
A: Ja, absolut.
J: Ni har väl min mailadress?
D: Ja.
J: Ja, och ni har mitt telefonnummer, det står någonstans där också.
D: Ja, det gör det nog ja.
A: Jag har fått lite introduktion av Jonas men bara lite. Ni läser alltså informa…
D: Informatik ja.
A: På systemvetenskapliga…
D: Ja precis.
A: Och ni va på C, är det kandidatuppsats?
D: Ah, C-uppsatsen är kandidatuppsatsen.
A: Ah. Ja.
D: Så det är sista terminen här nu sen så är vi klara.
A: Ingen som ska läsa master?
D: Jag ska göra det. Kör igång igen i höst.
A: Ah.
D: Det bli spännande. Då mailar vi ut det till er bara?
A: Ja, absolut

7.3 Intervju med Föreståndaren (Brahe Vård AB)

T = Tord, D = David, M = Markus

D: Vill du bara kort beskriva lite din egna position, vad du gör.
T: Jag? Jag är föreståndare för Brahe Vård AB som är en verksamhet inom socialtjänstområdet, med vård av ungdomar.
D: Hur ser din dagliga dag ut, eller dina dagliga uppgifter?
T: Min dagliga dag ser ut, kan nästan se ut hur som helst. Jag har bytt lite hjul idag, ibland får man slå upp lite väggar och bygga kök och sånt. Mycket telefonsamtal med social sekreterare, sjukvårdsinrättningar, skolor, mailkontakter. Träffar eleverna, jag träffar, vi har nio elever och jag träffar dem, försöker träffa dem en gång i veckan.
D: Så du är även inblandad i den dagliga tillsynen då av elever?
T: Ja i allra högsta grad, vi har en som bor i familjehem därinne (Pekar mot en dörr i längre bort i rummet), så honom träffar vi varje dag. Och så har vi en träningslägenhet där uppe, honom träffar vi så gott som varje dag också.
M: Hur mycket av det du gör är som föreståndare och hur mycket är som behandlingsarbetare? Om du skulle lägga procentsats på dem, på ett ungefär
T: Ja det är en tredje del som är ”allt i allo”, hantverkare och sånt, och den är inte liten. Kan väl säga en tredjedel på varje ungefär.
D: Vill du vara anonym också i undersökningen, i vår uppsats så är det helt okej.
M: Eller om det kommer fram någonting kanske så…
T: Ja, får vi ju se men jag tror inte det.
D: Så vi jobbar ju med informationssäkerhet, eller skriver om det. Så vi har läst mycket om risker, riskhantering och sådant som dyker. Vad ser ni som risker i ert arbete med känslig information, sekretess och sådant? Vad som kan gå fel liksom
T: Ja alltså dem risker som finns är ju att, ja dels eftersom att vi ibland måste ha kontoret på fickan, att man skulle glömma sin portfölj någonstans med något sekretesspapper i någonstans, och det är inte bra. Eller att man skulle kunna få journalsystemet hackat eller så.
D: Har ni tagit, har ni några särskilda motåtgärder för att minska dem riskerna på något sätt? Försöker ni, är det mera…
M: Sunt förnuft
D: Ja precis
T: Va?
M: Sunt förnuft eller är det att ni har någon typ av säkerhets…
T: Säkerhetsrutiner?
M: Ja, eller riktlinjer, eller policys eller någonting mer utkommunicerat.
T: Ja alltså det vi har är ju att sekretess skall förvaras här, inlåst i kontoret. Och ja man tar ju bara sekretesspapper med sig om man får, om man får dem någon annanstans och ska ta dem

hit, om man får dem i handen. Och det kan man ju inte undvika och då gäller det att vara, försöka göra det med detsamma, inte stanna på Ica på vägen och sådant. Det är väl sådana, den typen av rutiner vi har.
D: Är det, alla anställda vet om sådant?
T: Ja. Det är ju, alltså dem mötena som vi får sådan information är det mest, jag som är med i 95% av fallen. Så det är mest jag som får dem papperna.
D: Kan tänka mig att, era anställda, vårdare och sådant tar del av en stor del av känslig information också när dem är ute på sitt arbete med elever. Gällande sekretess
T: Ohja
D: Hur får dem, utbildning är kanske fel ord, men träning så att dem vet vad som är okej och inte okej?
T: Ja alltså, jo om man har en socionomutbildning som vissa av oss har så ingår det ju i utbildningen. Annars, alltså sekretesslagen och kunna den. Annars så har vi internutbildat till det.
D: Ni har det?
T: Ja för det är oerhört viktigt. Jag menar, ofta så är personalen med i samtal på BUP.
D: Vad är BUP förresten?
T: Barn och ungdomspsykiatrin. Och där kan barnen prata om de mest hemska saker dem har upplevt ju. Finns dem som varit ”danspojkar” i Afghanistan och sådana där kul saker. Och ja, det är ju ingenting man tycker att personalen ska informera andra elever och andra människor. Och det är ju jätteviktigt att dem inte pratar om.
D: Anställda, jobbar dem mycket ute på fältet liksom och hemma? Är det nästan bara det, dem är inte så mycket här?
T: Nej dem är här när dem har måndagsmöten, dem är här när dem ska rapportera något särskilt. Ibland har vi möten med vissa elever här. Han som bor där inne är från Marocko så när vi ska ha ett allvarligt möte så vill vi gärna ha någon som talar hans, arabiska också, då är en personal här. Vi kommer att ha, i den nya fastigheten vi har skaffat nu, kommer vi att ha ett rum där dem kan sitta och skriva journaler också. Men annars så jobbar dem en del hemifrån, därför har vi vissa regler för arbete som bygger på att man jobbar hemifrån.
D: Ser ni några risker just associerat just med jobba hemifrån? Jämfört med…
T: Nja sekretess, alltså informationssekretessmässigt, så är det ju om någon skulle kunna komma in i deras datorer hemma hos dem.
D: Finns det några, eller det kanske inte ni är så involverade i men finns det några, tar ni några åtgärder för att minska den risken att någon kommer åt deras datorer eller lägger ni, säger ni att okej, det här får ni sköta på ett bra sätt?
T: Nej vi säger att datorerna ska vara stationära i deras hem och inte flyttas runt. Och sen har vi ju haft ett gäng ungdomar som har arbetat fram det här systemet och lagt in ett oerhört avancerat sekretessystem.
D: Ja juste, har hört många bra saker om det.
T: Man måste åtminstone logga in.
D: Ja sen det här, känner ni som, du i ledningen då, känner ni att ni har tillräckligt med resurser för att hantera informationssäkerhet på ett bra sätt?
M: Eller är det annat som man hade önskat att man kunde göra? Är det anpassat till er storlek?

T: Nja det är väl klart att man hade kunnat ha, om man hade varit en större verksamhet så hade man kunnat ha en mer avancerad lokal med mer avancerade lås. Man hade kunnat ha mer avancerade säkerhetssystem på journalsystemet och så vidare. Det finns ju alltid dem möjligheterna om man har tillräckligt med kulor.
M: Men IVO sätter inga krav, lagen sätter inga krav på att man måste ha elektroniska lås på dörrar och sådant? Det ska bara vara låst?
T: Ja det ska vara låst och, ja sen, det räcker inte att dörren är låst, utan det ska vara i ett låsbart brandsäkert skåp också. Inne i det låsta rummet.
M: Ja okej.
D: Så står det med i lagen då? Eller är det mera som riktlinjer?
T: Det kan jag faktiskt inte svara på, hur det är reglerat. Men det är i alla fall reglerat av dem, ja dem direktiv Inspektion för Vård och Omsorg (IVO) ger en när dem inspekterar.
D: Hur, om vi kommer in på det här med IVO, kommer på ofta på inspektioner eller blir det mer om det är anmälningar?
T: Dem har rätt att komma två gånger per år. En gång på ett anmält besök, en gång på ett oanmält besök. Vi har varit i gång i snart tre år och vi har bara haft en inspektion. Dem har haft väldigt mycket att göra och, ja den första tiden tror jag inte att IVO kände till oss. Eftersom att vi inte då jobbade med en verksamhet som var tillståndspliktig.
M: Vad var det för inspektion dem gjorde, när dem var här den gången?
T: Ja då hade dem fått vetskap om att vi fanns och ville komma och göra en inspektion som framförallt handlade om, bedrev vi vård som var tillståndspliktig eller inte.
D: Så då var det inte en oanmäld inspektion då liksom?
T: Nej den var väldigt föranmäld, vi fick säkert en månads varsel om det.
D: Har ni något särskilt samarbete, står ni i kontakt med dem kontinuerligt? Eller blir det liksom bara om det dyker upp något?
T: Nja alltså nej, vi har stått i kontinuerlig kontakt Inspektionen för Vård och Omsorg i Stockholm när det gäller tillstånd. Men när det gäller tillsyn så är inte Inspektionen för Vård och Omsorg i Malmö särskilt intresserade av att någon sorts löpande kontakt. Utan dem vill inte vara rådgivande, utan bara vara tillsynande.
D: Det kanske var så som du sa, att dem har mycket annat att göra också.
T: Ja men dem har aldrig velat det alltså, även innan när jag jobbat på andra ställen, så har dem inte faktiskt inte velat vara behjälpliga med och svara på frågor och sådant.
D: Sen om det kommer, lagar och sådant som uppdateras eller ändras. Får ni liksom veta det i förväg då så att ni kan förbereda processen gällande sådant? Eller blir det liksom bara, okej nu ändrades den här lagen
T: Nej det är tyvärr upp till var och en att hålla reda på det.
D: Hos er då eller hos…
T: Hos oss ja, eller ja i olika verksamheter. Det är inte precis så att om dem ändrar någon, om det är lagligt att gå mot röd gubbe så får man inte något brev hem om det.
D: Får ni någon viss tid på er då att anpassa er till det då?
T: Ja så är det ju. Alltså vi, som exempel så drev vi ju stödboende och det va inte tillståndspliktigt fram till, vilket var mycket märkligt men det var så, framtill den 01-01-2016. Och då kom ju lagen, 01-01-2016, men det fanns ingen möjlighet att 30-12-2015 ansöka om tillstånd.
D: Lite skumt.

T: Så att vi ansökte någonstans… vi var väl färdiga i början på februari och sen tog det ett kalenderår innan vi fick tillståndet och då va inte inspektionen för vård och omsorg ut och sa att ”haha, ni har inte tillstånd” utan…
M: De lät er?
T: De lät oss hållas ja. Så nu är det väl inte omöjligt att vi får en tillsyn snart igen. Vår verksamhet är också svårare att göra tillsyn på eftersom de flesta eleverna inte bor här.
D: Jo, det kan jag tänka mig.
T: De är ju vara vid hem för vård och boende där de bor fem till trettio elever på samma ställe.
D: Ah, nä. Kan tänka mig det är lite lurigt för dem. Om vi hoppar tillbaka lite till er organisation. Era anställda, om ni har några regler som era anställda inte får bryta mot. Vad händer om de gör det, medvetet eller omedvetet, får det några konsekvenser för det eller blir det liksom…
T: Ja, självklart. Det är ju… Det beror ju på allvaret i vad de har gjort men ibland får man ju tillrättavisa och förmana och ibland skärpa tonen ordentligt men vi har ännu inte gått så långt att vi behöver agera arbetsrättsligt.
D: Vet dem vad konsekvenserna kan bli om de missköter sig eller straff kanske är fel ord så att säga med liksom…
T: Konsekvenser är ett bättre ord som du sa.
D: Ja.
T: Ja, alltså det är väl alla här i världen att det finns möjligheter att förlora sitt jobb om man inte sköter sig, så är det ju.
D: Er ledning då, du och Barbara, hur involverade är ni i säkerhetsarbetet, jag kan tänka mig det blir en del säkerhetsarbete för er också som du sa, du jobbar med allt möjligt.
T: Vi utvecklar ju hela arbetet här. Alltså allting som… Personalen jobbar i princip bara med vård av elever och de gör ju sådana här… ja de får ju ibland hjälpa till att städa och hjälpa till och flytta, hjälpa till att handla och alla möjliga sådana saker. Men det är ju inte dem som jobbar med driftsfrågor alltså säkerhetsriktlinjer och sånt.
D: Sen så finns det, vad ska man säga, när man motiverar någon, vad heter det?
T: Motivationsarbete?
M: Att de ska sköta sitt arbete…
D: Någon liten morot för dem, för era anställda då så att de ska följa och vara noga med sitt…
M: Hur man motiverar sina anställda att följa riktlinjerna och sånt som ni sätter ut. Eller är det…
T: Stryk
M: Så det är mer att man hotar? Ingen positivt att följa utan negativt att inte följa.
T: Nä men alltså vi… man kan väl säga att vi håller ganska hög svansföring. Vi tycker att vi är bättre än andra och det tycker vår personal också och vi tycker att vi… Vi avlönar dem efter det och att vi ställer krav på dem helt enkelt efter det. Och det tycker jag att du vill att vi ska göra. De vill att vi ska ha den höga kvalitén som vi påstår att vi har. Det ska vara en förmån att få jobba hos oss.
D: Så det ingår i jobbet att… eller lönen motiveras nog…
T: Ja. Lönen…
D: De ska spegla deras prestation typ…

T: Ja. Den ska spegla deras prestation och vi har från början haft schyssta löner och det vill vi ha. Det är den bästa motivationen som finns. De är det folk vill ha att av jobba ju. Sen vill man ju inte ha trakasserier på jobbet allt möjligt annat jobbigt, det vill man inte. Men vi vill ha bra lön, vi vill ha bra arbetsledning och vi vill ha bra handledning och bra tekniskt stöd och sånt. Det är ju en löneförmån att få sitta hemma och skriva sina journaler istället för att komma hit och skriva det. Om man har jobbat i Malmö hela dagen och bor i Malmö så är det rätt tradigt att köra hit och skriva journaler och sen hem.
D: Absolut. Det är jobbigt ja.
M: Och sen är det väl lite så att era anställda, många av dem kommer också från samma situation, flera av dem kommer från samma situation som de elever/klienter ni har. Så det finns väl en förståelse.
T: JA, de vill ju gärna göra ett bra jobb för dem. Vår förste anställde tog jag med mig från där jag jobbade innan för att han är marockan och de första eleverna vi fick var marockaner förutom en svensk tjej. Och han är väldigt motiverad av att hjälpa sina landsmän till ett bra liv i Sverige. Ja men asså dem får ändå känna väldigt stor delaktighet i hur vi jobbar, att de ska tycka att förhållandet mellan gränssättning och belöning till eleverna och stöd är rimligt. Att vi inte jobbar med att muta eleverna med pengar utan… Det låter självklart men det är inte riktigt det i denna branschen, att vi lägger massor med resurser… Vi har väldigt lite resurser på boende eftersom vi inte har dygnet runt personal och sådär i den meningen. Man kan nå oss dygnet runt på telefon men vi har inget ställe där det måste sitta folk och kosta pengar på nätterna så vi kan lägga resurser på att hjälpa ungdomarna med att gå och träna. Eftersom träning är det bästa som finns för när man är svag i psyket och mår dåligt. Och vi kan sitta och lyssna på dem och vi kan hjälpa dem med skolarbete och det gör vi jättemycket men vi hjälper dem inte med saker som köpa kläder och skor och Nike och resor och sånt. Vi kan hjälpa med en resa om vi tycker att den här eleven inte mår bra och skulle behöva träffa sin familj och då kan vi hjälpa till med en resa så de får träffa dem. Även om Sverigedemokraterna tycker det är en dålig ide ”Att de ska få åka på semester till sitt hemland dit de inte kan åka”. Det är dessutom inte till sitt hemland så ofta utan familjen har ju flytt och bor i ett annat land. Afghaner bor i Iran, om man är hazarer och i Pakistan om man är pashto. Och där bor familjerna och inte har det så bra och de hade hoppats på att barnen skulle kunna ta hem dem med det… ta hit dem men det kan dem inte när de fyllt arton. Då har man ingen rätt till de längre och då är det väl inte fel att låta dem hälsa på sin familj.
D: Har ni några, om vi går tillbaka till anställda lite, har ni några nyckeltal som ni kan mäta för att se hur väl informationssäkerhetsarbetet fungerar eller följs?
M: Hur följer man upp det? Har man någon kontroll att de följer de de ska göra eller man hanterar det när det inte följs?
T: Nä men det är ju… Det säkerhetsarbete dem ska hantera är ju dels journalsystemet och dels att hålla flabben stängd när de pratar med andra människor än folk i företaget. Och det senare är väldigt svårt att kontrollera och det första är ju ganska lätta att kontrollera. Se hur de sköter, skriver in och så. Det är väl möjligt att man skulle… jag vet inte om vi har någon funktion på automatisk utloggning, det har vi inte, det borde vi kanske ha.
D: Ja, det är en bra idé.
T: Ja, det är faktiskt en väldigt bra idé. Bra fråga! Jag har ju det här TelIQ som färdskrivare och den loggar ju alltid ut. Färdskrivare till bilar.

M: Körjournal till bilar.
D: Ahhh, okej!
M: Man ser var de har kört.
T: Ja så vi kan redovisa för skattemyndigheten för det var ju omöjligt att få personalen att göra det. Skriva körjournal, det är faktiskt rätt tråkigt. Jag har gjort det innan.
D: Ja, det kan jag tänka mig. Om vi går in på uppföljning igen, har ni någon sådan process eller någon sån tanke att man ska följa upp sitt säkerhetsarbete. Inte efter enskilda individer då utan som organisation. Typ såhär någon kontinuerlig riskgenomgång eller något sånt som händer en gång om året eller något liknande.
T: Nä, det ha vi inte haft någon ide om men det är väl mer kontinuerlig att man funderar över vad man kan göra för att förbättra säkerheten men inget systematiserat.
D: Inte någon sån här speciellt uppföljnings…
T: Nä men det kanske man skulle ha. Det är många regler som myndigheterna har det vill ju att man ska ha systematik i såntdär. Vad som helst liksom brandövningar och så ska man ju göra.
M: Men ni känner att ni har en dialog mer era anställda så skulle det vara något som de känner att de inte uppfyllt eller de har klantat sig så berättar de det för er och då tar man hand om det?
T: JA, det tycker jag. Det förväntar vi oss och det sker också.
M: Det kanske är enklare om man är en mindre organisation där man har daglig kontakt med alla.
T: Ja, vi är inte så många. Vi är fyra heltid inklusive mig och Barbara. Tre deltidare.
D: Finns det något ramverk och sånt? Standarder? Typ ISO och ITIL? Inget sånt ni applicerar i er verksamhet.
T: Jag har ingen aning.
D: Nä, okej.
T: Garanterat ingen aning.
M: Har ni använt någonstans där du jobba tidigare?
T: Nä alltså de är ju. De är ju väldigt mycket för tekniska verksamheter.
M: Jaha, det är mer åt det hållet.
T: Hur va det nu, det fanns någonting någon gång i tiden. ISO 9000 hade vi ju.
D: Det fanns något just för säkerhets… eller informationssäkerhet. Typ 27 000 eller något sånt.
T: Ja det finns det säkert.
M: Ja, och byggarbetare har sina.
T. Ja, i transport och…målare och allting.
M: Ja, och jag vet inte riktigt vad som står i dem men jag vet att man inte behöver följa dem utan bara ta delar av dem och inte certifiera sig i dem.
D: Och applicera det som passar en själv.
T: Ledningssystem. Det är för kvalitetsledning, 9000, så det va precis som jag sa.

7.4 Intervjuguide 1 (SUS)

- Introduktion av forskningen
- Inspelning ok?
- Vill du vara Anonym?
- Beskriv dig, din position och vad det är för jobb du utför.

- Vad ser ni som det största hotet mot informationssäkerhet i er organisation? Varför?
- Vilka åtgärder tar ni för att motverka dessa hot?

- Hur involverade är ledningen i säkerhetsarbetet?
- Har ni någon omfattande IS-policy som gäller hela organisationen eller har ni mera specifika policys som innehåller regler och riktlinjer för specifika situationer?
- Hur följer ni upp ert säkerhetsarbete i organisationen?
- Har ni några nyckeltal för att mäta hur väl anställda följer de regler/riktlinjer som finns i IS-policyn?

- I vilken utsträckning arbetar ni med teknisk säkerhetslösningar jämfört med andra lösningar?
- Hur arbetar anställda? På plats? Distans? Anledningar och risker med detta?
- Hur koordinerar ni säkerhetsarbete i organisationen?
- Följer ni eller använder ni någon/några ramverk eller standarder?

- Har ni någon intern säkerhetsutbildning för anställda? Isåfall hur ser den ut?
- Hur motiverar ni anställda att följa regler och policys?
- Vilka konsekvenser kan medföras om en anställd bryter en eller flera gånger som regler/policys?

- Hur fungerar ert samarbete med Ivo?
- Hur ofta blir det inspektion från Ivo?
- Hur fungerar arbetet vid anmälningar och inspektioner från IVO?
- Vid nya lagar och regler, hur hanteras förändring?
- Hur ser ni till att de krav som ställs på sammanhållen journalföring följs?

7.5 Intervjuguide 2 (Brahe Vård)

- Introduktion av forskningen
- Inspelning ok?
- Vill du vara Anonym?
- Beskriv dig, din position och vad det är för jobb du utför.

- Vilka risker hanterar ni i er organisation gällande informationssäkerhet?
- Vilka åtgärder tar ni för att motverka dessa risker?

- Hur jobbar ledningen gällande risker och informationssäkerhet?
- Har ni några särskilda regler eller riktlinjer gällande hantering av sekretess och informationssäkerhet?
- Följer ni upp ert säkerhetsarbete i organisationen?
- Känner ni att ni har tillräckligt med resurser för att hantera informationssäkerhet på ett bra sätt?
- Har ni några nyckeltal för att mäta hur väl anställda följer de regler/riktlinjer som finns?

- Hur arbetar anställda? På plats? Distans? Anledningar och risker med detta?
- Följer ni eller använder ni någon/några ramverk eller standarder?

- Har ni någon intern säkerhetsutbildning för anställda? Isåfall hur ser den ut?
- Hur motiverar ni anställda att följa regler och riktlinjer?
- Vilka konsekvenser kan medföras om en anställd bryter en eller flera gånger som regler/riktlinjer?

- Hur fungerar ert samarbete med Ivo?
- Hur ofta blir det inspektion från Ivo?
- Hur fungerar arbetet vid anmälningar och inspektioner från IVO?
- Vid nya lagar och regler, hur hanteras förändring?
- Hur ser ni till att de krav som ställs på sammanhållen journalföring följs?

Referenser

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. 2016. *Information Security Policy: A Management Practice Perspective*. Australasian Conference on Information Systems. Adelaide, South Australia .

Baskerville, R., & Siponen, M. 2002. *An information security meta-policy for emergent organizations*. Logistics Information Management, *15*(5/6), 337-346.

Black, A. D., Car, J., Pagliari, C., Anandan, C., Cresswell, K., Bokun, T., & Sheikh, A. 2011. *The impact of eHealth on the quality and safety of health care: a systematic overview*. *PLoS Med, 8*(1), e1000387.

Blakley, B., McDermott, E., & Geer, D. 2001. *Information security is information risk management*. In Proceedings of the 2001 workshop on New security paradigms (pp. 97-104). ACM.

BBC. 2017. *'Serious' hack attacks from China targeting UK firms.* BBC. 3 April. http://www.bbc.com/news/technology-39478975. (Hämtad 2017-05-04)

Berger, E. 2017. *Så gick attacken till - tog sig in via epost.* SVT. 5 April. https://www.svt.se/nyheter/inrikes/sakerhetsexperten-manniskan-ar-den-felande-lanken. (Hämtad 2017-05-04).

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. 2009. *Roles of information security awareness and perceived fairness in information security policy compliance*. AMCIS 2009 Proceedings, 419.

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

Cavusoglu, H., Mishra, B., & Raghunathan, S. 2004. *A model for evaluating IT security investments.* Communications of the ACM, *47*(7), 87-92.

Dahllöf, Mats. 2014. *Akademiska uppsatsers uppbyggnad.* Uppsala universitet.

Datainspektionen. 2017. *Personuppgiftslagen*. Datainspektionen. http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/. (Hämtad 2017-04-21).

Dhillon, G., & Backhouse, J. 2001. *Current Directions in Information Security Research: Toward Socio-Organizational Perspectives*. Information Systems Journal (11:2), pp. 127-153.

Disterer, G. 2013. *ISO/IEC 27000, 27001 and 27002 for information security management*. Journal of Information Security. Vol.4 No.2.

Ejenäs, M. 2012. *Friska system - eHälsa som lösning på hälso- och sjukvårdens utmaningar.* http://www2.vinnova.se/upload/EPiStorePDF/va_12_03.pdf. (Hämtad 2017-03-14).

Ernst & Young. 2008. *Moving Beyond Compliance: Ernst & Young's 2008 Global Information Security Survey.* http://www.ncc.co.uk/article/?articleref=500146&hilight=ernst+%26+young. (Hämtad 2017-03-11)

Gupta, A., & Hammond, R. 2005. *Information systems security issues and decisions for small businesses An empirical examination*. Information Management & Computer Security, 13(4), 297-310.

Hove, C., Tarnes, M., Line, M. B., & Bernsmed, K. 2014. *Information security incident management: identified practice in large organizations*. IT Security Incident Management & IT Forensics (IMF), 2014 Eighth International Conference on (pp. 27-46). IEEE.

Hu, Q., Hart, P., & Cooke, D. 2007. *The role of external and internal influences on information systems security–a neo-institutional perspective*. *The Journal of Strategic Information Systems*, *16*(2), 153-172.

Humphreys, E. 2008. *Information security management standards: Compliance, governance and risk management*. information security technical report, *13*(4), 247-255.

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

Kankanhalli, A., Teo, H, Tan, B. C. Y., & Wei, K. 2003. *An integrative study of information systems security effectiveness.* Department of Information Systems, School of Computing, National University of Singapore

MSB. 2014. *Strategi för stärkt informationssäkerhet inom vård och omsorg.* MSB. https://www.msb.se/RibData/Filer/pdf/27364.pdf. (Hämtad 2017-05-04)

MSB, NCSC & BSI. 2014. *Strategi för stärkt informationssäkerhet inom vård och omsorg.* MSB, NCSC & BSI. https://www.msb.se/RibData/Filer/pdf/27482.pdf. (Hämtad 2017-05-04)

MSB. 2015. *Uppföljning av informationssäkerhet i vården. Vårdgivarnas rapportering av kontroller, risker och incidenter.* MSB. https://www.msb.se/RibData/Filer/pdf/27547.pdf. (Hämtad 2017-05-04).

MSB. 2017. *Omfattande cyberangrepp hos driftleverantörer.* MSB. https://www.cert.se/2017/04/omfattande-cyberangrepp-hos-driftleverantorer. (Hämtad 2017-05-04).

Puhakainen, P & Siponen, M. 2010. *Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study*. MIS Quarterly Vol. 34, No. 4 (December 2010), pp. 757-778

Schützer, K. 2017. *Så avslöjades cyberattacken.* SVT. https://www.svt.se/nyheter/inrikes/sa-avslojades-cyberattacken. (Hämtad 2017-05-04).

SFS 1998:204. Personuppgiftslag

SFS: 2008:355. Patientdatalag.

SFS: 2009:400. Offentlighets- och sekretesslag.

Siponen, M. T. 2000a. *Critical Analysis of Different Approaches to Minimizing User-Related Faults in Information Systems Security: Implications for Research and Practice*, Information Management & Computer Security (8:5), pp. 197-210

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

Siponen, M. T. (2005). *An analysis of the traditional IS security approaches: implications for research and practice*. European Journal of Information Systems, *14*(3), 303-315.

Siponen, M., Mahmood, M. A., & Pahnila, S. 2014. *Employees' adherence to information security policies: An exploratory field study*. Information & Management, 51(2), 217-224.

Socialstyrelsen. 2016. *Statistik om kommunala hälso- och sjukvårdsinsatser 2015.* http://www.socialstyrelsen.se/Lists/Artikelkatalog/Attachments/20174/2016-5-3.pdf. (Hämtad 2017-05-05). Art.nr: 2016-5-3

Straub, D. W. 1986. C*omputer abuse and computer security: Update on an empirical study*. Security, Audit, and Control Review, 4(2), 21–31

Straub, D. W. 1990. *Effective IS security: An empirical study*. Information Systems Research, 1(3), 255–276.

Symantec. 2010. *Symantec Global Internet Security Threat Report Trends for 2009.* http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf. (Hämtad 2017-03-11).

Thong, J. Y. L., Yap, C. S., & Raman, K. S. 1996. *Top management support, external expertise and information systems implementation in small businesses*. Information Systems Research, 7(2), 248–267

Vetenskapsrådet. 2002. *Forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning.* Vetenskapsrådet. http://www.gu.se/digitalAssets/1268/1268494_forskningsetiska_principer_2002.pdf. (Hämtad 2017-04-17).

Vance, A., Siponen, M., & Pahnila, S. (2012). *Motivating IS security compliance: insights from habit and protection motivation theory*. Information & Management, *49*(3), 190-198.

Vårdförbundet. 2017. *Regelverket i vården.* Vårdförbundet. https://www.vardforbundet.se/rad-och-stod/regelverket-i-varden/. (Hämtad 2017-04-12).

Warkentin, M., and Willison, R. 2009. *Behavioral and Policy Issues in Information Systems Security: The Insider Threat.* European Journal of Information Systems (18:2), pp. 101-105

Whitman, M. E., Townsend, A. M., and Aalberts, R. J. 2001. *Information Systems Security and the Need for Policy*. in Information Security Management – Global Challenges in the Next Millennium, G. Dhillon, London: Idea Group, pp. 9-18.

Whitman, M. E. 2003. *Enemy At The Gate: Threats To Information Security.* Communications Of The ACM. Vol. 46. sid 91-95.

Zhang, X., Wuwong, N., Li, H., & Zhang, X. 2010. *Information security risk management framework for the cloud computing environments*. In *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on* (pp. 1328-1334). IEEE.