LULEÅ TEKNISKA UNIVERSITET

2003:148 SHU

EXAMENSARBETE

Efterlevnad av informationssäkerhetspolicy

TOMAS LIIKAMAA
THOMAS SANDSTRÖM

Samhällsvetenskapliga och ekonomiska utbildningar

SYSTEMVETENSKAPLIGA PROGRAMMET • C-NIVÅ

Institutionen för Industriell ekonomi och samhällsvetenskap
Avdelningen för Systemvetenskap • Data och systemvetenskap

2003:148 SHU • ISSN: 1404 – 5508 • ISRN: LTU - SHU - EX - - 03/148 - - SE

Förord

Denna c-uppsats omfattar 10 poäng och är ett examensarbete som ingår i en filosofi kandidatexamen på programmet för data och systemvetenskap. Programmet tillhör institutionen industriell ekonomi och samhällsvetenskap vid Luleå tekniska universitet.

Vi vill tacka våran handledare Hugo Quisbert och alla andra som hjälpt oss med våran rapport.

Slutligen vill vi tacka de personer på Riksskatteverket samt Skattemyndigheten i Luleå som hjälpt oss med våran undersökning.

Luleå den 15 Juni 2003

Tomas Liikamaa Thomas Sandström

Sammanfattning

Hoten är många i ett informationssäkerhetssystem och det är viktigt att ha fungerande säkerhetslösningar. Övergripande för en fungerande säkerhet är en informationssäkerhetspolicy. I informationssäkerhetspolicyn står de övergripande målen som organisationen har för säkerheten. Det är viktigt att ledningen tydligt klargör vad som gäller inom organisationen.

Det räcker inte att bara ha en informationssäkerhetspolicy utan ledningen måste se till så att de anställda också har en hög säkerhetsmedvetenhet. Ledningen måste göra alla inom organisationen medvetna om informationssäkerhetspolicyn och få dem att förstå den för att de ska kunna följa de regler och riktlinjer som finns.

Vi har i denna uppsats undersökt hur de anställda i en statlig organisation följer den informationssäkerhetspolicy som finns för organisationen och vilka eventuella brister som finns i informationssäkerhetspolicyn. Vår fallstudie har vi utfört på Riksskatteverket där vi har gjort en intervju och en enkätundersökning.

Resultatet visar att de har en väl utarbetad informationssäkerhetspolicy som nyligen har implementerats. Om de årligen fortsätter följa upp den, informera och utbilda i organisationen kommer den goda säkerhetsnivån att bli ännu bättre.

Abstract

The threats are many in a information security system and it is important to have working security solutions. Overall for a working security is an information security policy. The information security policy gives the overall goals that the organization has for the security. It is important for the management to clarify what the concerns are in the organization.

It is not enough just to have an information security policy but the management must make sure that the employers also have a high mind about the security. The management must make everybody in the organization aware about the information security policy and make them understand it so they can follow the rules and guidelines that exist.

We have in this rapport examined how the employees in a government organization follow the information security policy that exist for the organization and what eventual lacks that is in the information security policy. Our case study is performed at Riksskatteverket where we have made an intervju and a survey.

The result shows that they have a well developed information security policy that recently has been implemented. If they can continue to make a follow up every year, to inform and educate in the organization the good security level will be even better.

Innehållsförteckning

1 Inledning

1.1 Bakgrund

Information är en tillgång värd att skydda. Företagens verksamheter blir mer och mer IT-beroende och i samma takt ökar också riskerna och hoten. Varje dag hör vi om nya virus och hackerattacker, men vi glömmer att de flesta hot kommer inifrån. Dessa utgörs ofta av okunniga och nyfikna anställda, bristfälliga rutiner, system samt från bristande kunskap på ledningsnivå.

Information är i många fall verksamhetens mest värdefulla tillgång. Nya snabba, kreativa och komplexa möjligheter att skapa, använda och utbyta information skapas varje dag. Elektronisk information och synen på information som den centrala tillgången omvandlar vårt sätt att leva och arbeta. Men riskerna är stora att information går förlorad, förvanskas eller kommer i fel händer. Följderna av sådana incidenter är ibland förödande.

Den nya globaliserade miljön, där information kan flöda fritt mellan organisationer och människor, leder till att organisationers sårbarhet ökar dramatiskt.

Avbrott och informationsförluster är ovälkomna företeelser, som med rätt kunskap kan förhindras. Det är därför oerhört viktigt att lära sig analysera riskerna och implementera en fungerande informationssäkerhetspolicy inom organisationen.

Som medlem av en organisation är det viktigt att vara medveten om informationssäkerhetspolicyn och göra sitt yttersta för att följa den. Statskontoret (1997) påpekar att genom att ledningen på ett tydligt sätt uttalar sin syn på IT-säkerhet skapas medvetenhet och engagemang från personalens sida.

Statskontoret (1997) skriver att informationssäkerhetspolicyn utrycker företagsledningens syn på behovet av IT-säkerhet och anger målen för IT-säkerhetsarbete. Den ska ge en klar uppfattning om vilken inriktning säkerhetsarbetet ska ha.

Erikson (1998) menar att för att en informationssäkerhetspolicy ska få genomslagskraft krävs många åtgärder. Han lyfter också fram att företagets ledning självfallet måste leva upp till policyns innehåll redan från utgivningsdagen.

1.2 Problem

Information flödar fritt inom organisationen och det är viktigt att skydda sig. Detta gör man genom att ha rutiner och regler för att inte denna information hamnar hos obehöriga. Men det räcker inte bara att ha bra regler och riktlinjer utan det är viktigt att personalen följer reglerna.

1.3 Forskningsfråga

Hur efterlevs informationssäkerhetspolicyn i en organisation?

1.4 Syfte

Syftet är att visa på eventuella brister med informationssäkerhetspolicyn och säkerhetsmedvetenheten hos de anställda.

1.5 Avgränsningar

Undersökningen omfattar en informationssäkerhetspolicy och de anställda i en svensk organisation som följer stadskontorets rekommendationer.

2 Teori

2.1 Informationssäkerhet

Ledell (1991) säger att informationssäkerhet är en integrerad del av verksamheten men att det är nödvändigt med specialister inom området. VD:n har det övergripande ansvaret.

Enligt SIG Security (1998) kan informationssäkerhet kan delas in i tre olika aspekter:

- Fysisk säkerhet: fysiskt skydd av viktiga resurser,
- Organisatorisk säkerhet: administration, drift, underhåll,
- Logisk säkerhet: ”teknisk säkerhet”.

2.1.1 Fysisksäkerhet

Enligt Mitrovic (2001) handlar fysisk säkerhet om att förhindra att det uppstår en fysisk åverkan på informationssystemet eller att någon fysiskt får tillgång till informationssystemen. Oavsett hur bra det logiska skyddet är, är det inte tillräckligt ifall en katastrof inträffar.

SIG Security (1998) skriver att man måste tänka på saker som lås, passerkort, brandlarm och backup-tagning. Det är viktigt att analysera vilka konsekvenserna blir om någon utomstående får tillgång till nätverket och på samma sätt måste man tänka på att gömma servrar och annan känslig utrustning för anställda.

SIG Security (1998) skriver att då all nätverkstrafik och lösenord i det allra flesta fall skickas okrypterat är det även viktigt att kontrollera vilka som kan logga in på nätverket. Speciellt viktigt är det att kontrollera utomstående som är på tillfälligt besök och kanske bara behöver låna en dator för att kolla sin e-post eller liknande. Informationen behöver inte var konfidentiell utan det kan vara vilka program som används. Den informationen kan vara högintressant för en konkurrent eller en som säljer produkter till företaget.

2.1.2 Logisksäkerhet

Användare måste styras och deras beteende måste begränsas med hjälp av tekniska lösningar. Logisk säkerhet innefattar alla mekanismer och all den teknik som finns för att styra och begränsa olika beteende hos användare för att lösa säkerhetsproblem i informationssystem. Någon har sagt att ”säkerhet är till största delen en mängd tekniska lösningar till icke-tekniska problem”. Om alla användare varit lojala och aldrig försökt göra saker som är eller skulle kunna vara förbjudna och aldrig gjort något fel skulle säkerhetsarbetet vara enklare. (SIG Security 1998).

2.1.3 Organisatorisk säkerhet

Det är viktigt alla som använder och kommer i kontakt med informationssystemet är medvetna om vilka regler som finns, att reglerna är relevanta och kan efterföljas, och att alla inte minst förstår varför de finns. Detta är vad organisatorisk säkerhet handlar om, hur systemet ska administreras och hur drift och underhåll av systemet ska ske. Man kan säga att det i princip innefattar all mänsklig interaktion med systemet och de krav som måste ställas på användarna. Det är viktigt att de regler och krav som ställs på användarna och administratörerna är relevanta, kan efterföljas och alla förstår varför de finns. En informationssäkerhetspolicy anger huvudmålsättningen för företagets säkerhetsorganisation och ska spegla allt säkerhetsarbete, (SIG Security 1998).

2.2 Policy och riktlinjer

Ett IT-system ska på bästa sätt stödja en organisations hantering av information. Informationssystemet erbjuder olika möjligheter att lagra, bearbeta eller kommunicera information. Informationssäkerhetspolicy och riktlinjer ska styra:

- hur information hanteras och används i informationssystemet
- hur man hanterar och använder ingående resurser t.ex. applikationer och systemprogramvara.

En informationssäkerhetspolicy är ett långsiktigt dokument som fastställer den inriktning som ska gälla principiella frågor inom en organisation. Riktlinjer har en mer konkret inriktning än informationssäkerhetspolicyn och ska garantera en enhetlig tillämpning av en viss informationssäkerhetspolicy inom organisationen. Riktlinjerna ska revideras i takt med verksamhetens inriktning och den tekniska utvecklingen (Statskontoret, 1997).

Ledell (1991) påpekar att en informationssäkerhetspolicy berör samtliga anställda som arbetar med datorstöd verksamhet. Genom informationssäkerhetspolicyn fås ökad trygghet, trivsel och detta bidrar till ett bättre resultat. SIS (2001) säger att informationssäkerhetspolicyn också kan användas som en plattform för konsekvent agerande och göra de anställda medvetna om säkerhetens betydelse samt visa vägen för att uppnå säkerhetsmålen.

2.2.1 Policydokument

För att få personalen att tänka på IT-säkerheten när de arbetar bör ledningen göra klart för personalen att man tycker att informationssäkerhetspolicyn är viktig. Detta kan ledningen göra genom att sätta ihop ett dokument som talar om informationssäkerhetspolicyn som företaget ska följa och vilka riktlinjer som finns för att underlätta detta arbete.

Enligt Statskontoret (1997) ska detta informationssäkerhetspolicydokument ge den syn som ledningen har på IT-säkerhet och visa vilken inriktning säkerhetsarbetet ska ha. Vidare ska man även i informationssäkerhetspolicydokumentet ta upp hur ansvaret för informationssäkerheten ska fördelas i organisationen.
Ledell (1991) säger att det är nödvändigt dokumentera de principer och målsättningar inom organisationen som gäller för informationssäkerheten. Det mest

naturliga är att göra en informationssäkerhetspolicy som anger riktlinjerna för företagets informationssäkerhetsarbete. SIS (2001) påpekar att organisationens ledning bör klart ange viljeinriktning och visa sitt stöd och åtagande för informationssäkerhet. Detta fås genom att fastställa och underhålla dokumentet gällande informationssäkerhetspolicyn för sin organisation.

2.2.2 Hur ser en informationssäkerhetspolicy ut?

Enligt Statskontoret (1997) måste informationssäkerhetspolicyn ha ett samband med både IT-policyn och verksamheten. Nedan är ett exempel på hur en informationssäkerhetspolicy kan se ut. Under varje rubrik skriver man endast kortfattat vilka mål som finns och man går inte in på hur man ska göra för att uppnå målen.

- IT- informationssäkerhetspolicy för …….
- Definitioner
- Avgränsningar
- Syfte
- Motiv för IT-säkerhet
- IT-säkerhetsnivå
- Budget

Enligt SIS (2001) ska informationssäkerhetspolicyn besvara följande frågor:

- Vad ska skyddas?
- På vilken nivå ska skyddet vara?
- Vilka är ansvarig för informationssäkerheten?
- Hur ska arbetet bedrivs gällande informationssäkerheten?
- Var gäller informationssäkerhetspolicyn?
- Hur ska informationssäkerhetspolicyn följa verksamheten och hotbilden?
- Vilka rättigheter och skyldigheter har medarbetarna?
- Hur ska incidenter hanteras?
- Sanktioner?

Frågor som med stor sannolikhet uppstår utan en informationssäkerhetspolicy och enligt SIS (2001) kan skada verksamheten på olika sätt är:

- Vad är det som gäller?
- Vem är ansvarig för vad?
- Varför ska jag göra något när ingen annan gör det?
- Vad anser ledningen egentligen? Allt är ju prioriterat!
- Det är svårt att skapa underliggande dokument som riktlinjer, anvisningar och instruktioner.
- Vi får inte mellanchefer att prioritera säkerhetsarbetet.

SIS (2001) säger att vid verksamheter som har speciellt skyddsvärd information som personuppgifter och finansiell verksamhet får informationssäkerhetspolicyn ett extra stort värde. Det kan också vara att säkerheten precis blivit en viktig fråga och

det finns ett behov av att markera vad som gäller. Ytterligare ett exempel kan vara att man går in i ett nytt produktområde.

Enligt SIS (2001) har större delen av de organisationer som har ett stort säkerhetsinslag i sin verksamhet en av ledningen uttalad och antagen informationssäkerhetspolicyn som

- är mer genomtänkt än en som inte är antagen,
- kan delges interna och externa intressenter på ett auktoritativt sätt, vilket minskar risken för missförstånd och kan öka affärsmöjligheten genom att minska affärsrisken/-riskerna,
- underlättar granskning av det verkliga tillståndet med hänsyn till policyn.

SIS (2001) säger att en informationssäkerhetspolicy ska peka ut den övergripande inriktningen, slå fast de principer som ska gälla och tydliggöra organisationens inställning till arbetet, i detta fall informationssäkerhetsarbetet. Grunden för organisationens övergripande och detaljerade säkerhetsmål är informationssäkerhetspolicyn. Det är ett centralt och viktigt dokument som fastställs av organisationens högsta ledning och därmed har de också ansvar för att dess innehåll uppfylls.

SIS (2001) skriver att vidareutveckling av speciella frågor gällande ansvar, befogenheter, arbetssätt och beslutsordning liksom verksamhetsinriktning på kort sikt kan göras inom organisationen men beslut ska framgå av ett upprättat protokoll. Åtaganden enligt informationssäkerhetspolicyn måste kunna redovisas och dokumenteras på det sätt man utför dessa. Detta görs med hjälp av fastlagda rutiner som ska säkerställa vilka resultat som uppnåtts för att leva upp till innehållet i och innebörden av informationssäkerhetspolicyn. Det är viktigt att leverantörer, entreprenörer, kunder och samarbetspartners informeras om organisationens syn på säkerhet och deras informationssäkerhetspolicy samt de önskemål och krav som är förknippade med detta. Det innebär exempelvis att organisationens entreprenörer måste leva upp och ta hänsyn till organisationens informationssäkerhetspolicy.

Enligt SIS (2001) är policyn ett komplement till organisationens affärsplan, IT-strategi och de lagar och avtal som finns. Nedan följer ett antal nyckelpunkter som bör ingå i en informationssäkerhetspolicy:

- Viljedeklaration från högsta ledningen
- Fastläggande av att säkerheten är viktig i verksamheten där informationssäkerhetens betydelse för verksamheten anges.
- Definition av begreppet "informationssäkerhet".
- Motiv för varför och vilket slags säkerhet som behövs i organisationen:
  - hot-, sannolikhets- och konsekvensbeskrivning,
  - omvärldens krav eller förväntningar (lagar, avtal och andra krav),
  - den personliga säkerheten,
  - incidenthantering,
  - visa på vilket sätt säkerhet lönar sig.
- Övergripande mål och detaljmål för säkerhetsarbetet

- Ansvarsfördelning inom organisationen med en betoning på det personliga ansvaret.
- Beskrivning av säkerhetsorganisationens utseende, befattningsinnehavare och ansvar.
- Redogörelse för vikten av en avbrottsplan för verksamheten.
- Plan för policyns förverkligande genom exempelvis

  – information/utbildning,
  – säkerhetshöjande åtgärder

- Beskrivning av uppföljningssystem.
- Sanktioner vid i sidosättande av policyn eller andra säkerhetsregler.
- Angivande av dokumentansvarig för policyn och hur den ska revideras och följas upp.

SIS (2001) skriver att det finns lagar och avtal som reglerar organisationens verksamhet. Många verksamheter måste följa särskilda författningar eller krav som ställts upp av myndigheter. Att inte följa regelverket kan orsaka skador för verksamheten, inte bara ur ett juridiskt perspektiv. Synliga skador kan utebli men det finns risk att förtroendet naggas i kanten. Detta kan på sikt förstöra för organisationen. Därför är det viktigt att organisationen följer de lagar och avtal som finns för verksamheten.

2.3 Riktlinjer

För att uppnå målen som är uppsatta i informationssäkerhetspolicyn bör man sätta upp riktlinjer som ska följas av medarbetarna inom organisationen. Enligt Statskontoret (1997) anger riktlinjerna hur man ska uppnå målen i policyn. Riktlinjerna fungerar som ett stöd för de ansvariga inom organisationen som ska upprätthålla den IT-säkerhetsnivå som ledningen satt upp. Riktlinjerna måste tas fram av en inom organisationen som har goda kunskaper inom IT-säkerhet. Lämpliga frågor att söka svar på när man tar fram riktlinjerna kan vara:

- Vem?
- Vad?
- Varför?
- När?
- Hur?

Riktlinjerna som man ställer upp bör vara kortfattade och lätt begripliga samt endast innehålla det viktigaste av budskapet. Om det sker förändringar i omvärlden som påverkar IT-säkerheten måste man omarbeta riktlinjerna så de anpassas till verkligheten.

2.3.1 Exempel på riktlinjer

Statskontoret (1997) menar att syftet med riktlinjerna är att uppnå och vidmakthålla den säkerhetsnivå ledningen har bestämt. När man delar in riktlinjerna bör man dela

in dem i olika områden. Ett sätt att dela in dem är att göra det utifrån de olika driftmiljöer man har. Nedan är exempel på en indelning av riktlinjerna:

- Drift och driftplanering
- Avbrotts- och katastrofplanering
- Utbildning
- Fysiskt skydd
- Risk och sårbarhetsanalyser
- Lokala nätverk
- Arbetsplatser

När man tar fram riktlinjerna menar SIS (2001) att det är viktigt att göra klart vilka rätts- och avtalsregler som finns för varje system. Man ska även utse personer som ansvarar för efterlevnaden av riktlinjerna och förse dessa personer med medel för att kunna sköta denna uppgift.

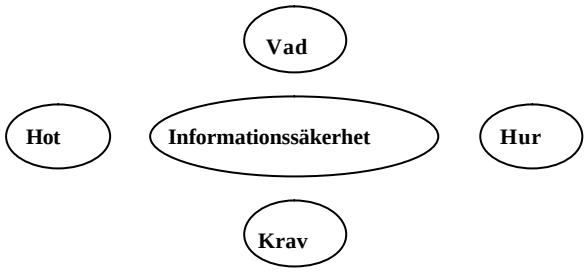
2.4 Ta fram en informationssäkerhetspolicy

När en organisation ska ta fram en informationssäkerhetspolicy är det lämpligt att göra en analys av läget som organisationen befinner sig i. Detta för att kunna utforma en informationssäkerhetspolicy som stämmer bra överens med organisationens behov. Att ta fram en informationssäkerhetspolicy kan vara en lång och ibland komplicerad process. Till sin hjälp bör organisationen använda en metod för att analysera läget.

SIS (2001) menar att om man vill att en informationssäkerhetspolicy ska få avsedd effekt är det några punkter som bör beaktas vid framtagandet av informationssäkerhetspolicy. Den ska

- avspegla huvuduppgiften,
- vara relevant i förhållande till organisationens verksamhet,
- vara långsiktig,
- vara övergripande,
- visa ambitionsnivå och inriktning,
- vara kommunicerbar med organisationens samarbetspartners,
- ha ett enkelt språk,
- vara kortfattad,
- föras ut på ett auktoritativt sätt.

Edwall och Söderbaum (1998) har en figur som visar de delar som ingår i ett informationssäkerhetsarbete. De har identifierat fyra områden som man behöver titta på för att uppnå god informationssäkerhet. Dessa områden är *Vad, Hot, Krav* och *Hur*. Vi menar att tittar man på dessa områden kan man utifrån dessa ta fram en informationssäkerhetspolicy som möter organisationens krav och behov. Nedan är en figur som Edwall och Söderbaum (1998) har tagit fram samt en beskrivning av vad man bör titta på inom varje område.



Figur 1 Informationssäkerhet

2.4.1 Vad

Här tar man reda på vad det är som ska skyddas. Vilken information ska skyddas från allmän åtkomst och vad ska skyddas inom organisationen mellan medarbetarna. Detta handlar även om vilka IT-system som finns i organisationen och vad som ingår i dessa system. Med IT-system menas organisationens databehandlingsresurser. För att få fram vilken information som skall skyddas bör organisationen göra en verksamhetsanalys där man klassificerar informationen utifrån verksamhetskraven och den lagstiftning som finns. (Statskontoret, 1997).

2.4.2 Hot

En definition på hot är enligt SIG Security (1998) ”alla oönskade händelser eller situationer som kan störa verksamheten” och *risk* är ”sannolikheten för att en störning, som medför skada eller förlust, ska inträffa”.

Det är enligt Statskontoret (1997) viktigt att organisationen känner till vilka hot som finns mot IT-systemet och att dessa hot kan variera över tiden. Organisationen måste därför uppdatera hotbilden för att svara mot de förändringar som sker i omvärlden.

Hoten mot organisationen kan vara externa eller interna. Med externa menas att hoten kommer från omvärlden och interna är följaktligen hot som kommer inifrån den egna organisationen. Enligt Statskontoret (1997) kan de interna hoten delas upp i oavsiktliga hot, orsakas av brister i administrativa rutiner, och avsiktliga hot.

Enligt Aronsson (1995) kan man dela in hoten i tre kategorier. Dessa är:

- *Fysiska hot* – dessa hot mot ett datasystem är förhållandevis påtagliga och lättbegripliga. Här handlar det om stöld, brand, sabotage, skadegörelse, vattenskador, elfel och liknande. I princip samtliga av de uppräknade fysiska hoten orsakar, när de verkställs, kortare eller längre avbrott i driften.

- *Logiska hot* – dessa hot innebär någon form av utnyttjande av datasystemet på ett eller annat sätt. Exempel på detta kan vara hackerintrång, avlyssning av data, virusattacker och sabotage.

- *Administrativa hot* – här handlar det om bristfällig hantering av behörighet och andra brister i regler för datasystemet.

2.4.3 Krav

Här tittar man på vilka krav som ställs på det som ska skyddas. Enligt Statskontoret (1997) kan dessa krav variera beroende på vilken organisation man tittar på, men generellt kan man dela in kraven i följande kategorier:

- *Riktighet* – informationen skall vara aktuell, korrekt och begriplig. Dålig kontroll vid inmatning av data, obehörig ändring av data och otillåten användning av systemresurser är exempel på aktiviteter som kan medföra problem med riktigheten.

- *Tillgänglighet* – innebär att användaren ska kunna använda informationen i den omfattning han behöver och inom önskad tid.

- *Sekretess* – med detta menas att känslig informationen inte får avslöjas för obehöriga eller nyttjas på ett otillåtet sätt.

- *Spårbarhet* – erbjuder skydd och återställande från förluster och brott mot säkerheten. Ett system där inloggning under falsk identitet finns gör att man får brist på korrekt spårbarhet. Autenticering är därför en viktig del. Med autenticering menas att användaren identifierar sig så systemet vet att användaren är den han utger sig för att vara.

2.4.4 Hur

Här tittar man på vilka sätt som finns att tillgå för att skydda organisationens informationssystem. Det handlar om tekniska och administrativa åtgärder som organisationen ska vidta för att skydda systemet. De administrativa åtgärderna består av olika regler som är uppsatta för IT-verksamhet och övrig verksamhet och är en förutsättning för att övriga skydd ska få avsedd effekt. De viktigaste administrativa åtgärderna är enligt Statskontoret (1997) att organisationen utarbetar en informationssäkerhetspolicy samt utbildar personalen.

Enligt Statskontoret (1997) ska organisationer som använder IT-stöd i sin verksamhet definiera:

- Riktlinjer för IT-säkerhetsarbetet och en informationssäkerhetspolicy.
- En handlingsplan för IT-säkerhetsarbetet, både på kort och lång sikt.
- Ett utbildningsprogram för personal som är användare av IT-system, detta för att de ska ha kunskapen att arbeta med systemet på rätt sätt.
- Ett utbildningsprogram för IT-personal så de har kunskap att sköta drift och förvaltning av systemet.

De tekniska hjälpmedel som organisationen har till sin hjälp för att skydda organisationens informationssystem är enligt Statskontoret (1997) följande:

Autenticering

Detta innebär att fastställa identiteten på parter som kommunicerar. Detta för att inte ”fel” person ska få tillträde till ett system. Det finns tre olika principer för att åstadkomma detta:

- Något man VET, t.ex. ett lösenord, en personlig kod.
- Något man HAR, t.ex. ett passerkort.
- Något man ÄR, t.ex. biometriska egenskaper som röstmönster eller fingeravtryck.

Enligt Statskontoret (1997) bör man inte skapa gemensamma lösenord till en resurs eftersom det inte går att knyta en viss händelse till en specifik användare.

Enligt Silberschatz, A & Galvin, P (1997) är ett konto en personlig egendom så det är av yttersta vikt för en användare att sätta ett lösenord som är svårt att lista ut för en hacker. Lösenordet ska vara minst 6 tecken långt och bestå av stora och små bokstäver. Vidare bör det innehålla siffror och specialtecken. Detta gör sammantaget att lösenordet blir svårt att gissa eller använda någon metod för att få fram lösenordet. Det är en användares skyldighet att skydda de tjänster han erhållit genom att bland annat:

- Välja ”bra” lösenord.
- Aldrig skriva upp sitt lösenord någonstans.
- Inte skylta med sitt användarkonto öppet så någon ser lösenord.
- Aldrig ge ut sitt lösenord till någon annan.

Kryptering

Kryptering är enligt Jensen (2000) en process i ett antal steg där man ändrar informationen för att åstadkomma en krypterad text hos avsändaren av ett meddelande. För krypteringen används en krypteringsalgoritm. Den motsatta operationen hos mottagaren kallas dekryptering.

Brandvägg

En brandvägg ser enligt Jensen (2000) till att ingen oönskad kommunikation sker utan upptäckt mellan två nät. I IT-informationssäkerhetspolicyn har man definierat vilken trafik som är tillåten i nätet.

Antivirusprogram

Dessa program letar efter kända virus i e-mail, filer och dokument. Vissa program oskadliggör viruset och andra talar om vad den funnit för virus och låter användaren ta bort viruset. Virus är en självreproducerande sekvens av instruktioner som oftast består av en utlösande del och en skadedel. Det är mycket vanligt att en användares dator smittas med ett virus från e-post. Det är viktigt att organisationen har en kontinuerlig uppdatering av sitt virusskydd då det ständigt kommer nya typer av virus (SIG Security, 1998).

Loggning

Loggning är en funktion som registrerar vad en viss användare gör vid ett visst tillfälle. Detta för att i efterhand kunna gå in och titta på vad som har skett (SIG Security, 1998).

2.5 Efterlevnad

För en organisation är det viktigt att medarbetarna följer de riktlinjer som finns uppsatta. Detta kan det finnas olika skäl till. Man kan inom organisationen ha krav som ställs pga säkerhet eller sekretess. Det kan också finnas krav som ställs på organisationen av olika myndigheter, lagar och avtal. Enligt SIS (2001) bör en organisation ta hjälp av en juridisk rådgivare eller annan person med rätt kunskap vid utformning av riktlinjerna för att inte göra fel. Att inte följa de direktiv som är uppsatta kan resultera i skador för organisationen och dessa skador kan vara av juridisk karaktär eller att förtroendet för organisationen skadas.

Ledell (1991) menar att det är VD:n som har det övergripande ansvaret för informationssäkerheten i organisationen. Det är VD: n som ska se till att det finns en informationssäkerhetspolicy och på olika sätt följa upp att denna policy efterlevs.

SIS (2001) menar att informationssäkerhetspolicyn är ledningens instrument för att klart ange inriktningen och visa sitt engagemang för informationssäkerheten -"det här är vår avsikt, så här vill vi ha det och så når vi dit". Att tillföra företagskulturen en ny dimension – "i vår verksamhet är säkerhet ett självklart inslag i arbetet"

I informationssäkerhetspolicyn bör det finnas riktlinjer för vad personalen har tillåtelse att göra och vad de inte får göra med organisationens informationsbehandlingsresurser. All utrustning finns för att stödja organisationen i dess arbete och all annan användning därutöver bör därför ses som obehörig. En medarbetare får inte heller skaffa tillgång till information som är skyddad, och det är upp till organisationens ledning att informera anställda vilken information som är skyddad och vilka följder det kan få att missbruka denna information. Mottagaren ska bekräfta att han fått denna information och detta kan lösas med dialogrutor där användaren vid inloggning bekräftar ett meddelande om att obehörig åtkomst är förbjuden. Bekräftas inte meddelandet ska inte inloggning kunna ske. SIS (2001).

För att kontrollera ifall missbruk sker bör det finnas någon form av uppföljning. För att sköta denna kontroll på ett korrekt sätt då det finns lagar för detta, bör organisationen ta hjälp av person med juridisk kompetens så man inte gör sig skyldig till lagbrott. SIS (2001).

2.6 Utbildning

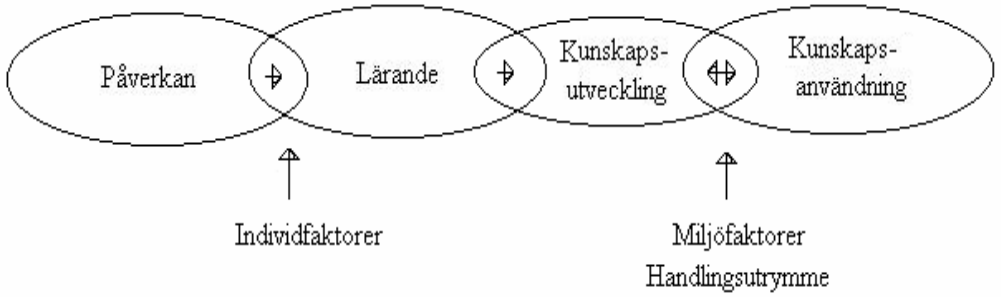
Intresset för lärande organisationer och hur det kan bidra till att öka kompetensen inom organisationen har under senare år ökat. Ur en pedagogisk synvinkel är detta förståeligt då en stor del av det lärande som är önskvärt inom organisationen bäst sker i samband med arbete tillsammans med arbetskamrater. Väl planerade och väl genomförda utbildningar är viktiga för ökad kompetens inom arbetslivet. *”Att sluta utbilda för att spara pengar, är som att att stanna klockan för att spara tid”*, Lundmark (1998).

Lundmark (1998) skriver i en nyutgiven antologi om livslångt lärande om vikten av utbildningsinsatser och lärandet i arbetet. Hon menar att det inte är tillräckligt med lärandet i vardagen grundat enbart på erfarenhet för att utveckla ny kunskap. För att lärandet ska kunna utvecklas krävs det distans till och reflektion av vardagligt

lärande och det fås genom olika planlagda insatser i form av utbildning, folkbildning och självstudier.

När det gäller planering och utbildning tycker Lundmark (1998) att det är viktigt att tänka i termer av olika analysnivåer. Hon menar att det är viktigt att även förstå processerna på individnivå om man skall förstå utbildning och utbildningsresultat. I arbetslivet liksom i det vanliga livet lär sig människor på olika sätt, likaså genom deltagande i utbildning som av arbetsuppgifter och genom kollegor. Det man försöker göra vid en personalutbildning är att systematisera och effektivisera den inlärning som för arbetet bedöms värdefull.

Centralt i detta sammanhang är att nya kunskaper verkligen används i arbetet. Nedan i figur 2 visas gången från påverkan till kunskapsanvändning. Figuren illustrerar den pedagogiska processen vid utbildning och annan pedagogisk påverkan, Lundmark (1998).



Figur 2 Förändringar vid pedagogiskt påverkan i arbetslivet med exempel på faktorer av intresse för effekter av utbildning.

Modellen ska uppfattas som en beskrivning av ett tidsmässigt skeende. Det första som sker är en påverkan som initialt leder till ett lärande. Lärandet bearbetas medvetet och omedvetet genom både tanke arbete och ytterligare erfarenheter. Vidare kan det man lärt sig förändras, vilket i figuren kallas kunskaps utveckling. Kunskapsanvändningen innebär att det man lärt sig används i arbetet. Ytterligare kunskapsutveckling sker ofta vid användandet av de nya kunskaperna, därav den dubbelriktade pilen. Lärandet varierar mellan deltagarna beroende på tidigare individuella faktorer. För att utbildningen ska resultera i kunskapsanvändning krävs att det finns ett handlingsutrymme dvs. att det finns förutsättningar i arbetssituationen för användning av den nya kunskapen. Lundmark (1998).

Dilschman och Berg (1996) skriver att det är lednings ansvar att utnyttja lärandet för organisationens bästa och sprida kunskap. Lundmark (1998) anser att ledningen behöver metakompetens d.v.s. kompetens om kompetens som innebär att de ska vara medvetna om den lärande processen. Ledningen måste se till att stödja lärandet och aktivt stimulera till nya kunskaper. Lärandet sker inte av sig själv. För ett lärande krävs det stödjande strukturer och system för att tillvarata, sprida och använda det lärande som sker.

3 Metod

Metoden beskriver vilken information som ska samlas in och hur det ska göras. När man förstår den använda metoden, blir också den insamlade informationen mer meningsfull. I följande kapitel kommer först vårt undersökningssätt att beskrivas och därefter redogörs vår datainsamlingsmetod och vilka datakällor vi har använt oss utav. I slutet av kapitlet berättar vi om vår fallstudie och vilket tillvägagångssätt vi har haft.

3.1 Undersökningssätt

3.1.1 Deduktivt eller induktivt

Vid ett forskningsarbete kan angreppssättet vara induktivt eller deduktivt. Det deduktiva angreppssättet kan sägas följa bevisandets väg, vilket innebär att den utgår från redan befintlig forskning, tidigare resultat och teorier. Forskaren har redan före forskningen en klar bild av den verklighet han ska studera. När forskaren tolkar, eller förutspår händelser och resultat, baserat på tidigare kunskap, drar han deduktiva slutsatser. Induktiv forskning utgår från händelser i verkligheten, som ger upphov till ny teori. Forskaren studerar forskningsobjektet utan att först ha förankrat undersökningen i en tidigare vedertagen teori, och utifrån den insamlade informationen, empirin, formulerar en teori. Detta innebär att forskaren lär sig ämnet genom sitt arbete. (Patel och Davidsson, 1994).

Vi har i våran undersökning valt att arbeta efter det deduktiva arbetssättet. Detta eftersom det redan finns relevant forskning och teorier inom vårat ämnesområde. Vi har inget forskningsobjekt som vi tittar på och skapar någon ny teori. Vi tittar på de teorier som redan finns och ser om vårt forskningsobjekt följer de kunskaper som redan finns inom området. Detta gör att vi kan dra deduktiva slutsatser om den information som vi samlar in.

3.1.2 Kvalitativt eller kvantitativt

En annan vanlig uppdelning av forskningsmetoder är mellan kvalitativ respektive kvantitativ forskning. Enligt Yin (1994) skiljer forskare på kvalitativ och kvantitativ forskning, inte genom typen av bevis utan genom olika filosofiska övertygelser. Dessa skillnader i synsätt har skapat en hel del debatt inom forskningens utvecklingsområde. Patel och Davidsson (1994) menar att man förenklat kan säga att beteckningarna ”kvalitativt” och ”kvantitativt” syftar på att berätta på vilket sätt man analyserar den information som är insamlad.

Enligt Patel och Davidsson (1994) innebär kvantitativt inriktad forskning att man använder sig av statistiska bearbetnings- och analysmetoder, medans man i kvalitativ forskning använder sig av verbala analysmetoder. Med en verbal analysmetod menar Patel och Davidsson (1994) att det inte är analysmetoderna som är verbala utan datans form.

Patel och Davidsson (1994) säger att de båda inriktningarna ofta framställs som oförenliga men menar att så inte är fallet i praktiskt forskningsarbete. De menar att kvalitativ och kvantitativ inriktning är var sin ändpunkt på ett kontinuum, och att

huvuddelen av dagens forskning befinner sig någonstans emellan dessa två ändpunkter.

Förenklat kan man säga att är vi intresserade av frågor som rör ”Var? Hur? Vilka är skillnaderna?” så är kvantitativa metoden att föredra. Vi har i vår forskning bestämt oss för att använda oss av den kvantitativa inriktningen eftersom vi har valt att undersöka hur de anställda följer organisationens informationssäkerhetspolicy. Eftersom vår forskningsfråga är ”Hur efterlevs informationssäkerhetspolicyn i en organisation?”, anser vi därför att den kvantitativa inriktningen är den metod vi bör använda i vår studie.

3.2 Datainsamlingsmetod

Den metod vi ska använda oss av i våran c-uppsats är en fallstudie. Sett till våran forskningsfråga och syftet med vår rapport anser vi det naturligt att använda oss utav en fallstudie eftersom vi tittar på en teori och ser hur det stämmer med verkligheten. Enligt Yin (1994) börjar en fallstudie med en definition av det problem eller ämne som skall studeras samt en uppbyggnad av fallstudiemetoden. Nästa steg är att förbereda datainsamlingen och sedan utföra intervjuer eller enkäter. Det är viktigt att förbereda sin datainsamling väl så att man får ett bra underlag. Denna datainsamling bygger på flera kriterier, bl.a. forskarens egenskaper, gruppförberedelser, datainsamlingsprotokoll samt pilotfallstudie.

Patel och Tebelius (1987) skriver att en fallstudie undersöker ett större antal variabler i detalj på ett mindre antal individer. Det innebär en undersökning av en mindre grupp där själva fallstudien oftast utförs i individens naturliga miljö. Syftet är för det mesta att studera processer och förändringar. Styrkan i att använda fallstudier i sin forskning är att den ger en möjlighet att generalisera från en kontext till en annan.

3.3 Metoddiskussion

För att få svar på vår problemfråga har vi valt att göra både en intervju och en enkätundersökning. Vi tyckte att i detta fall var praktiskt att först intervjua den säkerhetsansvarige på organisationen och sedan göra en enkätundersökning bland de anställda.

Intervjun var till för att få synpunkter från en person som varit med vid utvecklingen av policyn, och därmed kan berätta hur det är tänkt att det ska fungera, berätta lite om framtagningen och hur man har skött förankringen av policyn. Tanken var också att han kunde berätta om det hade hänt några olyckor, tex informationsförluster eller liknande, men då policyn var ny var det svårt för han att komma på någon händelse.

Vi tvekade länge om huruvida vi skulle göra intervjuer eller använda oss av enkäter bland de anställda. Men efter att ha intervjuat respondenten fick vi reda på att deras policy var ny och de inte hunnit göra någon utvärdering. Vi diskuterade detta med respondenten och kom fram till att det var bättre att göra en enkätundersökning sett ur forskningsfråga och vilket säkerhetsmedvetande de anställda har. Han ville även

att vi skulle använda oss av enkäter för att vi skulle nå ut till hela Skattemyndigheten i Luleå.

Det finns både för- och nackdelar med en enkätundersökning, dels finns det ingen närvarande som kan förklara frågor som är oklara, dels kan bortfallet bli stort och frågor som är öppna svaras bara av de som är mest intresserade. (Dahmström, 1996). Men för oss vägde fördelar in som:

- Möjlighet att skicka enkäter till många personer
- Många slag av frågor går att ställa
- Kan besvaras då respondenten har tid

Detta gjorde att vi valde att använda oss av enkäter. Intervjuer tar även upp väsentligt mer tid vid själva utförandet och det finns risk för att intervjueffekter uppstår. (Dahmström, 1996).

3.4 Datakällor

Det datakällor vi har använt oss av är:

Primära

- Intervju
- Enkäter

Sekundära

- Litteratur från Luleå universitets bibliotek
- Fjärrlån
- Internet

De nyckelord vi sökte på var bl.a. policy, utbildning, säkerhet och förankring. För det empiriska materialet använde vi oss av både intervjuer och enkäter. Vår intervju var dock mer en förberedelse för att kunna utforma vår enkät. Intervjun gav oss information av mer allmän karaktär av hur RSV och skattemyndigheten i Luleå är uppbyggd.

3.5 Vår Fallstudie

I dagens samhälle där fler människor använder myndigheters informationssystem för att utföra olika uppgifter är det viktigt att myndigheten kan erbjuda en hög säkerhet och få användarna att känna förtroende för systemet. Vi ska med tanke på detta genomföra en fallstudie där vi gör en undersökning av en statlig organisation.

Vi har valt att genomföra en kvantitativ fallstudie och därför har vi använt oss av dessa insamlingsmetoder:

- Intervjuer,
- Enkät

- Studier av dokument.

För att kunna genomföra vår undersökning har vi varit tvungen att sätta upp ett antal kriterier för den organisation vi ska undersöka. Detta har vi gjort för att få fram en organisation som är relevant för vår frågeställning. De kriterier vi har satt upp är:

- information i organisationen ska vara av sådan art att det är olämpligt ifall den kommer i orätta händer.
- Organisationen måste ha en definierad informationssäkerhetspolicy.

En definition på en informationssäkerhetspolicy är enligt Statskontoret (1997) att *”Policyn uttrycker företagsledningens syn på behovet av IT-säkerhet och anger målen för IT-säkerhetsarbetet”*. Vidare menar de att utformningen av informationssäkerhetspolicyn inte får vara för detaljerad eller för allmänt hållen. Detta för att man ska kunna följa upp innehållet i informationssäkerhetspolicyn.

Att hitta en organisation som uppfyllde våra kriterier var inte en uppgift som var helt och hållet enkel. I flera fall var det svårt att hitta en organisation som hade tid att avsätta för vår undersökning och i andra fall saknade man helt enkelt en klart definierad informationssäkerhetspolicy. Dessa faktorer gjorde att detta inte var en helt enkel uppgift.

3.6 Tillvägagångssätt

Vi satte oss först ner och funderade på vad det var vi skulle undersöka. När vi valt ämne började vi med att söka på Internet för att se vad ämnet handlade om i stora drag. Detta för att göra det möjligt att söka efter relevant litteratur i biblioteket på Luleå Tekniska universitet samt på biblioteket i Luleå. Vi sökte efter böcker som tog upp informationssäkerhet, policy, utbildning och hot mot företagets informationssystem.

Vi skrev ner de teorier som var relevanta för det problemområde vi valt. Vi gick sedan igenom teorierna för att kunna precisera problemet. När vi hade ett problem tittade vi på tänkbara undersökningsgrupper och kom fram till att vi skulle titta på en statlig organisation. Vi valde att titta på Riksskatteverket som är en stor organisation med många avdelningar som är utspridda över hela landet. Valet att enbart titta på en organisation motiverade vi med att Riksskatteverket har en typisk uppbyggnad av sin organisation och att titta på en liknande organisation ansåg vi inte skulle tillföra något. Riksskatteverket hade även nyligt infört en informationssäkerhetspolicy och vi ansåg att det var relevant att titta på hur den efterlevs.

Efter att ha valt undersökningsgrupp gick vi vidare och tittade på vilka metoder vi skulle använda för att samla in information. Vi kom fram till att vi skulle använda oss av intervjuer och enkäter. Enkäten utformade vi genom att läsa vår teori och granska vår organisations informationssäkerhetspolicy samt utbildningsmaterial. Detta gav oss underlag för att ta fram frågor till vår undersökning av empirin. Vår enkät delade vi ut till personalen på skattemyndigheten i Luleå. Enkäten delades ut till all personal utan hänsyn till befattning inom organisationen. Detta för att se om det skulle skilja något på kunskap om datasäkerhet beroende på befattning.

Materialet till intervjun tog vi fram genom att studera vår teori. Intervjun genomfördes genom telefonintervju med en respondent för skattemyndigheten i Luleå.

När vi hade gjort intervjun och samlat in de enkäter vi delat ut analyserade vi de svar som vi fått in. När det gäller enkäten tog vi i analysen endast med de frågor som var relevanta för våran studie och utelämnade de svar som inte hörde dit.

Till sist funderade vi på vilka slutsatser vi kunde dra av vår studie.

3.7 Reliabilitet och Validitet

Reliabilitet och validitet handlar om att man kritiskt ska granska den metod som har använts vid insamling av sina data. Detta gör man för att avgöra informationens tillförlitlighet och giltighet. Reliabiliteten, dvs. tillförlitligheten är alltså sättet att bedöma till vilken grad tillvägagångssättet skulle ge samma resultat om det skulle utföras vid ett senare tillfälle och med samma förutsättningar. (Bell, 2000).

Med begreppet reliabilitet kollar man med andra att: vi mäter på rätt sätt? Använder vi den bästa metoden för att utvärdera användbarhet eller finns det mer exaktare och bättre metoder? Vissa undersökningsmetoder är mer eller mindre precisa och kan därför, även om man genomför undersökningarna på exakt samma sätt flera gånger, ge mer eller mindre olika resultat - vi får en dålig träffbild. Ju exaktare vårt verktyg, det vill säga vår valda metod, är, desto bättre reliabilitet har vi. (Patel, 2003).

För att kunna återupprepa en tidigare genomförd studie är noggrann dokumentation av stor betydelse. (Yin, 1994).

Genom att vi har dokumenterat allt arbete i vår undersökning har vi bidragit till att öka vår reliabilitet. Genom att hämta våra frågor till vår intervju från vår teori och följa dessa frågor under intervjun gjorde att vi fick en ökad reliabilitet när det gäller intervjun. När det gäller enkäter finns det en risk för att enkätfrågor misstolkas av den svarande men detta har vi inte sett några större tecken på. De frågor vi ställt i enkäten har vi försökt göra kortfattade och med enkla svarsalternativ. Detta anser vi bidrar till att öka reliabiliteten.

Enligt Yin delas validiteten in i konstruktionsvaliditet, intern validitet och extern validitet.

- *konstruktionsvaliditeten* skapar korrekta sätt för att kunna möjliggöra mätbarhet i den undersökning som genomförs. För att öka validiteten ska man inhämta bevis från flera olika källor, tex dokumentation, arkivmaterial, intervjuer och direkta observationer. Sedan bör en kedja av bevis upprätthållas under hela arbetet. En extern person som läser fallstudien ska kunna följa alla steg i undersökningen. Det sista som kan göras för att öka validiteten är att låta respondenterna granska ett utkast på fallstudiens rapport. (Yin, 1994).

- *intern validitet* används i samband med beskrivande och kausala studier. Här skapas orsakssamband vilket innebär att söka händelser som leder till andra händelser. Om undersökaren finner ett orsakssamband mellan två händelser och missar en ytterligare händelse som har inverkan på företeelsen då kan den interna validiteten påverkas negativt. (Yin, 1994).

- *externa validiteten* lägger fokus på att bestämma om studiens resultat kan generaliseras utifrån de fall som ingår i fallstudien. (Yin, 1994).

Våra olika informationskällor var litteratur inom ämnet, en intervju, våran enkätundersökning samt dokumentation i form av informationsmaterial som vi fick av Riksskatteverket. För att öka konstruktionsvaliditeten dokumenterade vi datainsamlingens genomförande samt hur data skulle bearbetas och analyseras. Sen har vi låtit en respondent granskat ett utkast av våran rapport. Den interna validiteten kunde stärkas genom att vi använde oss av en personlig intervju samt dokumenterade intervjun ordagrant. Genom att intervjun dokumenterades kunde giltigheten hos orsakssambanden öka eftersom viktiga detaljer i intervjun inte förbisågs.

4 Empiri

4.1 RSV

Här ska vi skriva om Riksskatteverkets arbete kring deras informationssäkerhetspolicy. Informationen kommer från broschyrer som skickats till oss från RSV. Broschyrer som heter:

- Lathund om informationssäkerhet för RSV-koncernen
- Information om ledningssystem för informationssäkerhet (LIS)
- RSV LIS ledningssystem för informationssäkerhet

För att genomföra våran fallstudie valde vi RSV. De driver en omfattande verksamhet med en stor exponering och tänkbara aktörer med varierande uthållighet kan vilja skada deras verksamhet. Deras skydd ska vara uthålliga och med hög kvalitet både internt och externt.

En förutsättning för våran studie är att det finns en införd informationssäkerhetspolicy. RSV har nyligen infört och utbildat i RSV LIS, ledningssystem för informationssäkerhet. Respondenten som vi intervjuade hade själv varit med och utbildat personalen i RSV LIS. För att utveckla informationssäkerheten har RSV tagit fram broschyrer, utbildningsmaterial och en lathund för systemägare och anställda. Stämmer bra enligt teorin att utbildning är en viktig del i en organisation, se avsnitt 2.6.

4.1.1 Allmänt

Riksskatteverket är en samhällsviktig organisation och de skapar förutsättningar för ett fungerande samhälle. RSV har stora krav på deras rättsäkerhet i deras beslutfattanden. Koncernen har ett stort informationssystem med 105 koncerngemensamma IT-system, varav 21 är samhällsviktiga. Organisationen är beroende av sitt IT-stöd och man står inför många nya utmaningar bl.a. deklaration över Internet.

Riksskatteverkets vision är ett samhälle där alla gör rätt för sig där RSV ska bidra med enkla och tidsenliga regler samt den bästa förvaltning i medborgarnas tjänst.

4.2 Informationssäkerhetspolicy och riktlinjer

Riksskatteverket har en väl genomarbetad informationssäkerhetspolicy som infördes 2001-2002. Informationssäkerhetspolicyn kallas LIS som står för ledningssystem för informationssäkerhet. LIS innehåller regler och riktlinjer för hantering av information inom organisationen. Vilket också tas upp i teorin, se avsnitt 2.2.

RSV stod inför ett vägval efter en internrevision där de var missnöjda med informationssäkerheten och det var då man valde att ta ett rejält grepp om informationssäkerheten. LIS är grundat på den internationella standarden ISO 17799 som SIS (2001) handboken bl.a. är baserad på och vi tagit mycket av våran teori ifrån. Se avsnitt 2.2.2. Respondenten sa vid intervjun att man följt denna internationella standard men anpassat den till Riksskatteverkets organisation.

LIS säger att information som skapas, inhämtas och förvaltas inom RSV-koncernen är en strategisk viktig resurs. Med stöd av lagar och förordningar ska särskilda åtgärder vidtas för att säkerställa att informationen

- är korrekt och fullständig.
- finns tillgänglig vid behov.
- är skyddad mot obehörig åtkomst.
- kan spåras och återskapas.

Enligt teori avsnitt 2.2.2 är viktigt att klargöra vad som gäller. Nedan ser man att LIS inte bara handlar elektronisk information.

Ledningssystemet handlar inte bara om regler och rutiner hur vi hanterar elektronisk information. Regler och rutiner hur vi hanterar t.ex. dokument och muntlig information ingår också i LIS. Sammanställningen av dessa regler och rutiner finns i en ämnesdatabas ”Verksamhetsskydd” som de anställda kan söka i för information och vägledning.

4.3 Policydokument

Grundläggande krav som LIS har på informationssäkerheten och de anställda inom koncernen samt det externa samarbetspartnerna är:

- Alla medarbetare ska ha kunskap om och tillämpa gällande föreskrifter samt vara medvetna om det personliga ansvaret.

- Informationssäkerhetsfrågor integreras i det vardagliga arbetet. Personal som arbetar med sådan information som omfattas av säkerhetsskyddslagen ska genomgå säkerhetsprövning.

- Informationssäkerheten ska hålla lika god nivå vid extern åtkomst som vid arbete inom myndigheten.

- De ska finnas en definierad grundsäkerhetsnivå för alla lokaler och arbetsplatser.

- Det ska finnas ett definierat grundskydd för information.

- Tilldelning av behörigheter ska ske i ett enhetligt administrerat behörighetssystem. Behörigheter ska baseras på personliga tjänstecertifikat och definierad arbetsuppgifter.

- Krav på informationssäkerhet ska behandlas som en integrerad del av systemutvecklings- och systemförvaltningsprocesserna. Kontroll av kravuppfyllelse ska ske innan systemet tas i drift.

- Det ska finnas en kontinuitetsplan för koncerngemensamma informationssystem. Planen ska regelbundet granskas och uppdateras.

- Efterlevnad av riktlinjer, anvisningar och rutinbeskrivningar ska granskas genom återkommande uppföljning och kontroll.

Här har man angett sin viljeinriktning samt klart och tydligt skrivit ned de grundläggande kraven man har på det anställda och de externa samarbetspartnerna. Allt enligt teorin, avsnitt 2.2.1

För vem

LIS vänder sig till alla medarbetare inom koncernen och alla de som arbetar på uppdrag av koncernen. Systemet syftar till att fungera som stöd i arbetet för chefer, medarbetare och systemägare/projektledare. Alla har ett gemensamt ansvar att hantera information på ett korrekt sätt. LIS är ett strukturerat sätt att säkerställa RSV-koncernens krav på god informationssäkerhet. Detta stämmer bra överens med teorin, se avsnitt 2.2.

Nytta

Största nyttan med LIS är att alla regler och rutiner samlas på ett ställe. En annan vinst med LIS är att alla anställda får en gemensam helhetssyn på hur de ska bedriva sin verksamhet gällande informationssäkerhet. Gemensamma begrepp har skapats vilket gör att man pratar samma språk och kan starta en diskussion om normer för informationssäkerhet på arbetsplatsen. Enligt teorin är det nödvändigt att samla alla regler och rutiner på ett ställe. Se avsnitt 2.2.1.

Varför

RSV LIS kom till efter det att man själva uppmärksammat att de inte hanterade all information rätt. De kände att deras regler och rutiner inte hade hängt med i samhällsutvecklingen. Riksrevisionsverket och internrevisionerna konstaterade också att det fanns brister. RSV står inför nya utmaningar med ett ökat användande av t.ex. Internet. Kraven från deras uppdragsgivare är tydliga: information ska hanteras på ett säkert sätt. Allt enligt teorin, avsnitt 2.2.2.

Innehåll

Ledningssystemet omfattar elva nyckelområden som riktar sig till olika målgrupper:

1. Introduktion definierar bl.a. begreppet informationssäkerhet och innebörden av LIS.

2. Informationssäkerhetspolicyn är systemets ”hjärta” och innehåller de grundläggande värderingarna för informationssäkerhet. Målgruppen är alla anställda och uppdragstagare.

3. Säkerhetsorganisationen beskriver hur säkerhetsarbetet i stort organiseras inom RSV koncernen. Dessutom beskrivs vilket ansvar som följer med olika befattningar. Den talar även om hur informationssäkerhetsfrågorna ska hanteras vid kontrakt med utomstående personer och organisationer. Målgrupperna är alla anställda.

4. Klassificering och kontroll av informationstillgångar visar på behovet av att klassificera information och hålla kontroll över andra tillgångar. Den syftar till att ge vägledning om hur hantering och klassificering ska utföras. Målgruppen är chefer och systemägare.

5. Personal och säkerhet tar upp vad man ska tänka på vid rekrytering av medarbetare och den anställdes skyldigheter att bl.a. rapportera incidenter och programfel. Målgruppen är alla medarbetare.

6. Fysiskt skydd av information beskriver hur lokaler och utrustning ska skyddas. Här beskrivs också vad man ska tänka på när man hanterar information utanför den egna arbetsplatsen. Målgruppen är chefer/lokalansvariga.

7. Styrning av kommunikation och drift – tekniskinfrastruktur beskriver bla IT-säkerheten inom koncernen. Målgruppen är IT-avdelningens medarbetare, chefer och systemägare.

8. Tilldelning och uppföljning av användares behörigheter eller behörighetssättning behandlar frågor om behörighetstilldelning och loggar. Målgruppen är chefer och alla medarbetare.

9. Systemutveckling och underhåll rör informationssäkerheten i utvecklings- och underhållsprocesserna. Målgruppen är systemägare, systemförvaltare och projektledare.

10. Kontinuitets-, avbrott och katastrofplanering behandlar avbrott i IT-system och hur vi ska agera vid andra avbrott t ex vid brand eller översvämning. Målgruppen är systemägare och RSV IT.

11. Uppföljning tar upp hur vi ska undvika att handla i strid mot lagar och andra författningar, avtal och andra yttre säkerhetskrav. Målgruppen är myndighetschefer och systemägare.

Detta stämmer bra överens med teorin, se avsnitt 2.2.2.

4.4 Riktlinjer

Riksskatteverket har utformat en lathund för informationssäkerhet, där målet är att skapa säkerhetsmedvetenhet hos det anställda. Eftersom RSV-koncernen hanterar stora mängder information som är en strategisk viktig resurs och för att i fortsättningen ha samma förtroende från omvärlden är det viktigt att informationen som hanteras är riktig och att den inte kommer obehöriga till del. Lathunden är ett utdrag ur RSV-koncernens ledningssystem för informationssäkerhet, RSV LIS. Lathunden riktar sig till alla medarbetare och innehåller ett antal regler och riktlinjer som anställda kan följa för att behålla en god informationssäkerhet. Enligt lathunden bygger en god informationssäkerhet på en aktiv medverkan av de anställda. Lathunden är tänkt att bli ett bra hjälpmedel i det dagliga arbetet. Detta stämmer med teorin som säger att det är viktigt att sätta upp riktlinjer, se teoriavsnitt 2.3.

4.5 Fallstudie

Vår fallstudie har bestått av en intervju med säkerhetsansvarig på Riksskatteverket samt enkäter. Vi delade ut 105 enkäter som fördelades på de olika avdelningar (ekonomi-, analys-, rättsenhet osv.) som finns på skattekontoret i Luleå. Anledningen till att titta på flera avdelningar var att få en bredare bild av läget.

Respondenterna som svarat på vår enkät är användare som jobbar med personuppgifter och andra känsliga data. Av de 105 enkäter som vi skickade ut fick vi tillbaka 49 stycken, vilket ger en svarsfrekvens på cirka 47 %.

4.5.1 Enkätundersökning

I detta avsnitt har vi gjort en sammanställning av våran enkätundersökning. Vi har på ett enkelt och överskådligt sätt sammanställs svaren i tabellform nedan.

1. Man eller kvinna?

Man	Kvinna
18	31

2. Din ålder

16-24	25-35	36-45	46-55	56-
1	7	6	20	15

3. Vad har du för anställning?

Tillsvidare anställning	Vikarie	Timanställd
49		

4. Har du chefsbefattning?

Ja	Nej
4	45

5. Medelvärde anställningsår: 22,5

6. Har du något intresse av datorer?

Mycket intresserad	Intresserad	Lite intresserad	Inte alls intresserad
5	28	16	

7. Har du någon dator hemma?

Ja	Nej
44	5

8. Hur ofta använder du din dator hemma?

Varje dag	Någon gång i veckan	Någon gång i mån	Nästan aldrig	aldrig
14	17	11	2	

Utbildningsfrågor

9. Tar du på egen hand del av någon information rörande informationssäkerhet?

Ja	Nej
34	15

10. Har din yrkesutbildning gett dig någon utbildning/information i informationssäkerhet?

Ja	Nej	Vet ej
28	18	3

11. Har du deltagit i annan utbildning där informationssäkerhet har ingått? Exempelvis på annan arbetsplats (utanför RSV), annan utbildning eller studiecirkel.

Ja	Nej	Vet ej
9	37	3

12. Har RSV gett dig utbildning i informationssäkerhet?

Ja	Nej	Vet ej
37	9	3

13. Hur ofta får du utbildning i informationssäkerhet?

1 gång i månaden	1 gång per kvartal	1 gång per år	Aldrig	Annat alt.
		12	12	25

14. Om du fått någon utbildning gällande informationssäkerhet, beskriv i vilken form denna gavs? Exempelvis kurs, litteratur för självstudier eller webbaserad information.

Litteratur	Kurs	Information	Föreläsning	Webb	bortfall
5	18	5	3	13	5

15. Om du har mottagit någon utbildning ingick det någon skriftlig information av det som du fick lära dig? (Något som du fick behålla)

Ja	Nej	Bortfall
32	10	7

16. Om utbildning inte skett, har du då fått annan information i informationssäkerhet? Tex muntligt, dokument eller broschyr.

Ja	Nej
21	3

17. Har det skett någon kontroll av vad ni anställa kan rörande informationssäkerhet?

Ja	Nej
2	47

18. Anser du att du behöver mer utbildning i informationssäkerhet?

Ja	Nej
25	24

19. Hur ofta besöker du RSV:s egen hemsida gällande IT-säkerhet?

Dagligen	En gång i veckan	En gång i månaden	Aldrig
2	1	15	31

Frågor om Policy

20. Har du något intresse av informationssäkerhet?

Mycket intresserad	Intresserad	Lite intresserad	Inte alls intresserad
3	24	21	1

21. Känner du till om det finns någon IT-säkerhetspolicy på RSV?

Ja	Nej	Vet ej
44	1	4

22. Har du läst IT-säkerhetspolicyn eller på annat sätt tagit del av den?

Ja	Nej	Vet ej
37	10	2

23. Har du tillgång till något exemplar av IT-säkerhetspolicyn?

Ja	Nej	Vet ej
29	14	6

24. Tycker du att IT-säkerhetspolicyn är lätt att förstå och ta till sig?

Mycket lätt	Lätt	Varken lätt eller svårt	Svårt	Mycket svårt	Tveksam, vet ej, minns ej
1	7	23	1		17

25. Tycker du att din sektions/enhetschef har gjort tillräckligt för att göra dig medveten om att RSV har en IT-säkerhetspolicy?

Ja	Nej	Bortfall
25	22	2

26. Har ni någon ansvarig på din sektion/enhet som ser till att informationssäkerhetspolicyn följs?

Ja	Nej	Vet ej
8	14	27

27. Känner du till om RSV har några riktlinjer som ni ska följa för att kunna uppnå målen i IT-säkerhetspolicyn?

Ja	Nej	Vet ej
21	5	23

28. Har du läst dessa riktlinjer eller på annat sätt tagit del av dem?

Ja	Nej	Vet ej
15	17	17

Säkerhetsmedvetande frågor

29. Känner du till din arbetsplats regler som gäller när man lämnar sin dator obevakad?

Ja	Nej	Vet ej
47		2

30. Hur ofta bör du logga ut när du lämnar din dator obevakad?

Alltid	Ofta	Sällan	Aldrig
47	1	1	

9. Hur ofta bör du ändra ditt lösenord?

En gång i veckan	Varannan vecka	En gång i månaden	Varannan månad	En gång per år
1	2	8	37	1

10. Medelvärde antal tecken: 6

33. Känner du till hur ett säkert lösenord bör vara utformat?

Ja	Nej
30	19

34. Är det okej att lämna ut sitt lösenord till en kollega?

Ja	Nej	Ibland
1	47	1

35. Ifall du svarat ja på föregående fråga, byter du då lösenord efteråt?

Ja	Nej
1	

36. Låter du andra använda en dator som du loggat in på?

Ja	Ja, men bara då jag är med	Ibland	Nej aldrig
3	27	2	17

37. Har du tillgång till Internet på jobbet?

Ja	Nej
48	1

38. Är det okej att ladda ner program från Internet?

Ja	Nej	Ibland
2	42	5

39. Har du någon gång använt disketter hemifrån på jobbet?

Ja	Nej
8	41

40. Om du misstänker brott eller brister gällande din arbetsplats säkerhetsregler vet du då vem du skall vända dig till?

Ja	Nej
41	8

41. Har du fått information om vad du skall göra vid upptäckt av virus på din dator?

Ja	Nej	Vet ej
44	1	4

42. Använder du e-post på jobbet?

Ja	Nej
45	4

43. Känner du till om det finns några regler gällande e-post?

Ja	Nej
42	7

44. När du skickar e-post, vem kan läsa den förutom du själv?

Mottagare	Mottagare och systemansvarig	Alla med tillgång till RSV:s datorsystem	Vet ej
8	31	3	7

45. Brukar du använda e-posten för att skicka/ta emot privata meddelanden?

Ja	Nej
23	26

46. Har du någon gång öppnat e-post när du varit osäker vem avsändaren var?

Ja	Nej
13	36

47. Hur mycket loggas (kan spåras) av det som du gör på datorn?

Allt	En del	Ingenting	Vet ej
43	2		4

4.5.2 Sammanställning av enkätundersökning

Bakgrundsfrågor

Vi anser att det underlättar att ta till sig information om datasäkerhet ifall användaren har ett intresse av datorer. Majoriteten av respondenterna är intresserade eller mycket intresserade av datorer och har en dator hemma som de använder minst en gång i veckan.

Utbildning

De flesta som har svarat på enkäten, 2/3, tar på egen hand del av information om informationssäkerhet. Majoriteten har fått utbildning av skattemyndigheten angående datasäkerhet och lite mer än hälften har fått utbildning även på annan arbetsplats. Det är lite svårt att ange hur ofta de får utbildning eftersom 12 personer svarat att de får utbildning i datasäkerhet en gång per år och 12 anger aldrig. Däremot har 25 personer angett annat alternativ. De flesta har gått kurs i ämnet och en hel del har tagit del genom webbaserad information.

Bland de som inte fått någon utbildning så har majoriteten fått ta del av information om datasäkerhet. Däremot är det bara 2 av 47 som svarat Ja på frågan om det sker någon kontroll om vad de anställda kan rörande informationssäkerhet. Till sist anser cirka 51 % att de behöver mer utbildning om ämnet.

Frågor om policy

De flesta är intresserade av informationssäkerhet och känner även till att RSV har en informationssäkerhetspolicy. Samma sak gäller även att de flesta läst om informationssäkerhetspolicyn och har även tillgång till den.

Informationssäkerhetspolicyn är varken lätt eller svår att förstå. Nära hälften anser att enhetscheferna inte gör tillräckligt för att göra de anställda medvetna om att det finns en informationssäkerhetspolicy och de flesta svarar Nej eller Vet ej på frågan om de har någon ansvarig som ser till att policyn följs. Mer än 50 % känner inte till om RSV har några riktlinjer för att uppnå målen i policyn och 2/3 har inte läst dessa riktlinjer.

Frågor om säkerhetsmedvetande

Alla utom 2 personer känner till arbetsplatsens regler om vad som gäller när man lämnar datorn obevakad och samma antal (47 stycken) anser att man alltid bör logga ut när man lämnar datorn obevakad.

En majoritet byter lösenord varannan månad och medelvärdet för antal tecken i lösenordet är 6 stycken. Mer än hälften anser att de känner till hur man bör utforma ett korrekt lösenord. 47 personer anser att man inte bör lämna ut sitt lösenord till en kollega. Den som svarat Ja på den frågan anger att han byter lösenord efteråt.

De flesta sitter bredvid om de lånar ut datorn där de är inloggad till en kollega. Endast en av respondenterna har inte tillgång till Internet och majoriteten anser att man inte bör ladda hem program från Internet.

Disketter från hemmet används inte av de flesta, och en del känner till att man bör virus kontrollera disketten innan den placeras i jobbdatorn. Majoriteten vet vad som gäller vid misstanke om brott eller vid upptäckt av virus.

Merparten använder e-post på jobbet och känner även till att det finns regler gällande e-post. Mottagare och systemansvarig är de personalen tror kan läsa e-post som skickas och närmare hälften skickar privata e-postmeddelanden. De flesta har inte öppnat e-post som de inte vetat vem avsändaren varit och 43 stycken anser att allt de gör på datorn kan spåras.

4.6 Intervju

För våran undersökning har vi genomfört en intervju med säkerhetsansvarig för Luleåregionen. Vi ville skaffa lite bakgrund för våran fortsatta undersökning och höra vad en anställd på en högre position med ansvar för säkerheten tycker om deras informationssäkerhetspolicy.

Han berättade att det som gäller policyn sker ofta på koncernnivå och att de har någonting som kallas LIS som är ett ledningssystem för informationssäkerhet.

Beslut om LIS togs juni 2001 att det skulle införas i hela koncernen och det var så att säga det rättsnöret som man följer gällande informationssäkerhet.

Respondenten berättade att hela LIS finns dokumenterat men att det även finns på det interna nätet som riksskatteverkat har. Där kan alla anställda gå in och läsa och vad som gäller.

Respondenten säger att LIS är framarbetad från en internationell standard som är en engelsk förebild i området. Det Riksskatteverket har gjort är att man har tagit denna standard och anpassat den till koncernen. Mycket av det i LIS har bäring på informationssäkerhetsfrågor och yttrar sig till ansvariga i koncernen hur det har ansvar som systemägare och förvaltningsansvarig.

På frågan om hur det är med uppdatering svarar respondenten att det är högre upp man har ansvar för att se till att LIS är uppdaterat. RSV LIS ingår i den koncern övergripande ämnesdatabasen och databasskydd som tar upp hela säkerhetskonceptet för RSV koncernen. Men LIS är som sagt ganska nytt och det togs beslut 2001 om införandet och 2002 är det implementerat. De flesta i koncernen har genomgått en utbildning i LIS plus att man har gjort en handlingsplan för informationssäkerhet.

Han berättar vidare att det finns ett utbildningsmaterial och när det gäller handlingsplanen är det en enklare typ av riskanalys. Den innebär man sätter sig helt enkelt ner och ser vilka brister som finns och försöker plocka ut de fyra viktigaste, sen tas det fram ansvariga och skriver ned datum och kör efter det. Riskanalysen kommer årligen att göras för att ha aktuella handlingsplaner En kontinuerlig uppföljning av verksamheten görs och LIS är en integrerad del av verksamheten och kommer att följas upp vid internkontroller.

Vidare berättar han att han tror att RSV koncernen ligger i framkanten då det gäller informationssäkerhet och att han inte känner till något företag med en så fastslagen policy. Han tror även att deras ledningssystem för informationssäkerhet ligger i tiden.

Respondenten berättar att vid framtagandet av LIS var det en projektgrupp där han bland annat var med som arbetade fram LIS. Respondenten var själv med och tog fram utbildningsmaterialet som används i koncernen för att utbilda de anställda.

Respondenten säger att grundstenarna är att informationen är korrekt och fullständig, finns tillgänglig vid behov, är skyddad mot obehörig åtkomst och kan spåras och återskapas. De tre första tog de direkt från den engelska upplagan av standarden de följt och den fjärde har tillkommit.

Vi fick även reda på att grunden till att var bland annat att koncernen blev föremål för en internrevision som var kritisk i vissa avseenden, bland annat hur de hanterat datasystemen och att det dels skett olyckor med läckage av information.

På frågan om de har haft något läckage efter införandet av LIS svarar respondenten att det vet de inte fast i Stockholm hade de en medarbetare som rent brottsligt läckte information. Men det han ville komma fram till var att de kunde ha lappat, lagat och

fixat det med behörigheter osv. men det var att ta ett samlat kardinalgrepp om verksamheten och det var ju det vägvalet de gjorde och det är ju på förekommen anledning.

Vidare sa respondenten att det finns register över programvaror som organisationen har licenser för men att sköts centralt av IT-avdelningen i Stockholm.

En av grundbultarna i systemet är behörighetssystemet som är kopplat till arbetsuppgifterna och vid byte av arbetsuppgifter eller tillfälliga arbetsuppgifter eller byte av anställningsposition ska behörigheten anpassas till situationen. Vidare sa han att allt som körs i koncernens datasystem loggas.

5 Analys

När vi gjort vår analys har vi utgått ifrån våran enkätundersökning. I analysen kommer vi att titta på och analysera de frågor som vi anser är relevanta och mest intressanta för vår fallstudie. En del frågor från vår enkät har inte gått att dra några slutsatser ifrån och dessa frågor har vi därför inte tagit med i detta avsnitt. Exempel på sådana frågor har varit kön, ålder, typ av anställning och anställningsår. Vi har inte kunnat se någon indelning på svaren utifrån dessa olika grupper. Vi ville med dessa grupper se om vi kunde särskilja några tendenser när det gäller medvetandet om informationssäkerhet och hur mycket man kan om policy. Vi har inte funnit att det finns några direkta slutsatser som kan sägas ha att göra med ovanstående grupper.

Eftersom vår forskningsfråga är att undersöka hur informationssäkerhetspolicyn efterlevs i en organisation?" och eftersom vårt syfte är att visa på eventuella brister med informationssäkerhetspolicyn och säkerhetsmedvetenheten hos de anställda, kommer vi att analysera vad de anställda kan om policy och vad de har för säkerhetsmedvetande när det gäller datasäkerhet. Olika element som är intressanta att titta på för att analysera detta kan vara eventuell tidigare utbildning hos den anställde eller dennes intresse för informationssäkerhet.

Av de cirka 100 enkäter som vi lämnade ut fick vi tillbaka 49 stycken. Detta beror på att det var under en tid som riksskatteverket har en tung arbetsbörda och tiden för inlämnandet var begränsad till ett par dagar.

5.1 Analys av enkät

Den anställdes intresse för datorer

Fråga 6. Har du något intresse av datorer?

Mycket intresserad	Intresserad	Lite intresserad	Inte alls intresserad
10%	57%	33%	

Figur 3

En klar majoritet av de anställda på Riksskatteverket är intresserade eller mycket intresserade av datorer. Enligt teorin 2.6, har självstudier betydelse för hur pass mycket den anställde tar till sig gällande informationssäkerhet.

Fråga 8. Hur ofta använder du din dator hemma?

Varje dag	Någon gång i veckan	Någon gång i mån	Nästan aldrig	Aldrig
29%	35%	22%	4%	

Figur 4

Av de tillfrågade är det 29 % som använder datorn varje dag i hemmet. Enligt teorin 2.6, har självstudier betydelse.

Analys angående utbildning

Fråga 9. Tar du på egen hand del av någon information rörande informationssäkerhet?

Ja	Nej
69%	31%

Figur 5

En majoritet säger att de på egen hand tar del av information angående informationssäkerhet. Enligt teorin avsnitt 2.6, är det viktigt att ha en organisation som förmedlar information rörande säkerhet till de anställda.

Fråga 10. Har din yrkesutbildning gett dig någon utbildning/information i informationssäkerhet?

Ja	Nej	Vet ej
57%	38%	5%

Figur 6

57 % av de anställda har i sin yrkesutbildning fått utbildning i informationssäkerhet. Vi har sett en tendens till att dessa personer har ett högre säkerhetsmedvetande än de som inte har denna utbildning.

Fråga 12. Har SKM gett dig utbildning i informationssäkerhet?

Ja	Nej	Vet ej
76%	18%	6%

Figur 7

Här säger 76 % att de fått utbildning i informationssäkerhet och 18 % att de inte har fått det. Att det är så många som inte säger sig fått utbildning är lite märkligt då alla enligt ledningen ska ha fått utbildning i informationssäkerhet. En förklaring kan vara att dessa personer har varit frånvarande vid utbildning men det har vi inte något belägg för.

Fråga 13. Hur ofta får du utbildning i informationssäkerhet?

1 gång i månaden	1 gång per kvartal	1 gång per år	Aldrig	Annat alt.
		24%	24%	52%

Figur 8

Även när det gäller frekvens av utbildning finns det en grupp (24 %) som aldrig säger sig ha fått utbildning i informationssäkerhet.

Fråga 16. Om utbildning inte skett, har du då fått annan information i informationssäkerhet? Tex. Dokument eller broschyr.

Ja	Nej
43%	6%

Figur 9

21 stycken (43 %) säger att de har fått information i annan form än utbildning i informationssäkerhet. Detta kan vara en förklaring till de som i fråga 12 och 13 aldrig säger sig ha fått utbildning.

Fråga 17. Har det skett någon kontroll av vad ni anställa kan rörande informationssäkerhet?

Ja	Nej
4%	96%

Figur 10

Hela 96 % säger att de inte har skett någon kontroll av vad de anställda kan rörande informationssäkerhet. Enligt teorin är detta mindre bra eftersom Riksskatteverket har lagt ner resurser och har en väl utarbetad policy. Det är viktigt att göra en uppföljning för att som om policyn efterlevs. Se teoriavsnittet 2.5.

Analys av frågor rörande policy

Fråga 21. Känner du till om det finns någon IT-säkerhetspolicy på RSV?

Ja	Nej	Vet ej
90%	2%	8%

Figur 11

Nästan samtliga tillfrågade känner till att Riksskatteverket har en IT-säkerhetspolicy. Detta är mycket bra då ett av målen med RSV:s policy är att alla ska känna till den. Även teorin säger att en policy är något som berör samtliga anställda i en organisation och att de bör känna till den. Se teoriavsnitt 2.2.

Fråga 22. Har du läst IT-säkerhetspolicyn eller på annat sätt tagit del av den?

Ja	Nej	Vet ej
76%q	20%	4%

Figur 12

20 % har inte läst IT-säkerhetspolicyn. Det är en något hög siffra då man inte enbart bör känna till att policyn finns utan självklart bör man även veta vad som står i den. Se teoriavsnitt 2.2.1.

Fråga 23. Har du tillgång till något exemplar av IT-säkerhetspolicyn?

Ja	Nej	Vet ej
59%	29%	12%

Figur 13

29 % har inte något exemplar av IT-säkerhetspolicyn och 12 % vet inte om de har det. Detta är sammantaget en för hög siffra, fler borde veta var de har IT-säkerhetspolicyn för att kunna ta fram den och läsa vid oklarheter. Se teoriavsnitt 2.2.1.

Fråga 26 Har ni någon ansvarig på din sektion/enhet som ser till att informationssäkerhetspolicyn följs?

Ja	Nej	Vet ej
16%	29%	55%

Figur 14

Bara 16% har någon ansvarig på sin avdelning som ser till att informationssäkerhetspolicyn följs. Enligt Statskontoret (1997) ska man i organisationen ha tagit upp hur ansvaret ska se ut och se till så detta följs. Se teoriavsnitt 2.2.1

Fråga 27. Känner du till om RSV har några riktlinjer som ni ska följa för att kunna uppnå målen i IT-säkerhetspolicyn?

Ja	Nej	Vet ej
43%	10%	47%

Figur 15

Mer än hälften av de tillfrågade känner inte till om det finns några riktlinjer att följa för att kunna uppnå målen i IT-säkerhetspolicyn. Eftersom riktlinjerna är ett viktigt stöd för att uppnå målen bör organisationen se till att fler känner till riktlinjerna, se teoriavsnitt 2.3.

Fråga 28. Har du läst dessa riktlinjer eller på annat sätt tagit del av dem?

Ja	Nej	Vet ej
30%	35%	35%

Figur 16

En klar majoritet (70 %) har inte läst eller vet inte om de läst dessa riktlinjer. Eftersom syftet med riktlinjerna är att upprätthålla den säkerhetsnivå ledningen har bestämt, är det viktigt att medarbetarna inom organisationen har läst riktlinjerna, se teoriavsnitt 2.3.1.

Säkerhetsmedvetande

Fråga 29. Känner du till din arbetsplats regler som gäller när man lämnar sin dator obevakad?

Ja	Nej	Vet ej
96%		4%

Figur 17

De flesta på SKM känner till de regler som finns när det gäller att lämna sin dator obevakad. Se teoriavsnitt 2.3.

Fråga 31. Hur ofta bör du ändra ditt lösenord?

En gång i veck	Varannan veck	En gång i mån	Varannan mån	En gång år
2%	4%	16%	76%	2%

Figur 18

Riksskatteverket har en fastställd tidsperiod då det gäller ändring av lösenord. Där varannan månad mest stämde överens med deras rekommendationer. Tre tredjedelar kände till detta men det är dåligt att de andra inte gör det. Det sköts automatiskt dvs. datorn säger till när lösenordet ska ändras och att de inte då tänker på det speciellt.

Fråga 32. Medelvärde antal tecken: 6

Lösenord på 6 tecken verkar gälla på RSV men i enkäten var det några enskilda svar som ville ha 4:a och vissa upp till 8:a. 6 var dock det som majoriteten svarade. Enligt teorin ska man ha minst 6 tecken i ett lösenord, se teoriavsnitt 2.4.4.

Fråga 33. Känner du till hur ett säkert lösenord bör vara utformat?

Ja	Nej
61%	39%

Figur 19

Inte bra att man inte känner till hur ett lösenord bör vara utformat. Det är enkelt för någon att knäcka ett lösenord om det inte är ordenligt. Användaren ska sätta ett lösenord som är svårt att lista ut för obehörig, se teoriavsnitt 2.4.4. Hela 39 % vet inte hur det ska se ut.

Fråga 34. Är det okej att lämna ut sitt lösenord till en kollega?

Ja	Nej	Ibland
2%	96%	2%

Figur 20

Det är aldrig okej att lämna ut sitt lösenord. Men ibland tycker man nog som anställd att det är nödvändigt. 96 % vet dock att det inte är okej. Ett konto med ett lösenord är en personlig egendom och därför ska en användare aldrig lämna ut sitt lösenord, se teoriavsnitt 2.4.4.

Fråga 35. Ifall du svarat ja på föregående fråga, byter du då lösenord efteråt?

Ja	Nej
2%	

Figur 21

2 % av de som lånar ut sitt lösenord byter användarnamn och det är bra men 2 % gör det inte. Har man då otur kan deras dator bli utnyttjad av någon annan tex. Något olagligt, se teoriavsnitt 2.4.4.

Fråga 38. Är det okej att ladda ner program från Internet?

Ja	Nej	Ibland
4%	86%	10%

Figur 22

Relativt många tror att det är okej att ladda ned program från Internet. 86 % vet dock att det inte är okej. En risk med att ladda ner program från Internet är virusrisken, se teoriavsnitt 2.4.4.

Fråga 39. Har du någon gång använt disketter hemifrån på jobbet?

Ja	Nej
16%	84%

Figur 23

Virusrisk finns med att använda disketter hemifrån. Men hela 16 % svarar att de brukar använda disketter hemifrån. En hade dock skrivit att han viruskontrollerade disketten före. Men det är dock ingen garanti för att den är virusfri. Virusprogram och version spelar stor roll för att inte något virus ska missas. Se teorins avsnitt 2.4.4.

Fråga 40. Om du misstänker brott eller brister gällande din arbetsplats säkerhetsregler vet du då vem du skall vända dig till?

Ja	Nej
84%	16%

Figur 24

De flesta vet till vem de ska vända sig. 16% vet dock inte vem man ska vända sig till vid bekymmer. Enligt teorin ska det finnas personer med ansvar för informationssäkerheten och alla bör känna till vilka dessa personer är. Se teoriavsnitt 2.2.2.

Fråga 41. Har du fått information om vad du skall göra vid upptäckt av virus på din dator?

Ja	Nej	Vet ej
90%	2%	8%

Figur 25

9 av 10 vet vad de ska göra om de får virus. Det är viktigt att så fort som möjligt få reda på virus som kommit in i systemet för att minska skadorna och därför är det av stor betydelse att användaren vet hur han ska agera och vem han ska vända sig till. Se teoriavsnitt 2.2.2.

Fråga 43. Känner du till om det finns några regler gällande e-post?

Ja	Nej
86%	14%

Figur 26

Många känner till reglerna, närmare bestämt 86 %. De övriga måste man se till att informera. Det är viktigt att kunna regler gällande e-post då virusrisken är stor gällande e-post. Se teoriavsnitt 2.4.4.

Fråga 45. Brukar du använda e-posten för att skicka/ta emot privata meddelanden?

Ja	Nej
47%	53%

Figur 27

Detta står klart och tydligt i policyn att e-posten ska användas för att skicka meddelanden gällande jobbet och inga privata meddelanden ska skickas. Nästan hälften brukar ändå skicka privata meddelanden. Det innebär att många av de som känner till reglerna inte bryr sig om dem. Se teoriavsnitt 2.4.4.

Fråga 46. Har du någon gång öppnat e-post när du varit osäker vem avsändaren var?

Ja	Nej
27%	73%

Figur 28

Det står klart och tydligt i policyn att man inte ska öppna okänd e-post. Virusrisken är stor, se teoriavsnitt 2.4.4. Nästan en tredjedel bryter mot dessa regler.

Fråga 47. Hur mycket loggas (kan spåras) av det som du gör på datorn?

Allt	En del	Ingenting	Vet ej
88%	4%		8%

Figur 29

Allt loggas i koncernens system och det är självklart att det loggas i ett system som måste vara säkert. Spårbarhet är ett viktigt krav som ska ställas på ett säkert system, se teoriavsnitt 2.4.3. Om något händer måste det gå att spåra händelsen.

6 Slutsatser och avslutande diskussion

6.1 Slutsats

Syftet i våran rapport var att visa på eventuella brister med informationssäkerhetspolicyn och säkerhetsmedvetenheten hos de anställda.

Det vi kunnat se är att LIS verkar vara ett lyckat projekt, de anställda är säkerhetsmedvetna överlag men bryter mot vissa regler. Vi tycker ändå att de på Riksskatteverket har kommit långt i deras säkerhetstänkande. Fortsätter de bara och ser till att följa upp och uppdatera eftersom förutsättningarna förändras kommer riksskatteverket att ha en hög säkerhet inom organisationen. Det viktiga är att fortsätta utbilda och göra personalen medveten om ansvaret som även finns hos dem.

Riksskatteverket ska inte känna sig nöjd med det som finns utan hela tiden utveckla LIS inom organisationen och i samma takt som organisationens utveckling. Teorin säger att det är viktigt att klart och tydligt visa för personalen vad som gäller redan från början och betydelsen av en hög informationssäkerhet och göra de anställda medvetna om kraven och reglerna som finns. På RSV har man tagit ett krafttag gällande informationssäkerheten och klart och tydligt visat vad ledning vill göra och att det är viktigt med en god säkerhet inom koncernen. Enligt respondenten vid intervjun var det ett vägval man var tvungen att göra för att få ett tillfredställande resultat. Det finns dock några brister som vi ser det och även saker som är bra. Nedan har vi skrivit upp det mest relevanta sakerna, först brister som vi ser det och sen saker som är bra enligt oss.

Det är en femtedel som inte läst informationssäkerhetspolicyn. Det är en något hög siffra då man inte enbart bör känna till att policyn finns utan självklart bör man även veta vad som står i den. Samma sak gäller de som inte vet ifall de har något exemplar av informationssäkerhetspolicyn. Detta är sammantaget en för hög siffra, fler borde veta var de har informationssäkerhetspolicyn för att kunna ta fram den och läsa vid oklarheter.

Bara några få känner till att de har någon ansvarig på sin avdelning som ser till att informationssäkerhetspolicyn följs. Enligt teorin ska man i organisationen ha tagit upp hur ansvaret ska se ut och se till att detta följs.

Mer än hälften av de tillfrågade känner inte till om det finns några riktlinjer att följa för att kunna uppnå målen i informationssäkerhetssäkerhetspolicyn. Eftersom riktlinjerna är ett viktigt stöd för att uppnå målen bör organisationen se till att fler känner till riktlinjerna.

En klar majoritet har inte läst eller vet inte om de läst dessa riktlinjer. Eftersom syftet med riktlinjerna är att upprätthålla den säkerhetsnivå ledningen har bestämt, är det viktigt att medarbetarna inom organisationen har läst riktlinjerna.

Det är inte bra att de anställda inte känner till hur ett lösenord bör vara utformat. Det är enkelt för någon att knäcka ett lösenord om det inte är ordenligt. Användaren ska sätta ett lösenord som är svårt att lista ut för obehörig. Nästan hälften vet inte

hur det ska se ut. Men de verkar förstå att man inte ska ha sitt namn, personnummer eller liknande i alla fall.

Mer än hälften är villiga att låna ut sin dator då de står vid sidan om. Oftast handlar det då om att de behöver hjälp med något tror vi. Att de anställda lånar ut sin dator utan att ha uppsikt över den är inte bra. Precis som att låna ut lösenordet, om de har otur kan datorn användas till olagligheter eller annat som den inte får användas till.

Det står klart och tydligt i policyn att e-posten ska användas för att skicka meddelanden gällande jobbet och inga privata meddelanden ska skickas. Nästan hälften brukar ändå skicka privata meddelanden. Det innebär att många av dem som känner till reglerna inte bryr sig om dem. Det står även klart och tydligt i policyn att man inte ska öppna okänd e-post. Virusrisken är stor. Nästan en tredjedel bryter mot dessa regler.

Hälften tycker att de har fått för lite utbildning gällande informationssäkerheten och detta tycker vi att riksskatteverket behöver göra någonting åt. Det har inte heller skett någon kontroll av vad de anställda kan rörande informationssäkerheten. Men det kan bero på att LIS är så pass nytt att man inte har hunnit med att kolla det än. Det är viktigt att göra en uppföljning för att se som om policyn efterlevs.

Nästan samtliga tillfrågade känner till att Riksskatteverket har en informationssäkerhetspolicy. Detta är mycket bra då ett av målen med RSV:s policy är att alla ska känna till den. Även teorin säger att en policy är något som berör samtliga anställda i en organisation och att de bör känna till den. Även en klar majoritet säger att de på egen hand tar del av information angående informationssäkerhet. Detta anser vi tyder på att Riksskatteverket har en organisation som förmedlar information rörande säkerhet till de anställda.

Riksskatteverket har en fastställd tidsperiod då det gäller ändring av lösenord. Där varannan månad mest stämde överens med deras rekommendationer. Två tredjedelar kände till detta men det är dåligt att de andra inte gör det. Kan tänkas att det sköts automatiskt dvs. att datorn säger till när lösenordet ska ändras och att man inte då tänker på det speciellt.

Det är aldrig okej att lämna ut sitt lösenord. Men ibland tycker man nog som anställd att det är nödvändigt. De flesta känner dock till att det inte är okej. Fast egentligen ska alla veta att det inte är okej. Ett konto med ett lösenord är en personlig egendom och därför ska en användare aldrig lämna ut sitt lösenord.

De anställda vet vad de ska göra om de får virus. Det är viktigt att så fort som möjligt få reda på det för att minska skadorna och därför är det av stor betydelse att användaren vet hur han ska agera och vem han ska vända sig till.

Hälften av de anställda har i sin yrkesutbildning fått utbildning i informationssäkerhet. Vi har sett en tendens till att dessa personer har ett högre säkerhetsmedvetande än de som inte har denna utbildning.

6.2 Ärlighet och kritisk distans

När det gäller ärlighet och kritisk distans finns det ett par punkter som vi tycker är värt att tänka på när man läser denna rapport. När vi har tittat på vad de anställda känner till om sin informationssäkerhetspolicy och vad de har för säkerhetsmedvetande ska man ha klart för sig att det är relativt kort tid mellan implementering och vår undersökning. Denna tid är cirka ett år. Detta kan ha betydelse för resultatet av vår enkätundersökning.

När vi genomförde enkätundersökningen var det cirka hälften av de tillfrågade som svarade på undersökningen. Även detta kan ha betydelse för resultatet av undersökningen. Hade tex den andra halvan som inte svarade på undersökningen svarat, kan resultatet sett annorlunda ut. Att endast hälften av de tillfrågade svarade på enkätundersökningen beror sannolikt på att tiden för inlämnandet var begränsad till ett par dagar och att tiden för denna inlämning låg under en tidsperiod då de anställda hade en stor arbetsbörda i sina respektive arbeten.

6.3 Avslutande diskussion

De anställdas kunskaper kan lätt tas för givna inom det område de arbetar med. Ny teknik införs och nya sätt att utföra de gamla, vilket gör att arbetsgivaren glömmer att utbilda personalen i informationssäkerhet. Samtidigt med ny teknik och nya sätt att utföra arbetsuppgifterna kommer även nya risker och hot.

Organisationen hanterar känslig information och då är det viktigt att den har en informationssäkerhetspolicy med mål för att göra de anställda säkerhetsmedvetna. Anställda inom organisationen kan själva ta del av viljan och de mål som ledningen satt upp och sedan kunna ställa egna krav på att de får utbildning i informationssäkerhet.

Att utbilda användarna och se till att de följer sin informationssäkerhetspolicy ser vi som den kanske viktigaste delen för att få en hög informationssäkerhet. Organisationen har en stark tro till tekniska säkerhetslösningar och tar för givet att användarna själva tar del av och följer de policys och riktlinjer som gäller inom organisationen. Vi menar att organisationens skydd inte är starkare än dess svagaste länk och därför är det väldigt viktigt arbeta efter och uppfylla de krav och mål som finns i informationssäkerhetspolicyn. Följer medarbetarna sin informationssäkerhetspolicy finns det enligt oss bra möjligheter att få en hög informationssäkerhet.

6.4 Förslag till fortsatt forskning

Vi har i denna undersökning fokuserat på hur en informationssäkerhetspolicy efterlevs i en organisation. Informationssäkerhetspolicyn i den organisation vi undersökte var nyligen implementerad och ett förslag till fortsatt forskning är därför att göra om denna undersökning vid ett senare tillfälle.

7 Referenser

Aronsson, Rolf. (1995). *ADB-säkerhet – Grundbok för säker ADB-hantering.* Bokförlaget Kommunlitteratur, Ängelholm.

Bell, J. (2000). *Introduktion till forskningsmetodik*. Lund, Studentlitteratur.

Erikson, Peter. (1998). *Planerad Kommunikation*. Liber AB, Stockholm.

Edwall, T. & Söderbaum, J. (1998). *Informationssäkerhet, en marknads- och omvärldsstudie.* Kungliga Tekniska Högskolan, Stockholm.

Jensen, Stig. (2000). *Datakommunikation.* Liber AB, Stockholm.

Ledell, Göran. (1991). *Gör en informationssäkerhetsstrategi.* DF Förlags AB, Stockholm.

Mitrovic Predrag. (2001). *Handbok i IT-säkerhet,* Pagina Förlags AB, Sundbyberg.

Patel, R. & Tebelius, U. (1987). Grundbok i forskningmetodik. Studentlitteratur, Lund.

Patel, R. (2003). *Forskningsmetodikens grunder: att planera, genomföra och rapportera en undersökning*. Lund, Studentlitteratur.

Patel, R. & Davidsson, B. (1994). Forskningsmetodikens grunder. Studentlitteratur, Lund.

SIG Security. (1998). *Säkerhetsarkitekturer*. Studentlitteratur, Lund.

Silberschatz, A & Galvin, P (1997). *Operating system consepts.* John Wiley & Sons, New York.

Statskontoret. (1997). *Handbok i IT-säkerhet del 1 – Introduktion.* CM Gruppen AB, Stockholm.

Statskontoret. (1997). *Handbok i IT-säkerhet del 2 – Policy, ansvar och organisation.* CM Gruppen AB, Stockholm.

Statskontoret. (1997). *Handbok i IT-säkerhet del 3 – Skyddsåtgärder.* CM Gruppen AB, Stockholm.

Swedish Standards Institute. (2002). *Handbok i informationssäkerhetsarbete.* SIS Förlag AB, Stockholm.

Yin, Robert K. (1994). *Applications of case study research.* Thousand Oaks, CA.

Bilaga A: Enkätundersökning

Bakgrundfrågor

1. ? Man ? Kvinna

2. Din ålder

   ? 16-24 ? 25-35 ? 36-45
   ? 46-55 ? 56-

3. Vad har du för anställning?

   ? Tillsvidare anställning ? Vikarie ? Timanställd

4. Har du chefsbefattning?

   ? Ja ? Nej

5. Anställningstid på organisationen? _____ år.

6. Har du något intresse av datorer?

   ? Mycket intresserad ? Intresserad
   ? Lite intresserad ? Inte alls intresserad

7. Har du någon dator hemma?

   ? Ja ? Nej

8. Hur ofta använder du din dator hemma?

   ? Varje dag ? Någon gång i veckan
   ? Någon gång i månaden ? Nästan aldrig
   ? Aldrig

Utbildningsfrågor

Med informationssäkerhet så menar vi hantering av känslig information i datormiljö, exempelvis personuppgifter eller journaler mm.

9. Tar du på egen hand del av någon information rörande informationssäkerhet?

   ? Ja
   ? Nej
   Om Ja Hur?_____

10. Har din yrkesutbildning gett dig någon utbildning/information i informationssäkerhet?

? Ja ? Nej ? Vet ej

11. Har du deltagit i annan utbildning där informationssäkerhet har ingått? Exempelvis på annan arbetsplats (utanför RSV), annan utbildning eller studiecirkel.

? Ja ? Nej ? Vet ej

12. Har SKM gett dig utbildning i informationssäkerhet?

? Ja ? Nej ? Vet ej

13. Hur ofta får du utbildning i informationssäkerhet?

? 1 gång i månaden ? 1 gång per kvartal
? 1 gång per år ? Aldrig
? Annat alternative (Fyll i)
_____

14. Om du fått någon utbildning gällande informationssäkerhet, beskriv i vilken form denna gavs? Exempelvis kurs, litteratur för självstudier eller webbaserad information.

_____

15. Om du har mottagit någon utbildning ingick det någon skriftlig information av det som du fick lära dig? (Något som du fick behålla)

? Ja ? Nej

16. Om utbildning inte skett, har du då fått annan information i informationssäkerhet? Tex muntligt, dokument eller broschyr.

? Ja ? Nej

17. Har det skett någon kontroll av vad ni anställa kan rörande informationssäkerhet?

? Ja ? Nej

18. Anser du att du behöver mer utbildning i informationssäkerhet?

? Ja ? Nej

19. Hur ofta besöker du RSV:s egen hemsida gällande IT-säkerhet?

? Dagligen ? en gång i veckan
? en gång i månaden ? Aldrig

Frågor om Policy

IT-säkerhetspolicy innebär att organisationen har tagit fram ett dokument som talar om vilka mål man ska uppnå gällande informationssäkerhet.

Riktlinjer är ”regler” organisationen satt upp att följa för att uppnå målen i IT-säkerhetspolicyn.

20. Har du något intresse av informationssäkerhet?

? Mycket intresserad ? Intresserad
? Lite intresserad ? Inte alls intresserad

21. Känner du till om det finns någon IT-säkerhetspolicy på RSV?

? Ja ? Nej ? Vet ej

22. Har du läst IT-säkerhetspolicyn eller på annat sätt tagit del av den?

? Ja ? Nej ? Vet ej

23. Har du tillgång till något exemplar av IT-säkerhetspolicyn?

? Ja ? Nej ? Vet ej

24. Tycker du att IT-säkerhetspolicyn är lätt att förstå och ta till sig?

? Mycket lätt ? Lätt ? Varken Lätt eller Svårt
? Svårt ? Mycket Svårt ? Tveksam, Vet ej, Minns ej

25. Tycker du att din sektions/enhetschef har gjort tillräckligt för att göra dig medveten om att RSV har en IT-säkerhetspolicy?

? Ja ? Nej

26. Har ni någon ansvarig på din sektion/enhet som ser till att informationssäkerhetspolicyn följs?

? Ja ? Nej ? Vet ej

27. Känner du till om RSV har några riktlinjer som ni ska följa för att kunna uppnå målen i IT-säkerhetspolicyn?

? Ja ? Nej ? Vet ej

28. Har du läst dessa riktlinjer eller på annat sätt tagit del av dem?

? Ja ? Nej ? Vet ej

Säkerhetsmedvetande frågor

29. Känner du till din arbetsplats regler som gäller när man lämnar sin dator obevakad?

? Ja ? Nej ? Vet ej

30. Hur ofta bör du logga ut när du lämnar din dator obevakad?

? Alltid ? Ofta ? Sällan ? Aldrig

31. Hur ofta bör du ändra ditt lösenord?

? En gång i veckan ? Varannan vecka ? En gång i månaden
? Varannan månad ? En gång per år

32. Hur många tecken ska ett lösenord minst bestå av?_____ antal tecken

33. Känner du till hur ett säkert lösenord bör vara utformat?

? Ja Ge exempel:_____
? Nej

34. Är det okej att lämna ut sitt lösenord till en kollega?

? Ja ? Nej ? Ibland (t ex vid sjukdom)

35. Ifall du svarat ja på föregående fråga, byter du då lösenord efteråt?

? Ja ? Nej

36. Låter du andra använda en dator som du loggat in på?

? Ja ? Ja, men bara då jag är med
? Ibland ? Nej aldrig

37. Har du tillgång till Internet på jobbet?

? Ja ? Nej

38. Är det okej att ladda ner program från Internet?

? Ja ? Nej ? Ibland

39. Har du någon gång använt disketter hemifrån på jobbet?

? Ja ? Nej

40. Om du misstänker brott eller brister gällande din arbetsplats säkerhetsregler vet du då vem du skall vända dig till?

? Ja ? Nej

Vem?_____

41. Har du fått information om vad du skall göra vid upptäckt av virus på din dator?

? Ja ? Nej ? Vet ej

42. Använder du e-post på jobbet?

? Ja ? Nej

43. Känner du till om det finns några regler gällande e-post?

? Ja ? Nej

44. När du skickar e-post, vem kan läsa den förutom du själv?

? Mottagare
? Mottagare och systemansvarig
? Alla med tillgång till RSV:s datorsystem
? Vet ej

45. Brukar du använda e-posten för att skicka/ta emot privata meddelanden?

? Ja ? Nej

46. Har du någon gång öppnat e-post när du varit osäker vem avsändaren var?

? Ja ? Nej

47. Hur mycket loggas (kan spåras) av det som du gör på datorn?

? Allt ? En del ? Ingenting ? Vet ej

Tack för din medverkan!

Thomas Sandström thosan-0@student.luth.se
Tomas Liikamaa tomlii-0@student.luth.se