LUNDS UNIVERSITET
Ekonomihögskolan

Effektivitet versus Informationssäkerhet

En empirisk studie om hur en informationssäkerhetspolicy påverkar effektivt användande av informationssystem

Kandidatuppsats, 15 högskolepoäng, SYSK01 i informatik

Framlagd: Juni, 2010
Presenterad: Juni, 2010

Författare: Johan Carlsson
Marcus Fornell
Carl Otterheim

Handledare: Anders Svensson
Examinator: Claus Persson, Magnus Wärja

Titel: Effektivitet versus Informationssäkerhet
Författare: Johan Carlsson, Marcus Fornell, Carl Otterheim
Utgivare: Institutionen för informatik
Handledare: Anders Svensson
Examinatorer: Claus Persson, Magnus Wärja
Publiceringsår: 2010
Uppsatstyp: Kandidatuppsats
Språk: Svenska
Nyckelord: Informationssäkerhet, Säkerhetspolicy, Effektivitet, Internet Access, Användarkonto, Tillgång till information

Abstrakt

Organisationer är idag i allt större utsträckning beroende av IS (informationssystem) för att utföra vitala uppgifter. Med den stigande brottsligheten på Internet och krav på säkra IS får informationssäkerhet allt större uppmärksamhet inom organisationer. Informationssäkerhet har länge uppfattats som ett tekniskt problem. Bara på senare tid har informationssäkerhet börjat uppfattas som en komplex interaktion som involverar tekniska, organisatoriska och mänskliga faktorer. För att skapa en effektiv informationssäkerhet i en organisation bör omfattande arbete läggas på att utveckla informationssäkerhetspolicyn. Huvudsyftet med denna studie är att undersöka vilken påverkan informationssäkerhetspolicyn har på användares effektiva användning av IS. För att genomföra studien har intervjuer och enkätformulär används för att samla empirisk data. Intervjuerna genomfördes med personer som har nära kontakt med organisationens informationssäkerhetspolicy. Enkätundersökningen utfördes med användarna av IS i organisationerna. Undersökningen har utförts på två stora organisationer i Öresunds-regionen. Säkerhet är ett känsligt område och därför har båda organisationerna valt att vara anonyma i studien. Slutligen presenteras en modell som tar upp faktorer som bör hanteras i förberedandet, genomförandet och upprätthållandet av en effektiv informationssäkerhet. I litteraturstudien, expertintervjuerna och enkätformulären visas det tydligt att säkerhet, kostnad och funktionalitet påverkar effektiviteten.

Abstract

Organizations today are increasingly dependent on IS (information systems) to perform vital tasks. Dependence of the IS, and the fact that organizations are exposed to an increasing number of threats has given information security increasing attention within the organizations. Information security has long been perceived as a technical problem. Only recently information security begun to be understood as an interaction involving technical, organizational and human factors. To create an effective information security within an organization, extensive work should be put on developing the organizations information security policy. The main purpose of this study is to investigate the impact information security policies have on the IS users effective use of IS. To complete the study interviews with questionnaires was used to gather empirical data. The interviews were conducted with persons who have close contact with the organization's information security policy. The survey has been carried out with users of the IS in the organizations. The audit was conducted in two large organizations in the Øresund Region. Security is a sensitive area and therefore both organizations have chosen to remain anonymous in the study. Finally a model which deals with factors that should be handled in the preparation, implementation and maintenance of effective information security is presented. What's clearly shown in the thesis, literature review, expert interviews and questionnaires is that the safety, cost and functionality affect efficiency.

Vi vill tacka

säkerhetsansvarig och säkerhetsexpert på Företag A för att de ställt upp på en expertintervju samt gett oss tillstånd att utföra enkäter på företaget. Vi vill tacka säkerhetsansvarig på Företag B för att vi fick genomföra expertintervjun samt fick tillåtelse att genomföra stickprovsundersökningen på företaget. Vi vill också tacka alla respondenter på Företag A och Företag B. Slutligen vill vi tacka vår handledare Anders Svensson och alla de personer som fungerat som "beta"-testare av uppsatsen och gett oss feedback.

Utan ert stöd skulle inte uppsatsen varit möjlig att genomföra. Tack!

/ Johan, Marcus och Carl

Innehåll

Tabellförteckning

Ordlista

IS - Informationssystem

ISS - Information Security System

ISO - International Organization for Standardization

IEC - International Electrotechnical Commission

1. INLEDNING

Inledningsvis presenteras bakgrunden till frågeställningen. Problemet presenteras och diskuteras. Syftet och målet med undersökningen presenteras samt de avgränsningar som gjorts för att kunna skapa en så fullvärdig undersökning av det valda problemet som möjligt.

1.1. Bakgrund

Organisationer är idag i allt större utsträckning beroende av IS för att utföra vitala uppgifter (Karyda et al., 2005). Med den stigande brottsligheten på Internet och krav på säkra IS får även informationssäkerhet allt större uppmärksamhet inom organisationer. (Dutta & Roy, 2008)

Informationssäkerhet definieras av Committee on National Security (CNSS) som:

"Protection of information and its critical elements, including the systems hardware that use, store and transmit that information."

För att skydda information och IS måste organisationer implementera verktyg som policy, träning och utbildning, säkerhetsmedvetande och teknik. (Whitman & Mattord, 2009)

Historiskt har informationssäkerhet primärt setts som en tekniskt fråga. Det perspektivet har gjort att organisationer endast fokuserat på tekniska lösningar för att lösa problem i samband med informationssäkerhet (Dutta & Roy, 2008). IS innehåller den information som lagras eller på något sätt används av organisationen, ett socialt system som bildas genom åtgärder och relationer mellan IS-användarna samt procedurerna som styr användarnas åtgärder. Enligt detta perspektiv är det inte bara en teknisk del utan även en social dimension (Karyda et al., 2005). Bara på senare tid har informationssäkerhet börjat uppfattas som en komplex interaktion som involverar tekniska, organisatoriska och mänskliga faktorer. (Dutta & Roy, 2008)

Trots den bästa planeringen och implementeringen är det omöjligt att uppnå en perfekt informationssäkerhet. Informationssäkerhet är inte ett mål, utan en process. IS ska balansera skydd och tillgänglighet. Ett system som tillåter access till vem som helst, var som helst, när som helst skulle utgöra ett hot mot informationens integritet. Ett helt säkert system skulle å andra sidan inte tillåta någon access alls. För att nå en balans, det vill säga att hantera ett IS på ett sätt som både användarna och säkerhetsansvariga kan vara nöjda med, måste säkerheten tillåta rimlig access samtidigt som den skyddar mot hot (Whitman & Mattord, 2009).

1.2. Problemdiskussion och forskningsfråga

Innan en undersökning utförs på hur olika typer av informationssäkerhetspolicys fungerar, är det viktigt att förstå exakt vad en policy är och hur den kan och ska användas. En policy är en plan eller ett tillvägagångssätt som används för att förmedla instruktioner från organisationens ledning till dem som utför uppgifter och fattar beslut. Policyn är organisatoriska lagar som dikterar acceptabla och oacceptabelt beteende i organisationen. (Whitman & Mattord, 2009)

Doherty & Fulford (2005) beskriver 11 komponenter som en informationssäkerhetspolicy bör innefatta.

1. Personal usage of information systems
2. Disclosure of information
3. Physical security of infrastructure and information resources
4. Violations and breaches of security
5. Prevention of viruses and worms
6. User access management
7. Mobile computing
8. Internet access
9. Software development and maintenance
10. Encryption
11. Contingency/continuity planning

Ovan nämnda komponenter kommer att användas som ett verktyg för att dela upp informationssäkerhetspolicyn. Komponenterna har legat till grund för den litteratur som valdes vid genomförandet av undersökningen.

För att kunna skapa en effektiv och väl anpassad informationssäkerhet i en organisation bör en organisation lägga ner ett omfattande arbete på att utveckla sin informationssäkerhetspolicy (Simms, 2009).

Utifrån de 11 komponenter ovan undersöker vi i uppsatsen hur effektiviteten påverkas av implementeringen av dem i verkligheten. Forskningsfrågan har tagits fram genom analys av problemets omvärld och lyder följande:

Hur påverkas det effektiva IS-användandet av de säkerhetsregler som finns i en organisations informationssäkerhetspolicy?

1.3. Syfte

Huvudsyftet med studien är att reda ut hur de säkerhetsregler som finns i informations-säkerhetspolicyn påverkar det effektiva användandet av informationssystem. Vår undersökning och analys går ut på att presentera huruvida säkerhet påverkar effektivitet.

Vi vill således med hjälp av litteraturgranskning samt en empirisk undersökning utreda hur faktorer i säkerhetspolicyn påverkar det effektiva användandet av IS.

1.4. Avgränsningar

Uppsatsen är avgränsad till att undersöka hur de anställda upplever sin situation vid användandet av IS och inte den faktiska begränsningen i verkliga processer. Den empiriska undersökningen kommer alltså inte undersöka informationssystems utformning eller användbarhet.

Avsikten är inte att undersöka vilka enskilda komponenter i informationssäkerhetspolicyn som påverkar effektiviteten, utan att ge en övergripande bild av hur informationssäkerhetspolicyn och dess kringliggande faktorer kan påverka IS-användarnas effektivitet.

2. LITTERATURSTUDIE

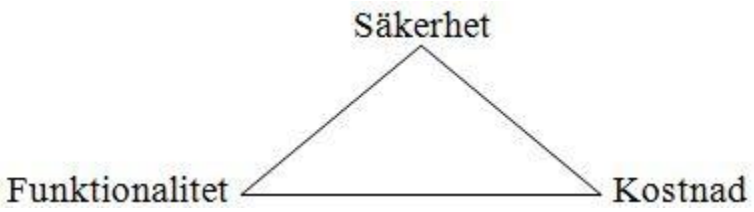
I detta avsnitt presenteras olika teorier. De olika teorierna används för att skapa en referensram som använts för att kunna skapa, genomföra och analysera den empiriska studien.

2.1. Informationssäkerhet

De flesta av dagens organisationer kan inte fungera utan att de har god tillgänglighet till organisationens information. Nyttan av skyddad information är ofta svår att mäta, vilket medför att det är svårt att visa konkret att informationssäkerhet ger någon vinst för företaget. Ur en organisatorisk synpunkt ska en informationssäkerhetslösning vara så kostnadseffektiv och användarvänlig som möjligt, för att generera så mycket vinst som möjligt. (Van Niekerk & Von Solms, 2010)

2.1.1. "The magic triangle of information security"

Ett exempel på organisationers syn på informationssäkerhet kan ritas upp enligt följande modell:



Figur 2.1. *The magic triangle of information security (Oberlaender, 2010)*

En organisation kan inte uppfylla alla aspekter till 100 procent i triangeln utan måste besluta vad som är viktigt och går i enlighet med målen i organisationen. Innan dataintrång blev vanligt diskuterades en endimensionell graf med en lina mellan önskad funktionalitet och nödvändig kostnad för att nå fastställda mål. Säkerhet var nästan aldrig en del av beslutsfattarprocessen. I dagsläget måste en till dimension läggas till i ekvationen, säkerhet. I många, om inte alla fall, är säkerhet motsatsen till funktionell bekvämlighet. Det krävs extra arbete för att tilldela roller och behörigheter, begränsa den breda informationsspridningen, begränsa tillgängligheten till Internet, sätta upp brandväggar, virusprogram med mera. (Oberlaender, 2010)

2.2. Informationssäkerhetspolicys

För att reglera användandet av information och informationssystem gällande informations-säkerhet skapar en organisation en informationssäkerhetspolicy. Det är ett dokument som beskriver de krav och kriterier som måste uppfyllas inom organisationen. Huvudmålet med en informationssäkerhetspolicy är att förhindra obehöriga att få tillgång till, ändra, eller ta bort känslig företagsinformation. Genom att en organisation har en väl fungerande säkerhetspolicy skyddar sig organisationen bland annat mot attacker och att data inte hanteras på ett felaktigt sätt. (Gonzalez & Sawicka, 2002)

För att kunna skapa en effektiv och väl anpassad informationssäkerhet i en organisation bör en organisation lägga ner ett omfattande arbete på att utveckla sin informationssäkerhetspolicy (Simms, 2009). Informationssäkerhetspolicyn ska alltid bli utvärderad av IS användarna så fort det sker några större förändringar eller konfigureringar på informationssystemet. (Karyda et al., 2005)

En kritisk komponent vid framtagandet av en informationssäkerhetspolicy är riskutvärdering. En riskutvärdering bör ske iterativt tillsammans med input från användare som använder olika funktioner i systemet. När riskutvärderingen har blivit fastställd, måste organisationen se till att säkerhetspolicyn tar hänsyn till prestanda och olika användbarhetskrav som finns på organisationens informationssystem. (Simms, 2009)

Karyda et al. (2005) har i sin undersökning om säkerhetspolicys kommit fram till att ett företags organisatoriska struktur spelar en oerhört viktig roll för hur framgångsrikt det ska gå att implementera informationssäkerhetspolicyn. (Karyda et al., 2005)

Karyda et al.s (2005) undersökning av två fallstudier har visat att formuleringen och implementeringen av säkerhetspolicyn oftast bidrar med mer jobb, inte bara för IT-personalen utan det påverkar alla som har någon form av kontakt med informationssystemet och säkerhetspolicyn. Undersökningen visade att en duktig säkerhetsansvarig med personalens förtroende kan ha positiv inverkan vid implementeringen och anpassningen av informations-säkerhetspolicyn. IS-användarna följer vägledningen samt procedurerna i säkerhetspolicyn i större grad om den är uppbyggd ifrån professionella mål och kan effektivisera deras arbete. (Karyda et al., 2005)

En stel och fast hierarkisk organisationsstomme kan påverka informationspolicyn negativt. Det krävs en flexibel organisation om det ska vara möjligt för företaget att anpassa sig till nya roller, men även till de befintliga. (Karyda et al., 2005)

2.2.1. Internetaccess

Internetanvändande ökar allt eftersom fler människor får upp ögonen för fenomenet, vilket skapar problem för organisationer. Internettillgängligheten är en komponent i säkerhetspolicyns grundregler och det krävs oftast strikta regler så personlig Internetanvändning och sökningar på pornografi inte förekommer under arbetstid. (Doherty & Fulford, 2006)

En undersökning presenterad av Websense (2006) visade att ca. 60% av internetanvändandet på arbetstid var för personlig räkning. Det vanligaste Internet användes till var att surfa på pornografiska sidor. Andra aktiviteter som utfördes var exempelvis online-shopping, online-poker och att se prisförändringar på aktier. (Websense, 2006)

En annan företeelse är ”streaming” av musik och filmer. Denna typ av aktivitet kan märkbart påverka en organisations nätverksprestanda. (Sfakiyanudis, 2008)

Brodkin (2008) skriver om hur företag med anställda som har full tillgång till Internet upplever att de förlorar stora resurser genom att de anställdas arbetsutförande minskar. Det påverkar även bandbredden negativt och beskrivs som ett stort problem. De två faktorerna kostar organisationer miljarder dollar varje år. (Brodkin, 2008)

Det privata internetanvändandet ökar tillväxten av "sociala nätverks"-hemsidor vilka med tiden blivit allt mer populära och fått en stor publik världen över. Sociala medier har skapat en debatt inom många organisationer. Det finns många företag som bortser från att sociala medier kan skapa problem för företaget och låter personal använda hemsidorna, medan andra organisationer ser sociala medier som produktivitetsdödare. (Brodkin, 2008)

Internetanvändningen behöver nödvändigtvis inte resultera i någon av de negativa faktorerna ovan. Enligt Arnesen & William (2007) kan tillgången till e-post och Internet bygga upp ett större förtroende mellan de anställda och arbetsgivaren. De menar på att ökat förtroende ökar produktiviteten hos de anställda. Används Internet och e-post på ett felaktigt sätt av anställda i en organisation kan det skapa svåra situationer för både arbetsgivaren såväl som de anställda. Situationer kan uppstå där den/de skyldiga får stå till svars för stämning, förlorad produktivitet och andra problem, till exempel förtal och överföring av värdefull företagsinformation eller affärshemligheter. (Arnesen & William, 2007)

Ett framgångsrikt företag bör tillhandahålla ett reglerat användande av internet och e-post men också tillåta att anställda använder internet och e-post i en rimlig mängd. Detta kan i slutändan vara en fördel för både arbetsgivare och arbetstagare. (Arnesen & William, 2007)

2.2.2. Användarkonto

Det främsta målet med användarkonton är att tillhandahålla ett kontrollerat och säkert användande av nätverkets information. Säkerheten kräver autentisering av användaren samt godkännande av säkerhetspolicyn och den resurs som tillhandahåller användarens virtuella organisation. En virtuell organisation är en organisation som delar resurser för att uppnå ett gemensamt mål. Användarna måste tillåtas använda resurser i den utsträckning som tillåts av roller och policyn, samtidigt som resurserna måste vara säkrade mot avsiktliga såväl som oavsiktliga brott mot policyn. En annan viktig aspekt med användarkonton är att det ger möjligheten till loggning av användarnas aktiviteter. Från användarnas perspektiv anses det viktigt att ha en så kallad ”single sign-on” lösning. (Denemark et al., 2005)

Single sign-on innebär en lösning där användare endast ska behöva autentisera sig en gång för att få full access till de resurser och system som de har behörighet till. (De la Hoz et al., 2009)

Layton (2007) menar att ”user access management” kan delas upp i fyra områden. Varje område har specifika problem och författaren ställer nyckelfrågor kring dessa problem för att få en förståelse för hur användarkonton i organisationen ska fungera.

- Användarregistrering
- Behörighetshantering
- Lösenordshantering
- Granskning av användarnas behörigheter

2.2.2.1. Användarregistrering

Ledningen bör utveckla tydliga rutiner baserade på organisationens policy för hur användare ska läggas till och tas bort från informationssystem och applikationer. Organisationer bör överväga utveckling och implementering av rollbaserade kontosystem baserade på arbetsuppgift. Detta för att minimera den tid och maximera det resursutnyttjandet som behövs för att göra en ordentlig implementering av dessa nyckelfrågor (Layton, 2007). Samtliga nyckelfrågor är översatta av oss.

Nyckelfrågor (Layton, 2007):

- Finns det något tillfälle då unika användarkonton inte är nödvändiga i företagets informationssystem eller applikationer?
- Har organisationen rutiner för registrering och borttagning av användarkonton?
- Hur fastställs varje användarkontos åtkomstgrad?
- Krävs det att användarna skriver under avtal?
- Är personalavdelningen involverad i registrerings- och avregistreringsprocessen? Om ja, hur?
- Delar ledningen ut en skriven sammanställning användarnas behörigheter i organisationens system?

2.2.2.2. Behörighetshantering

När ett giltigt användarkonto skapas för att få tillgång till system för informationsbehandling, bör behörigheter begränsas och kontrolleras i enlighet med gällande policy och riktlinjer. Begreppet behörighet är viktigt för informationssäkerhet, eftersom det är baserat på tillit. (Layton, 2007)

Nyckelfrågor (Layton, 2007):

- Hur kontrollerar organisationen behörigheter för informationssystem och program?
- Vilken typ av uppgifter loggas för att hjälpa till vid tilldelning av behörigheter?
- Hur beviljas behörigheter i organisationen?

2.2.2.3. Lösenordshantering

Lösenords hantering är en viktig del i styrning och hantering av tillgång till information. En formell policy och uppsättning bör tas fram och tillvägagångssätt för lösenords hantering. (Layton (2007)

Nyckelfrågor (Layton, 2007):

1. Vilken typ av hanteringsprocess har organisationen för lösenord?
2. Är användare tvungna att skriva under avtal för att hålla sina lösenord konfidentiella och privat från andra?
3. Måste användaren ändra sitt lösenord i enlighet med företagets policy då ett nytt användarkonto skapas? Om ja, vad har företaget för policy för lösenord?
4. Är det tillåtet med standardlösenord i system eller applikationer i någon av företagets informationsprocess anläggningar? Om ja, under vilka omständigheter?
5. Om en användare blir av med sitt lösenord, vilken typ av validitetskontroll sker innan användaren återfår sitt lösenord?

2.2.2.4. Granskning av användarnas behörigheter

Accessrättigheter bör granskas regelbundet av kvalificerad personal som inte är ansvarig för skapandet av konton. Detta för att försäkra att behörigheterna går i linje med användarnas roller och ansvarsområden. (Layton, 2007)

Nyckelfrågor (Layton, 2007):

- Hur frekvent granskas användarnas behörigheter?
- Används en tidigare process eller metod för att granska användarnas behörigheter? Om ja, utveckla.
- Granskas konton med högre behörigheter oftare?

- Hur ser tillvägagångssättet ut vid modifiering av användarkonton med högre behörigheter och finns ändringarna att tillgå i någon logg?

2.2.3. Tillgång till information

Ett av de viktigaste områdena att hantera när man tittar på riskreducerande strategier för att bekämpa social engineering (se avsnitt 2.6.1) är skyddandet av kritisk information. Det är viktigt att en organisation identifierar vilken information som är kritisk för organisationen. Dessutom bör ett företag försöka identifiera den information som kan skada organisationen om den offentliggörs. När den kritiska informationen har identifierats kan den integreras i organisationens utbildningsplaner för att säkerställa att de anställda förstår vilken information de måste skydda. Informationschefer bör ha en djup förståelse för informationssystemets arkitektur, kunskap om var känslig information lagras i systemet och hur den överförs eller överlämnas. (Applegate, 2009)

En annan metod som organisationer bör implementera för att skydda viktig/kritisk information är att minimera tillgången till den. Tillgång till viktig information eller information som är potentiellt skadlig för en organisation bör begränsas till dem som verkligen har ett behov av informationen. (Applegate, 2009)

Till exempel kan en person som arbetar på marknadsföringsavdelningen i en organisation ha behörighet att se känslig information, men om de inte har ett tydligt behov av att se känslig information bör de inte ha fri tillgång till den. Förutom att kontrollera åtkomst till kritisk information, är det viktigt att en organisation kontrollerar klassificeringen av viktig information, både internt i organisationen och i det offentliga rummet. Innan uppgifterna lämnas ut till allmän egendom bör de utvärderas av säkerhetspersonal. (Applegate, 2009)

Större organisationer som är fysiskt belägna på olika platser vill ofta fungera som en helhet gällande kunskapsspridning. Det innebär att delning av information inom organisationen ska ske som om organisationen endast var belägen på en plats. För att större organisationer ska kunna fungera som en helhet har de ofta öppna interna system vilket medför en ökad säkerhetsrisk. (Kamel et al., 2007)

En organisation bör utformas för att underlätta både det vertikala och horisontella informationsflödet som behövs för att förverkliga organisationens övergripande mål. Om strukturen inte passar de krav på information som finns i organisationen kommer de anställda antingen ha för lite information eller lägga tid på att bearbeta information som inte är viktig för deras uppgift. Vilket i sin tur bidrar till minskad effektivitet. Det finns dock en spänning mellan vertikala och horisontella mekanismer i en organisation. Vertikala kopplingar är designade framförallt för kontroll medan den horisontella kopplingen är designad för koordination och samarbete, vilket vanligtvis betyder minskad kontroll. (Daft, 2008)

2.2.4. Säkerhetsuppdateringar

Datorer blir allt större utsträckning kopplade till nätverk, vilket bara komplicerar hanteringen av problem, med tanke på den myriad av virus och andra attacker som är vanliga i dagens nätverk. Säkerhetsproblem kan ha förödande konsekvenser på en organisations datainfrastruktur. För att förhindra detta släpper programvaruleverantörer ofta uppdateringar som kan tillämpas för att behandla problem med säkerhet och underhåll som har upptäckts. Detta innebär en administrativ mardröm för administratörer som tar hand om stora grupper av datorer. För att dessa uppdateringar ska fungera måste de tillämpas på maskinerna. (Potter & Nieh, 2005)

Det är inte ovanligt att system fortsätts köra med programvara som inte är uppdaterad långt efter en säkerhetsbrist har blivit välkänd (Rescorla, 2003)

På vilket sätt olika uppdateringar ska hanteras är en viktig faktor inom informationssäkerhet. Det är viktigt att fastställa hur uppdateringar ska släppas, för att ta hand om sårbarheter och för att på ett effektivt sätt införas i informationssystemen. (Dutta & Roy, 2008)

En programuppdatering avsedd att behandla säkerhets- och underhållsproblem kan resultera i att systemet sätts ur drift. En uppdatering av ett operativsystem kan leda till att hela systemet måste vara nere under en period. Om en systemadministratör väljer att fastställa ett operativsystems säkerhetsproblem omedelbart riskerar han att störa sina användare på grund av förlust av data. Därför måste en systemadministratör i samarbete med de anställda schemalägga driftstopp i förväg, vilket lämnar datorerna sårbara tills de repareras. Om operativsystemets uppdatering lyckas kan systemets driftstopp begränsas till bara ett par minuter under omstarten men även då får användarna besvär med förseningar. Detta i och med att de måste starta om program igen och återställa sina sessioner till det tillstånd de var i innan avstängningen. Om uppdateringen inte lyckas kan driftstoppet vara i flera timmar medan problemet diagnostiseras och en lösning hittas. Driftstopp på grund av säkerhetsunderhåll är inte bara störande utan även kostsamt (Potter & Nieh, 2005).

2.3. Ramverk för informationssäkerhetspolicys

Nedan kommer ramverk för hur en informationssäkerhetspolicy kan byggas upp och underhållas att presenteras.

2.3.1. ISO/IEC 27000

ISO arbetar kontinuerligt tillsammans med IEC för att forma en specialiserad standard gällande informationssäkerhet och säkerhetspolicys för hela världen. (ISO/IEC 27000:2009 (E))

Internationella informationssäkerhetssystems standard är känd under namnet ISMS. ISMS är en sammansättning av tio delar med samhörighet på området informationsteknik till säkerhets-metoder. Vid användning av ISMS kan organisationer utveckla och implementera ramverk som

ska hjälpa till att hantera säkerheten och skydda viktig information, t.ex. finansiell information, personuppgifter för anställda och information som företag tilldelats av kunder eller från en tredje part. (ISO/IEC 27000:2009 (E))

Under bilagan till ISO/IEC 27005:2008 presenteras termer som står med relation till informationssäkerhet. Några av de viktiga termerna är:

- Ansvar - Alla enheter ansvarar för sina handlingar och beslut.
- Sekretess - Företagsinformation som inte är eller ska vara tillgänglig för allmänheten.
- Integritet - Företagets integritet försvarar noggrannheten och helheten av tillgångar

2.3.2. PFIRES

De flesta ramverk som finns gällande informationssäkerhetspolicys tar endast upp hur policyn ska tas fram och inte hur policyn ska underhållas. PFIRES är ett ramverk som fokuserar både på hur en informationssäkerhetspolicy kan utvecklas, byggas upp samt hur den ska underhållas. PFIRES ramverk för informationssäkerhetspolicys hjälper även till att skapa en förståelse för hur en säkerhetspolicy påverkar en organisation. (Reese et al., 2003)

Dagens informationssystem är under konstant förändring och kräver därför också en dynamisk säkerhetspolicy som förändras över tiden tillsammans med de nya krav på säkerhet som uppstår. (Reese et al., 2003)

PFIERS ramverk (Reese et al., 2003) består utav ett antal huvudkomponenter som kommer att presenteras nedan.

- Bedömningsfas – Är den fas som organisationen oftast börjar genomföra. Assess phase går ut på att utvärdera de befintliga policys samt att undersöka vilka risker och hot som säkerhetspolicyn bör täcka. (Reese et al., 2003)
- Planeringsfas – Under planeringsfasen tas en plan fram för hur policyn skal utvecklas. Det är viktigt att göra en riskutvärdering för att kunna skapa en säkerhetspolicy som stämmer överens med organisationens strategi samt organisationens övriga policys. (Reese et al., 2003)

- Leveransfas – Denna fas går ut på att implementera den policy som har tagits fram. Vid implementeringen skall olika kontrollinstrument tas fram och implementeras. Dessa kontroller används för att minimera riskerna mot informationssystemet. (Reese et al., 2003)

- Underhållningsfas – Denna fas innefattar den tid som policyn är i bruk. Meningen är att de kontrollinstrument som implementeras skall användas när olika hot och risker uppstår. (Reese et al., 2003)

- Feedback - en komponent som handlar om att användarna av systemet ska ge feedback på hur väl de anser att systemet fungerar. Feedback är viktigt för att säkerställa att de krav som framtagits i de tidigare stegen i PFIRES-processen har uppnåtts. (Reese et al., 2003)

2.4. Förankring av Informationssäkerhetspolicy

Flertalet författare beskriver att det är viktigt att nå ut med budskapet som tas upp i organisationens informationssäkerhetspolicy. Exempelvis så skriver Simms(2009) att tidigare arbete visar på att utbildning och träning i informationssäkerhet är en viktig del i att skapa effektiv säkerhet. Karyda et al. (2005) menar att efter en informationssäkerhetspolicy har implementerats är det viktigt att få ut budskapet till de anställda samt att informations-säkerhetspolicyn ska granskas och utvärderas periodvis vid större förändringar i informations-systemet.

2.4.1. Chefens roll

Ett nytt synsätt på en effektiv informationssäkerhetspolicy är att det numera ligger inom varje enskild chefs ansvarsområde att skapa en effektiv informationssäkerhetspolicy. Tidigare var IT-avdelningen ansvarig. Chefen har en syn på organisationen som inte IT-avdelningen har. (Dutta & Roy, 2008).

Chefens uppgift för att hantera informationssäkerhet går ofta ut på att hitta en bra balans mellan robusta säkerhetsåtgärder och en acceptabel arbetsmiljö för användarna. (Simms, 2009)
Att skapa säkerhetsmedvetenhet och förse de anställda med säkerhetsträning inkluderas vidare i chefens ansvarsområde inom informationssäkerhet. Chefen ska också övervaka informations-säkerhetspolicys och se till att de hålls uppdaterade. (Karyda et al., 2005) .

2.4.2. Utbildning

Ofta vill ledningen för en organisation investera stora resurser i informationssäkerhet, ofta dyra tekniska lösningar, vilket i sin tur kan medföra att de anställdas riskmedvetande minskar. Det är därför viktigt att öka medvetandet gällande de risker som finns vid användandet av organisationens IS. Medvetenheten skapas på effektivast sätt genom olika typer av aktiviteter och utbildningar. (Dutta & Roy, 2008)

Utbildning kan gå ut på att få anställd att förstå vilka konsekvenser deras handlingar kan få, eller att de anställda tränas i att använda informationssystemet på ett effektivt sätt. (Simms, 2009)
Karyda et al. (2005) skriver att organisationer som låter sin personal delta i olika aktiviteter har lättare för att bygga en säkerhetsnivå med hög kvalité och främst en förståelse för informationssäkerheten. Förståelsen bland organisationens anställda bidrar i sin tur till en förbättrad säkerhetskultur (Karyda et al., 2005).

Ligger informationssäkerhetspolicyn i användarnas intresse och de har förståelse av policyn skapas ett större ansvar mot missbruk av policyn. Förtroendet mellan anställda och organisation är en kritisk faktor för att anställda ska vilja följa organisationens policy ansvarsfullt. Arnesen & William (2007) påstår att en policy bör vara skapad för en specifik arbetsplats istället för att den är utvecklad utifrån vad arbetsgivaren anser bör vara otillåtet. Det ska finnas en harmoni mellan anställda och arbetsgivare och en policy ska vara skapad utifrån bådas intressen. (Arnesen & William, 2007)

2.5. Effektivitet

I detta avsnitt presenteras effektivitet ur ett organisatoriskt perspektiv.

2.5.1. "The work system model"

Steven Alter (2006) har komponerat ihop en form av "work system" ramverk. Om informationsflödet och dess relevans skriver Steven Alter (2006) följande:

"Better information leads to better work system results only if the new information helps participants perform work more efficiently or effectively". (Alter, 2006)

Med det menar Alter (2006) att oavsett hur stort informationsflödet är och hur pass relevant det är har det ingen betydande påverkan på effektiviteten. Det krävs någon form av selektion och sortering av information för att användare ska kunna arbeta med den. Ett överflöd påverkar effektiviteten negativt då det är svårare att hantera. Alter (2006) diskuterar också teknologin och att den inte nödvändigtvis behöver påverka hur arbetssättet effektiviserar användare. Alter (2006) skriver att bättre information och bättre teknologi bör leda till bättre resultat om teknologin i sin tur hjälper till att utföra processen mer effektivt. Exempelvis behöver det inte betyda att det hjälper med ny och avancerad teknik om man ska skriva en bok. Det kan finnas samma möjlighet att skriva en bok med en två år gammal dator. (Alter, 2006)

Alter (2006) sammanfattar positiv och negativ effektivitet med åtta komponenter i en matris som han kallar för "Performance indicators for business processes". Performance indicators for business processes består av följande komponenter som även samlas under begreppet "Positiv efficiency":

- activity rate
- output rate
- consistency
- speed
- uptime

Betydelsen av ”efficiency” (verkningsgrad) är tagen från ISO/IEC 27000:2009 Overview and vocabulary. De skriver att ”efficiency” är en term som relateras till management inom informationssäkerhet. ”Efficiency” är relationen mellan det uppnådda resultatet och hur väl resurserna har blivit använda. (ISO/IEC 27000:2009 (E))

De komponenter som tillhör den andra skalan av "Negative efficiency"(Alter, 2006):

- error rate
- rework rate
- vulnerability

Alter har skapat en tabell där alla indikatorer för effektivitet är samlade och där även mätmetoder är inkluderade vid bestämmelse av utförande för affärsprocesser.(Alter, 2006)

Performance indicators	**Typiska Mätmetoder**
Activity rate	• Antal steg utförda / timme • Antal enheter startade / timme
Output rate	• Antal transporter / vecka
Defect rate	• Antal fel / 1000 enheter • Antal fel / dag
Rework rate	• Antal enheter omarbetade / vecka • Andel arbetstid / vecka dedikerat till omarbete
Consistency	• Antal avvikelser / 1000 bearbetade enheter • Antal betydande avvikelser från standarden / vecka
Speed	• Genomsnittlig tid från start till mål (ibland kallat lead time eller cycle time) • Genomsnittlig kostnad av försäljning delat med genomsnittlig kostnad för inventering för en viss period(så kallad lageromsättning)

Efficiency	• Enheter / arbetad eller maskinell timme • Time efficiency: tid tillägnad värdeskapande aktiviteter delat med total leveranstid
Value added	• Antal färdigställda produkter minus den totala kostnaden för ingredienser
Uptime	• Andel tid i drift • Andel tid tillgänglig för drift
Vulnerability	• Antal säkerhetsrelaterade incidenter / månad • Antal kända säkerhetsrelaterade svagheter, vägda mot hur alvarliga svagheterna är.

Tabell 2.1. *Performance indicators (Alter, 2006)*

Indikationerna ovan beskrivs ur ett arbetsprocessperspektiv och "performance indicators" kan vara positiva respektive negativa beroende på mätningarnas resultat. Indikationerna kan påvisa ett negativt och positivt resultat beroende på hur utförandet har genomförts, där olika aspekter av utförande kan interagerar mot varandra. Om en performance indikator är positiv är en annan performance indikator negativ. (Alter, 2006)

2.5.2. ”Self-efficacy”

Bandura & Jourden (1991) tar upp begreppet ”self-efficacy” som innebär människors tro på hur väl de kan utnyttja sina förmågor. Det kan innebära förmågan att mobilisera sin motivation. En användare med en stark self-efficacy är mer trolig att uppmärksamma och analysera och formulera lösningar till de problem de kommer i kontakt med. Användare med lägre self-efficacy har tendens till att oftare fokusera på potentiellt farliga situationer istället för sin arbetsuppgift. En person med hög self-efficacy har ett högre säkerhetsmedvetande än de personer som inte känner samma självsäkerhet vid användande av datorer. Den mänskliga faktorn är betydande när det handlar om verkningsgrad (Bandura & Jourden, 1991). Rheea, Kimb & Ryuc (2009) menar även att användare med högre self-efficacy använder sig oftare av säkerhetsprogram, exempelvis antivirusprogram.

Den mänskliga faktorn påverkar i stor grad self-efficacy. När användare blir utsatta för säkerhetsproblem såsom virus, spyware attacker och/eller offer för internetbedrägeri, sjunker self-efficacy markant. Self-efficacy kan också stärkas hos en användare om de får deltaga på olika utbildningar eller social övertalning. (Rheea H-S, et al., 2009)

2.6. Den mänskliga faktorn

Många av de processer som ingår i informationssäkerhet är beroende av människors beteende. Det förekommer ofta att användare av informationssystem inte förstår hur de ska hantera alla de olika säkerhetsregler som organisationen satt upp. (Van Niekerk & Von Solms, 2010)

Inom området informationssäkerhet blir det allt tydligare att den mänskliga faktorn är en akilleshäl (Gonzalez & Sawicka, 2002). Även Hyeun-Suk et al. (2009) beskriver att informationssäkerhetens svagaste punkt den mänskliga faktorn. Det perspektivet på informationssäkerhet har resulterat i att man i vissa fall inte ens försöker lösa problemet, utan ser det som en flaskhals som inte går att åtgärda (Hyeun-Suk et al., 2009). Problemen med den mänskliga faktorn har genom undersökningar på informationssäkerheten påvisat att Hyeun-Suk et al.s (2009) teorier om att det är den mänskliga faktorn som den svagaste länken stämmer. (Dhillon & Backhouse, 2000; Lee & Kozar, 2005; Straub & Welk, 1998)

Enligt Dutta & Roy (2008) är det först på senare tid som organisationer tar hänsyn till komplexa tekniska, organisatoriska och beteendemässiga faktorer när de granskar sin informationssäkerhet. Tidigare har organisationer endast fokuserat på de tekniska lösningarna och inte tagit hänsyn till de mänskliga faktorerna (Dutta & Roy, 2008). Det är därför viktigt att företagets informationssäkerhetspolicy hanterar den mänskliga faktorn (Van Niekerk & Von Solms, 2010).

Nyare studier visar också på att det är viktigt att skapa en säkerhetskultur i organisationen så att de anställda får ett intresse för informationssäkerheten. En säkerhetskultur i en organisation bidrar också med att skapa en effektiv informationssäkerhet. (Van Niekerk & Von Solms, 2010)

2.6.1. ”Social engineering”

Social engineering är det begrepp inom informationssäkerhet som refererar till de attacker som sker mot den mänskliga faktorn. Social engineering går ut på att försöka ta sig förbi tekniska säkerhetslösningar med utgångspunkt att utnyttja den mänskliga faktorn. Vanliga attacker inom social engineering är Phising, Trojaner, mutor och att uppge sig för att vara någon annan. (Applegate, 2009)

En ”social engineering”-attack kan medföra stora förluster för en organisation. Förutom uppenbara förluster i pengar så kan organisationen förlora sin konkurrensfördel, marknadsandelar och kundförtroende. Social engineering ökar kontinuerligt och det är därför viktigt för organisationer att ta hänsyn till de risker som den mänskliga faktorn och social engineering medför. (Applegate, 2009)

2.6.2. Att skapa hinder mot den mänskliga faktorn

För att minimera riskerna som den mänskliga faktorn bidrar med är det viktigt att organisationer designar sina informationssystem så att de skapar utrymme för att användarnas säkerhets-medvetenhet främjas. Först efter att en organisation klargjort att informationssäkerhets-medvetandet ska främjas kan organisationen specificera arkitekturen av systemet. (Dutta & Roy, 2008)

Även Applegate(2009) beskriver att det viktigaste är att se till att användarna utbildas så att de är medvetna om de risker och angrepp som sker mot informationssystem via människor. Det ska också finnas en grund i organisationens informationssäkerhetspolicy som hanterar hur attacker som sker via människor ska motarbetas. Det är alltså vikigt att tillsammans med tekniska lösningar skapa en strategi för hur den mänskliga faktorn ska hanteras för att skapa en så väl fungerande säkerhet som möjligt. (Applegate, 2009)

2.7 . Studiens Ramverk

För att skapa en bättre överblick över vilka faktorer som påverkat urvalet av intervjuunderlag till expertintervjuerna och enkätfrågor, skapas nedan en sammanställning av den litteratur som granskats.

Tabellen skapades utifrån de principer som gäller vid utformande av ett ”orsak/verkan-diagram”. Enligt van Aken et al.(2007) ska ett orsak/verkan-diagram presentera symtom som skapas av olika orsaker. Vidare har nödvändiga faktorer lagts till för att tabellen skulle vara anpassad efter studien. Nedan förklaras innebörden av de faktorer som valts i tabellen:

- Begrepp/Faktor – Ett begrepp eller en faktor som valts ut från litteraturstudien för att användas under expertintervjuer, enkäter, analys, diskussion och slutsats.
- Risk/Orsak – Den risk eller orsak som begreppet eller faktorn bidrar med.
- Uppgift/Krav – Begreppets/faktorns sammanhang i informationssäkerhet.
- Påverkan på effektivitet – Begreppets/faktorns påverkan på effektivitet.
- Referens – Var informationen är hämtad i litteraturgenomgången.

Tabellen är konstruerad med utgångspunkt att de flesta begrepp och faktorer har en innebörd eller inverkan på ovanstående punkter. Även om det inte går att ange exempelvis risk, uppgift eller påverkan på effektivitet tas begreppet upp då det anses som relevant för undersökningen, men de rutor som inte går att fylla i har lämnats tomma.

Begrepp / Faktor	**Risk / Orsak**	**Uppgift/Krav**	**Påverkan på effektivitet**	**Referens *(Kapitel)***
Ramverk för policy	Fel i utveckling av policy, Fel målgrupp	Skapa en struktur för hur organisationen arbetar med säkerhet	Dåligt utvecklad policy kan medföra minskad säkerhetsmedvetenhet hos IS-användare.	2.2 2.3
ISO -standard	Misslyckad implementering av informations-säkerhetspolicyn.	Grundpelare för utformning av säkerhetspolicyn	ISO-standarden ska vägleda säkerhetsansvariga så att regler kan vara så användarvänliga som möjligt med professionella mål	2.3
PFIRES		Skapa en struktur för att implementera och underhålla säkerhetspolicy	Låta användare ge feedback, bättre anpassad policy.	2.3
Användar-konto	Brott mot policyn, avsiktliga såväl som oavsiktliga.	Tillhandahålla ett kontrollerat och säkert användande av nätverkets resurser.	För lite information eller för mycket information beroende på behörigheter	2.2
Användar-registrering	Förlust av resurser i form av tid och pengar.	Utveckling och implementering av rollbaserade kontosystem	Fastställning av vem som ska ha tillgång till vilken information	2.2
Lösenords-hantering	Dåliga lösenord, information hamnar i fel händer	En formell policy och uppsättning bör tas fram och tillvägagångssätt för lösenords hantering.	Tidskrävande att byta eller hämta nytt lösenord.	2.2
Informationss äkerhet	Stora förluster för organisationer	Skydda företagets information	Avvägning mellan funktionalitet kostnad och säkerhet	2.1
Informations-säkerhets-policy	Dåligt förankrad medför låg säkerhets-medvetenhet hos anställda.	Ska innehålla krav och kriterier för informationssäkerhet som en organisation måste uppfylla		2.2 2.4
”Speed”		Mätverktyg för effektivitet		2.5
”Uptime”		Mätverktyg för effektivitet		2.5

Begrepp / Faktor	**Risk / Orsak**	**Uppgift/Krav**	**Påverkan på effektivitet**	**Referens *(Kapitel)***
Utbildning	Ökat kvalitativt arbetsutförande	Förmedla informationssäkerhetsregler till de anställda	Ökat kvalitativt arbetsutförande	2.4
Användar-behörigheter	Anställd har fel behörigheter.	Begränsa och kontrollera att behörigheter i enlighet med gällande policy och riktlinjer	För lite information eller för mycket information vilket leder till bearbetning av information som inte hör uppgiften till	2.2
Tillgång till information	Överflödig eller undermålig information till användaren.	Anpassa tillgången till information efter strukturen i organisationen	För lite information eller för mycket information vilket leder till bearbetning av information som inte hör uppgiften till	2.2
Uppdateringar	System ur drift, förlust av data. System körs en tid utan säkerhetsuppdateringar	Planera uppdateringar så de effektivt sätt införs i informations-systemen.	Ett system ur drift påverkar effektiviteten direkt negativt, likaså förlust av data.	2.2
Self-efficacy		Stärks via utbildning och aktiviteter.	Hög self-efficacy ger ökad effektivitet	2.5
Social engineering	Obehöriga får tillgång till information / "mänskliga faktorn"	Att anställda är medvetna om riskerna.	Måste hela tiden finnas i åtanke	2.6
Mänskliga faktorn	Förluster i marknadsandelar, ekonomiska resurser, kundförtroende	Att anställda är medvetna om riskerna. System anpassade efter användarna minskar risker.	Minskad effektivitet	2.6
Privat surfande	Virus, påverkar bandbrädd / Sidor ej låsta		Tar bort fokus från det arbete som ska utföras.	2.2
Chefens Roll		skapa säkerhets-medvetande, effektivisera policys	Ökat säkerhetsmedvetande bland anställda, ökad effektivitet i säkerhetsrutiner	2.4

Tabell 2.2. *Studiens Ramverk*

3. METOD

I detta avsnitt presenterar vi de metoder och tillvägagångssätt vi valt att arbeta efter för att genomföra vår undersökning. Vi kommer även att diskutera reliabiliteten av de metoder vi använt och validiteten utav källorna som använts.

3.1. Forskningsstrategi och Metodval

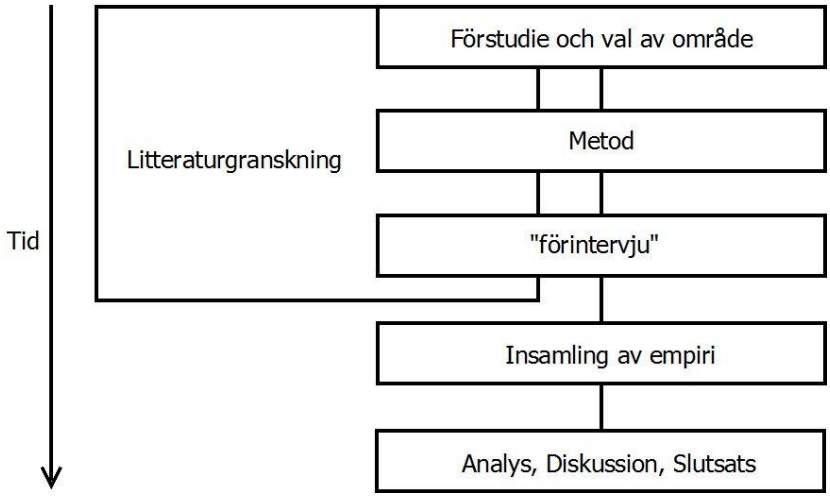
I det tidiga undersökningsarbetet utformades problemställning, syfte och avgränsningar. Att välja problemställning medför en avgränsning av det vi skulle inrikta oss på (Jacobsen, 2002). När området som undersökningen skulle genomföras på valts, effektivitet och informationssäkerhet, började vi att granska litteratur. Litteratur som det fokuserades på i det tidiga undersökningsarbetet var framförallt gällande informationssäkerhetspolicys och effektivitet i allmänhet.

Efter att vi skapat en kunskapsbas utifrån den litteratur som granskats valdes utformningen av hur undersökningen skulle genomföras. När vi skulle välja undersökningsmetod var problemformuleringen fortfarande något oklar och inte särskilt avgränsad. Vårt uppsatsarbete blev således indelat i två delar. Jacobsen (2002) beskriver att problemformuleringen avgör vilken slags undersökningsupplägg som undersökningen bör använda. Då vår problemformulering var oklar valde vi att utgå från en explorativ undersökningsansats. Enligt Jacobsen (2002) handlar ofta en explorativ undersökning om att ta reda på vilka variabler som är relevanta samt vilka värden variablerna kan inta. Första delen i undersökningsmetoden kan ses som en explorativ undersökning.

Efter att problemformuleringen var formulerad påbörjades den andra delen av vår undersökning som gick ut på att införskaffa relevant empiri. Metoden för insamling av empiri valdes utifrån en kvalitativ och kvantitativ ansats. Genom att kombinera en rent kvalitativ metod med en ren kvantitativ metod kan nackdelar begränsas hos varje metod (Jacobsen, 2002).

Expertintervjuer genomfördes på både Företag A och Företag B som tillsammans med den granskade litteraturen resulterade i enkäter som ett stort urval informanter var ämnade att besvara.

På nästa sida presenteras en illustration över hur forskningsstrategin varit upplagd under utförandet av kandidatuppsatsen. I avsnitten som följer kommer olika faktorer och komponenter att presenteras från figuren.



Figur 3.1. *Kandidatarbetets forskningsstrategi*

3.2. Datainsamling

Datainsamling har bestått av litteratur, expertintervjuer och enkäter. I den första explorativa delen av uppsatsarbetet genomfördes en "förintervju" med Företag A, vilken hjälpte till att specificera problemformuleringen ytterligare. Intervjun medförde en ytterligare förståelse för varför informationssäkerhet kan hämma effektivt användande av informationssystem. Förintervjun medförde även att vi kunde granska ytterligare relevant litteratur som kunde ligga till grund för de kommande expertintervjuerna. Förintervjun spelades inte in eller transkriberades då den endast var till grund för expertintervjun. Bilaga 1 innehåller intervjuguiden till förintervjun.

Genom att granska litteratur fick vi också en klarare bild över vilken metod som var bäst för att utföra en undersökning mellan effektivitet och säkerhet. Enligt Gonzalez & Sawicka (2002) är den bästa metoden för att mäta samspelet mellan datorer och människor att utföra empiriska studier. Det finns då två sätt att samla in data till empiriska studier, fältstudier samt experiment med så kallade ”microworlds” (Gonzalez & Sawicka, 2002). Vi valde därför att utföra en fältstudie enligt en akademisk empirisk metod.

Metoden som används vid datainsamling under undersökningen har genomförts med en deduktiv ansats, med en kompletterande induktiv ansats. Den deduktiva ansatsen, som beskrivs av Jacobsen (2002) enligt frasen "från teori till empiri", har varit den huvudsakliga stommen i undersökningen. Teori har i första hand granskats för att skapa en grund till den empiri som samlats in. Motsatsen, induktiv ansats, har som tidigare nämnts använts då problemformuleringen skulle specificeras. Jacobsen (2002) beskriver en induktiv ansats med frasen "från empiri till teori".

3.3. Urval och Informanter

Enligt Jacobsen (2002) är det nästan omöjligt att undersöka alla objekt som är intressanta för den kvalitativa undersökningen. När urval genomförs är det viktigt att ha i åtanke att det alltid är ett utsnitt av a)tema och variabler, b)tid, c)personer och d)händelser (Jacobsen, 2002).

3.3.1 Urval av företag

Undersökningen byggdes upp genom att välja ut två företag för att kunna skapa en jämförelse och analys. Ett krav var att organisationernas belägenhet var i Sverige samt Öresundsregionen. Företagen skulle ha potential att svara på den problemformulering vi valt.

Den första organisationen, Företag A, är en organisation som har försäljning i nästan alla länder i världen. Deras huvudsakliga belägenhet är i Sverige. Den andra organisationen som valts för undersökningen, Företag B, är också en organisation som har försäljning internationellt med belägenhet i Sverige.

3.3.2 Urval av informanter inom företagen

När urval av informanter väljs ska hänsyn tas till den problemställning som valts (Jacobsen, 2002). Urval av informanter inom företagen avser de experter som hade potential att ge oss information om säkerhetens uppbyggnad i organisationen. Det var också viktigt att experterna kunde besvara organisatoriska frågor för att vi skulle kunna få en bredare grund till enkätfrågorna.

De personer som valdes till expertintervjun valdes utefter deras kunskap om organisationen, samt uppbyggnad av organisationens informationssäkerhetspolicy. På Företag A utfördes, som tidigare nämnts, en tidig intervju för att beskriva vårt problemområde samt diskutera hur en eventuell undersökning skulle kunna komma att se ut. Intervjun genomfördes med företagets säkerhetsansvarige för Sverige tillsammans med en säkerhetsexpert på företaget som senare blev vår kontaktperson. På Företag B utfördes en expertintervju med organisationens säkerhets-ansvariga.

3.3.3. Enkätens målgrupp och urval

Enligt Jacobsen(2002) är det viktigt att göra ett brett urval för att kunna få en så stor bredd i de upplysningar som samlas in som möjligt. I båda fallen valdes informanter tillsammans med de säkerhetsansvariga på respektive företag. Det var viktigt att intervjuobjekten kunde besvara frågor om användande av IS och hur det påverkade deras effektivitet. Urval av informanter gjordes tillsammans med de enskilda företagen utefter ett antal kriterier.

1. Individen skulle besitta god generell information om företaget.

2. Individen skulle ha en central roll i företaget med arbetsuppgifter som innehåller användande av informationssystem.

3. Antalet svarande skulle vara runt 50 personer.

Urval av informanter till enkäterna i de två företagen gjordes på två olika sätt. På grund av den korta tid undersökningen utfördes på skickades enkäten på Företag A ut till 150 anställda för att vid 50 svarande stoppas. Urvalet av informanter var slumpmässigt på en avdelning som experterna valde. Urvalet var stort vilket medför att valet av informanter inte i stor utsträckning påverkats för att ge positiva svar för företaget.

Enkäten på Företag B utfördes något senare och blev därför utformad som en stickprovs-undersökning. Enkäten skickades till 15 respondenter med avsikt att stoppas vid 10 svarande. Urvalet gjordes med hjälp av informationssäkerhetsansvarig på Företag B, där specifika personer valdes ut för att få en bredd i urvalet. Jacobsen (2002) skriver att ett slumpmässigt urval inte lämpar sig då ett mindre antal informanter deltar i undersökningen. Således kunde experten på Företag B välja de personer som skulle kunna ge svar som företaget ansåg som positiva för företaget. Dock skiljer sig inte resultaten i undersökningen mellan företag A och Företag B särskilt mycket och urvalen kan därför ses som representativa för både Företag A och Företag B. Då båda företagen var anonyma i undersökningen bör det inte finnas något intresse i att vinkla enkätundersökningen.

3.4. Utformning av Intervjuguiden till expertintervjuerna

Jacobsen (2002) beskriver att en ostrukturerad ansats leder till att insamlade data blir väldigt svåra att analysera. De intervjuer som genomfördes på Företag A och Företag B var väl planerade och hade sin grund i litteraturstudien och det ramverk som presenteras (Tabell 2.2).

Intervjuerna som genomfördes var semistrukturerade. Jacobsen (2002) nämner att en för strukturerad intervju kan ses av vissa som en slutning av datainsamlingen. Även om en klar struktur finns på intervjun går det att upprätthålla en hög grad av öppenhet (Jacobsen, 2002). Under expertintervjuerna ville vi följa de intervjufrågor som strukturerats upp men samtidigt skapa möjlighet för att intervjun var så öppen som möjligt. Framförallt ville vi få ut så mycket information som möjligt gällande informationssäkerhet och effektivt användande av experterna, då de hade många års erfarenhet i branschen.

3.4.1. Frågornas utformning till expertintervjuerna

Frågorna till expertintervjuerna byggdes upp enligt de punkter som Jacobsen (2002) anser som viktiga för att skapa en väl genomförd intervju, tillsammans med förintervju och övrig

litteraturgranskning. Några av de viktiga aspekter som Jacobsen (2002) tar upp för att skapa en bra intervju är följande:

- Börja med en snabb översikt över vad som ska genomföras.
- Inled med allmänna frågor.
- Gå in på djupet.
- Avsluta mjukt.

Frågorna i Intervjuguiden lades i en ordning som skulle medföra att vi följde den ovan nämnda strukturen. Intervjuguiden till förintervjun som genomfördes på Företag A finns under Bilaga1. Intervjuguiden till expertintervjuerna som användes på respektive företag kan ses under Bilaga 2.

Inledningsvis diskuterades frågor gällande organisationens struktur. Vidare gick vi in på djupet i undersökningen och diskuterade frågor som var känsliga, så som frågor gällande informationssäkerhet och informationssäkerhetspolicys. Avslutningsvis diskuterades på vilket sätt enkäterna skulle utformas samt vilka ytterligare oklarheter som fans inför den kommande enkätundersökningen.

3.4.2. Expertintervjuernas genomförande

Vid genomförandet av expertintervjuerna på båda företagen användes ljudupptagning. Det gjordes för att på ett effektivare sätt kunna analysera och diskutera kring resultatet av intervjuerna.

Anteckningar fördes också under intervjun ifall något skulle hända med inspelningsutrustningen. Jacobsen (2002) beskriver också att det är viktigt att föra anteckningar då det kan medföra att intervjuobjekten kan sporras att tala ännu öppnare.

I början på expertintervjuerna diskuterades intervjuguiden och dagordningen presenterades. Under båda intervjuerna följdes den intervjuguide som skapats, men respondenterna tilläts att diskutera kring frågorna vilket medförde att nya frågor uppstod. Genom att kontinuerligt be experterna att utveckla sina svar kunde vi styra så att de frågor som var viktiga för problemställningen blev besvarade. Jacobsen (2002) nämner att det kan vara bra att gräva sig djupare ner i de strukturerade frågorna då det kan ge svar på undersökningens problemställning. Diskussioner kring frågor kan utvecklas genom att ställa frågor så som, hur menar du? Kan du utveckla lite? (Jacobsen, 2002). Metoden att ställa frågor för att fördjupa svaren användes frekvent under expertintervjuerna.

3.5. Enkätundersökningens utformning

Vid utformande av en kvantitativ undersökning måste centrala begrepp preciseras och kategoriseras innan undersökningen genomförs (Jacobsen, 2002).

Enkäten som genomfördes på Företag A kan ses under Bilaga 5. Enkäten som genomfördes på Företag B kan ses under Bilaga 7.

3.5.1. Enkätfrågornas utformning

Enkätfrågorna grundades med hjälp av det ramverk som skapats för studien(Tabell 2.2) tillsammans med de expertintervjuer som genomförts på respektive företag. När kvantitativ data ska samlas in måste begrepp konkretiseras (Jacobsen, 2002). Frågorna i en kvantitativ insamling av data måste också utformas så korrekt som möjligt för att undvika att frågorna ger upphov till oönskade resultat (Jacobsen, 2002). För att skapa frågor till enkäterna där inte tekniska begrepp skulle påverka resultatet fick vi hjälp av experterna på respektive företag för att frågorna inte skulle vara svåra att tolka och besvara.

Frågorna är neutralt utformade för att inte styra informanterna. För att effektivt kunna analysera svaren och arbeta fram statistik till svarsalternativen var frågorna stängda. Målet med den kvantitativa metoden är att samla in systematiserbar information som är standardiserad för att på ett effektivt sätt analysera många enheter (Jacobsen, 2002). Målet med enkätfrågorna var således att de i så liten utsträckning som möjligt skulle vara företagsspecifika. På så sätt skulle det gå att skapa en jämförelse mellan Företag A och Företag B.

Enkätfrågorna skickades till de säkerhetsansvariga för granskning och godkännande innan de skickades ut i respektive företag. Företag B godkände alla frågor, men Företag A ansåg en av de frågor som valts som irrelevant för undersökningen och ville därför inte ta med den i enkäten. Frågan löd:

Sker det ofta automatiska uppdateringar på din arbetsstation under arbetstid (vilket medför att datorn måste startas om o.s.v.)? (Bilaga 7)

Frågan togs därför bort från enkäten som genomfördes på Företag A, men lämnades kvar på enkäten som genomfördes på Företag B, då den litteratur vi granskat visade på att uppdateringar kan vara en stor effektivitetshämmare (Tabell 2.2). Frågan lämnades således också kvar för att vi skulle kunna analysera frågans resultat och relevans.

För att effektivt kunna mäta resultatet på enkäterna strukturerades frågorna upp enligt två strukturer. Den första strukturen vi valde var kategorisvar. Jacobsen (2002) skriver att kategorisvar innebär att uppgiftslämnaren väljer mellan tydliga alternativ. Den andra strukturen

på svar vi valde var rangordnade svar. Rangordnade svar är lämpliga då olika nyanser ska mätas i uppgiftslämnarens svar (Jacobsen, 2002).

- Kategorisvar: Frågor ställdes så att svaren kunde vara ja eller nej.

- Rangordnade svar: Frågor var utformade som påstående med en femgradig skala.

Den femgradiga skalan på de frågor med rangordnade svarsalternativ var först utformad enligt en fyragradig skala för att undvika svar som skulle kunna klassificeras som neutrala. Kontaktpersonen på företag A bad dock om att vi skulle skapa enkäter med femgradig skala. Svarsalternativen blev till slut: Instämmer helt, instämmer till stor del, instämmer till viss del, instämmer lite och instämmer inte alls.

På Företag A var enkätfrågorna på engelska och på Företag B var enkätfrågorna på svenska.
Då vi som författare har goda kunskaper i engelska har vi på bästa sätt hanterat de eventuella betydelseglidningar som skulle kunna förekomma när enkäten inte var på samma språk på Företag A och Företag B. I enstaka fall kan betydelseglidning ha förekommit, dock har det inte haft någon inverkan på resultatet då svaren pekar i samma riktning.

Frågorna förekom också i en något olika ordningsföljd på Företag A och Företag B. Det beror på att enkäten på Företag B utformades några dagar efter enkäten på Företag A. Då vi själva placerade enkäten i ett webbenkät system till Företag B flyttades ett antal frågor för att enkäten skulle få en naturligare struktur. Inte heller i detta fall, när frågor flyttats runt kan en tydlig resultatskillnad återfinnas i enkäten. Ordningsföljden ska alltså inte påverkat resultatet på undersökningen.

3.5.2. Enkätens genomförande

Då några frågor kan vara känsliga att besvara är informanterna till enkäten anonyma och identiteten på informanterna kan inte härledas via svaren på enkäterna. Personligt avstånd till undersökaren ökar känslan av anonymitet och medför ofta att fler och sannare svar produceras (Jacobsen, 2002).

Enkäterna "beta"-testades för att se om det var några frågor som var svåra att förstå. Tiden för genomförandet av enkäten testades också så att enkäten inte skulle ta allt för lång tid att besvara. Genom att testa frågeformuläret kan undersökningen besparas förtretligheten att få in svar som är oanvändbara (Jacobsen, 2002)

Både Företag A och Företag B hade regler för att anställda inte har tillåtelse att svara på enkäter gällande organisationens säkerhet som kommer ifrån annat håll än det egna företaget. Det medförde att enkäterna var tvungna att hanteras enligt de krav som fanns på respektive organisation. Enkäterna genomfördes därför något olika på Företag A och Företag B.

På Företag A skickades enkäterna ut via företagets egna enkätsystem. Enkäterna var tvungna att gå via Företag A:s säkerhetsexpert för att bli godkända och sedan utskickade på avdelningen inom organisationen. Enkäten blev skickade till en stor avdelning där ett stort urval informanter hade möjlighet att svara. Enkäten stoppades då 53 informanter svarat.

När enkäten genomfördes på Företag B utformade vi själva en webbenkät. Ett mindre antal informanter på högre avdelningar valdes ut att besvara enkäterna. Vi skapade enkäterna och skickade en länk till den säkerhetsansvariga på Företag B som sedan skickade ut till informanterna för att vi skulle kunna få svar från ett representativt urval. Slutligen svarade nio informanter på enkäten.

3.6. Bearbetning av data

De två metoder som används för insamling av data har som tidigare nämnts utformats enligt en kvalitativ och kvantitativ ansats. Kvalitativa ansatser ger en mer nyanserad data än vad kvantitativa ansatser ger (Jacobsen, 2002). För att kunna analysera data måste den struktureras upp på något sätt för att ge en överblick (Jacobsen, 2002).

Nedan beskrivs hur de kvantitativa och kvalitativa data som samlats in bearbetats för att kunna presenteras i uppsatsen.

3.6.1. Bearbetning av litteratur

För kunna skapa en grund för undersökningen valdes relevant litteratur ut till de områden som undersökningen avgränsats till. Litteraturen presenteras i en logisk ordning för att förenkla för läsaren. För att skapa överblick över de viktiga begrepp som används i diskussionen och slutsatsen skapades även ett ramverk för studien.

3.6.2. Bearbetning av expertintervjuer

Data som bearbetats gällande expertintervjuerna presenteras på två sätt i uppsatsen.

1) För att bearbeta de kvalitativa data som samlades in under expertintervjuerna transkriberades intervjuerna för att kunna skapa en analys över resultatet. (Jacobsen, 2002) beskriver att en transkribering är ett effektivt sätt att få med all information som en intervju bidrar med. Transkriberingen av expertintervjun till Företag A ligger under Bilaga 3 och transkriberingen av expertintervjun som genomfördes på Företag B ligger under Bilaga 4.

2) En sammanfattning skapades i form av en övergripande tabell som presenteras i empiri avsnittet, med korta och koncisa svar för att ge läsaren en överblick över resultatet på expertintervjuerna.

Det är viktigt att i så stor utsträckning som möjligt återge resultatet i sitt fullständiga sammanhang (Jacobsen, 2002). För att inte resultaten på expertintervjuerna skulle bli lidande transkriberades intervjuerna i sin helhet. Ord och fraser som kunde avslöja företagen ersattes för att behålla anonymiteten. Anonymitet har hanterats genom att alla namn på exempelvis personer, avdelningar m.m. har ersatts med ord så som "Avdelning1" och "Dotterbolag1". Metoden medförde att vi i stor utsträckning kunde återge resultatet av intervjuerna i sitt fullständiga sammanhang.

3.6.3. Bearbetning av enkäter

Bearbetning av data gällande de enkäter som skickats ut har skilts åt mellan Företag A och Företag B. På Företag A sammanställdes enkätsvaren via det interna enkätsystemet. Resultaten granskades sedan av den säkerhetsansvariga och säkerhetsexperten på Företag A. Resultaten skickades sedan till oss i Excelformat. Vi valde att skapa diagram för att få en bättre överblick över resultaten. Enligt Jacobsen (2002), är det vanligaste sättet att presentera svar på en enkät att utforma a) cirkeldiagram och b) stapeldiagram. Cirkeldiagram valdes till de frågor där svarsalternativen var Ja och Nej, och stapeldiagram valdes till frågor med en femgradig skala. Resultat samt sammanställning av diagram för enkätundersökningen på Företag A kan ses under Bilaga 6.

Enkätsvaren från Företag B sparades automatiskt direkt i Google Docs databas. Detta medförde att vi kunde följa utvecklingen. Statistik sammanställdes automatisk i form av diagram och procentenheter för svarsalternativen. Resultaten för enkätundersökningen på Företag B kan ses under bilaga 8.

I Empiri avsnittet presenteras även utdrag samt en sammanställning utav resultatet på enkäterna. Då ordningsföljden på frågorna inte stämde överens mellan enkäterna sammanställdes svaren genom att frågan togs ut från respektive enkät. Resultaten presenteras därefter bredvid varandra. Alla frågor står emot varandra och de frågor som var företagsspecifika är utsatta men har inte ett motsvarigt resultat från det andra företaget.

3.7. Reliabilitet och validitet

För att skapa reliabilitet och validitet har undersökningen utformats utefter en akademisk metod. En metod hjälper till på så sätt att kritiska frågor ställs om de val som görs samt konsekvenserna av dessa val (Jacobsen, 2002).

För att insamlingen av uppsatsens empiriska material skulle hålla så hög kvalitet som möjligt utgick vi efter de krav som Jacobsen (2002) ställer på insamling av empiri. Enligt Jacobsen (2002) måste empiri i en undersökning uppfylla två krav. Den ska vara giltig och relevant, alltså valid. Empirin ska också vara tillförlitlig och trovärdig, alltså reliabel.

För att se till att litteratur som valdes skulle vara valid granskades flertalet artiklar gällande liknande områden. Eftersom IT ständigt utvecklas var ett krav att den litteratur som granskades skulle vara publicerad så nyligen som möjligt. För att öka reliabiliteten valdes också flertalet artiklar ut på samma område för att styrka de teorier som tagits fram.

För att säkra att data som samlades in via expertintervjuerna skulle vara så valida och reliabla som möjligt har expertintervjuerna utförts med personer som är högt uppsatta i respektive organisation gällande informationssäkerhet. Intervjupersonerna var de personer som var mest välinformerade och på bästa sätt skulle kunna svara på de frågor vi valt att utforma till expertintervjuerna.

Informanterna som var ämnade att besvara enkäterna valdes tillsammans med de säkerhetsansvariga. På så sätt ökade också validiteten och reliabiliteten gällande urvalet av informanter. Enkäterna genomfördes som vi tidigare nämnt på två olika sätt på respektive företag. På Företag A skickades enkäten ut via det interna enkätsystemet till personer som skulle kunna ge oss den information vi var ute efter. Det medförde att data som samlades in var reliabel.

Enkäten som utfördes via Google på Företag B var något mer problematisk. Enkätverktyget som användes på Google har två stora brister. 1) Det går inte att lösenorsskydda enkäten 2) det går inte att stänga enkäten på så sätt att en respondent endast kan svara en gång på enkäten. Vi var medvetna om verktygets brister, och skrev således tydligt i den inledande texten på enkäten att vi var tacksamma för att informanterna endast besvarar enkäten en gång. Vi fick också en lista över de informanter som var ämnade att besvara enkäten och kunde på så sätt utläsa om ett orimligt antal svar skulle visa sig i enkätsvaren. På så sätt uppnådde vi den maximala validiteten med det verktyg vi hade tillgång till.

Genom att hela tiden sträva efter att införskaffa så reliabel och valid data som möjligt har en grund lagts för att diskussionen och de slutsatser som presenteras i uppsatsen ska vara så valid och reliabel som möjligt.

3.8. Etiska aspekter

Utöver det som redan nämnts gällande hur etiska aspekter behandlas i undersökningen presenteras i detta avsnitt ett antal etiska aspekter som undersökningen behandlat. Vi arbetade utefter de centrala begrepp som Jacobsen (2002) tar upp gällande etik:

- Informerat samtycke
- Rätt till privatliv
- Krav på riktig presentation av data

Informerat samtycke innebär att de personer som deltog i undersökningen gjorde det frivilligt (Jacobsen, 2002). Vi ställde inga krav på att personer skulle svara på de enkäter som skickades ut. Enkäten skickades till en stor andel informanter för att de informanter som fick enkäten själv skulle kunna avgöra om de ville svara på den eller inte.

Som tidigare nämnts är organisationer, säkerhetsexperter och säkerhetsansvariga samt informanter som svarat på enkäterna anonyma i undersökningen. På Företag A har även sekretessavtal skrivits på av alla tre författare. Då säkerhet är ett känsligt område för ett företag ställde vi inga krav på att de experter vi valt ut skulle svara på frågor som de inte kände sig bekväma att besvara.

Privatliv var inte av intresse för undersökningen. Inga frågor gällande något personligt förekom i undersökningen, varken på expert- eller enkätundersökningen. Faktorer så som kön och ålder har häller inte varit avgörande faktorer för undersökningen och därför har informanterna inte behövt ange några personliga uppgifter.

Jacobsen (2002) skriver att manipulation av data är etiskt förkastligt. Krav har därmed också ställts på att data presenteras och hanteras på ett riktigt sätt. Manipulation av data skulle inte ge någon vinst för företagen eller skribenterna. Enligt Jacobsen (2002) är det svårt att tillgodose alla de ovan nämnda kraven på etik. Undersökningen har i så stor utsträckning som möjligt följt kraven för att kunna skapa en väl fungerande forskningsstrategi.

4. EMPIRI

I detta avsnitt presenteras expertintervjuerna och enkätundersökningarna som genomförts samt deras resultat.

4.1. Undersökningsobjekt

Undersökningen byggdes upp genom att studera två företag för att kunna skapa en jämförelse och analys. Organisationerna är belägna inom Sveriges landsgräns, mer specifikt kring Öresunds-regionen. Båda organisationerna är av global karaktär. För att delta i undersökningen begärde företagen att de skulle vara anonyma.

Den första organisationen, Företag A, är en organisation som har försäljning i nästan alla länder i världen. Deras huvudsakliga belägenhet är i Sverige. Den andra organisationen som valts för undersökningen, Företag B, är också en organisation som har försäljning internationellt med belägenhet i Sverige.

4.2. Expertintervjuns insamling av data

Undersökningen har genomförts i två faser. Det utfördes två expertintervjuer med representanter från båda företagen. Expertintervjuerna och litteraturgranskning grundade strukturen till enkät-formulären som senare skickades ut till utvalda delar för organisationerna.

4.3. Resultatsammanställning av expertintervjuer

Från expertintervjun har de frågor som är intressanta för analysen tagits ut och strukturerats upp. Svaren från respektive företag ställs mot varandra. Frågorna som presenteras gäller företagens organisation, informationssäkerhetspolicy, internettillgång, hantering av användarkonto och information. Alla svarsresultat är utdrag från transkriberingen. Referens till bilaga 3 och 4 presenteras för varje svarsalternativ och fråga.

4.3.1. Organisationen

De frågor som ställdes gällande organisationen skulle vara de inledande frågor på intervjuerna och frambringa en generell uppfattning om hur organisationerna är uppbyggda. Det var meningen att informanterna skulle berätta grundläggande om organisationerna. Företagen gav likartade svarsresultat på de organisatoriska frågorna. Den största skillnaden var hur företagen arbetade med uppdateringar av deras IS gällande säkerhet. Företag B hade strikta regler om att efter ett uppdateringssläpp ska det installeras senast fem dagar efter. Företag A organisation beskrev frågan mer som ett upplysningssvar. Då uppdateringar av säkerhetssystem skulle genomföras, informerade Företag A de anställda via e-post, utbildningar etc.

Fråga	Företag A	Företag B
1. Vilken sorts organisationsstruktur har ert företag?	Hierarkiskt uppbyggd samt matrisorganisation (Bilaga 3, stycke 13)	Matrisorganisation (Bilaga 4 stycke 13)
2. Hur arbetar ni med era anställda vid uppdateringar av säkerhetssystem?	Information via e-post, utbildning, artiklar, interntidningar och via tv-apparater. (Bilaga 3 stycke 27 och 80)	Vi begär att stora uppdateringar ska utföras 5 dagar efter release. (Bilaga 4 stycke 27)
3. Är er säkerhet uppbyggd enligt ISO 27000?	Ja (Bilaga 3, stycke 116)	Ja (Bilaga 4 stycke 21, 23)
4. Är ert ramverk från ISO 27000 modifierat för organisationens behov?	Policyn är uppbyggd och modifierad kring den. (bilaga 3 stycke 120)	Den grundar sig från ISO 27000 men modifieras efter Företag B:s behov. (Bilaga 4 stycke 23)

Tabell 4.1. *Organisatoriska frågor*

4.3.2 Säkerhetspolicy

Frågor knutna till säkerhetspolicyn var mer av ingående karaktär än organisationsfrågorna. Vissa frågor blev endast besvarade av ett företag. Anledningen var att vid genomförandet av intervjuerna, blev de frågorna inte besvarade av båda företagen av olika anledningar. Avsnittet var förberedande för nästkommande frågor kring användarkonto och tillgång av information.

Fråga	Företag A	Företag B
5. På vilket sätt reglerar ni användarkonto i er informationssäkerhetspolicy och kan en användare ha flera användarkonton?	Hur konstruktionen på användarkontot ska vara och vad man får göra med det. Användarkontot får inte lånas ut och lösenordet ska hållas krypterat. (Bilaga 3 stycke 144,147 och 157)	Lösenord får inte vara samma i olika konton. (Bilaga 4 stycke 29)
6. På vilket sätt reglerar ni/hanterar tillgång till information i er informationssäkerhetspolicy?	Inget svar.	Att all inloggning ska utföras i egen behörighet. (Bilaga 4 stycke 51)
7. Vad har ni för metoder för att öka lojaliteten hos anställda och motverka social engineering?	Utbildningar om social engineering. Skriver om det i interntidningen. (Bilaga 3 stycke 192, 217)	Inget svar.

8. På vilket sätt reglerar ni tillgång till internet i er informationssäkerhetspolicy?	Det styrs hur mycket man får surfa privat. (Bilaga 3 stycke 230)	Man skriver på användarföreskrifter vid anställning som säger att man får använda internet till en rimlig mängd. e-post är tillåtet så länge arbetet inte påverkas. (Bilaga 4 stycke 57)
9. På vilket sätt är era informationssäkerhetsansvariga delaktiga i att implementera informationssäkerhetspolicyn?	Genom utbildning och GAP-analys. (Bilaga 3 stycke 240)	Inget svar.
10. Har alla i ert företag tillgång till policydokumentet?	Ja.(Bilaga 3 stycke 127, 263)	Ja. (Bilaga 4 stycke 21)
11. På vilket sätt utbildas de anställda i säkerhetspolicyn? (Gällande tillgång till information, Internetåtkomst och Användarkonto)	Med utbildningar. (Bilaga 3 stycke 230	De utbildas med PowerPoint föreläsningar och lathundar. Samt ett spel. (Bilaga 4 stycke 23)
12. Är det något ni vill tillägga som kan påverka effektivt användande i er säkerhetspolicy?	Det är inte enkelt att nå ut till användarna. Verktyget är utbildning. (Bilaga 3 stycke 127)	Inget svar.

Tabell 4.2. *Frågor gällande säkerhetspolicy*

4.3.3 Användarkonto och tillgång till information

Hantering av användarkonto och information ställdes för att fördjupa undersökningen och få svar som kunde påverka frågeställningen. Expertintervjufrågorna var utvalda så att underlag skulle finnas till utformning av enkätfrågor, där anställda kunde besvara och ge sin synvinkel på området hantering av användarkonto och information.

Fråga	**Företag A**	**Företag B**
13. Vilka är de valda metoderna för inloggning i de olika delarna av informationssystemet?	På arbetsplatsen är det inloggning med lösenord och användarnamn enligt policyn. Hemifrån är det ID Secure. (Bilaga 3 stycke 477, 479, 481, 485, 491och 497)	Inloggning sker med KID - är kopplat med ett användarnamn och lösenord. (Bilaga 4 stycke 29)
14. Hur ofta byts lösenord?	Lösenord byts när man misstänker att en användare har tappat bort det. Annars är det ett system som kräver lösenordbyte en gång i månaden. (Bilaga 3 stycke 501)	KID byts vart annat år. Förutom det finns ett system som kräver byte av lösenord var 90:e dag. (Bilaga 4 stycke 87)

15. Har ni någon single sign-on lösning?	Nej. (Bilaga 3 stycke 450)	Nej. (Bilaga 4 stycke 29)
16. Om en användare glömmer ett lösenord, hur hanteras det?	Då kontaktar användaren IT-bolaget. (Bilaga 3 stycke 515)	Användaren kontaktar servicedesk. Ett tappat KID har en längre väntetid att återfå. (Bilaga 3 stycke 43)
17. Behöver användaren uppge personuppgifter för att återfå sitt lösenord?	Det är en rutinkontroll där användaren identifierar sig. Det ställs olika frågor som berör personen. (Bilaga 3 stycke 517)	Inget svar.
18. Är det en omfattande procedur som tar lång tid?	Nej. (Bilaga 3 stycke 521)	Det är en omfattande process att återfå sitt KID. Lösenord ringer man till servicedesk för att återfår. (Bilaga 4 stycke 33 och 43)
19. Har de anställda tillgång till för lite information?	Nej, om något så har de tillgång till för mycket. Det är det vi vill styra (Bilaga 3 stycke 353)	Inget svar.
20. Hur behandlas dokumenthantering i företaget?	Inget gemensamt dokumenthanteringssystem, det är däremot många användare som vill ha det.(Bilaga 3 stycke 313)	Inget svar.

Tabell 4.3. *Frågor gällande användarkonto och tillgång till information*

4.3.4 Internetaccess

Liksom avsnittet 4.3.3 var det viktigare att svaren hade kvalitet än kvantitet. Allt för att få ett välstrukturerat enkätformulär.

Fråga	Företag A	Företag B
21. Hur tar ni reda på vilka Internetsidor som ska spärras?	Det är inget vi utför. (Bilaga 3 stycke 508)	Inget svar.
22. Hur arbetar ni för att förbättra informationssäkerhetskulturen?	Utbildning med hjälp av broschyrer, tidningar, artiklar etc. (Bilaga 3 stycke 252, 254, 259 och 260)	Med hjälp av PowerPoint, lathundar och ett spel med inriktning på policyn. (Bilaga 4 stycke 23)
23. I vilken omfattning får anställda använda Internet?	De får använda Internet inom en rimlig omfattning. Så länge det inte påverkar arbetet. (Bilaga 3 stycke 516)	Användningen är tillåten både för Internet och för e-post så länge det inte påverkar arbetet. (Bilaga 4 stycke 5)

24. Anser ni att Internet kan användas för att effektivisera anställdas arbete?	Vi förstår om hemsidor kan hjälpa användaren att effektivisera arbetet. Men mycket som inte gör det också. (Bilaga 3 stycke 584)	Vi försöker att policyn om Internet inte ska vara något effektivitetshinder. (Bilaga 4 stycke 115)

Tabell 4.4. *Frågor gällande Internetaccess*

4.3.5. Övriga frågor

Sista avsnittet tar upp övriga frågor som inte gick under en specifik överskrift. Frågorna användes som backup vid intervjuerna om det i slutet på intervjuerna var något som informanterna inte hade svarat på valde vi ut övriga frågor för att förtydliga. Under detta avsnitt är också frågor som företagen själv besvarat under intervjun i den diskussion som fördes.

Fråga	Företag A	Företag B
25. Är det någon speciell del i policyn som ni ser begränsar mest?	Nej. (Bilaga 3 stycke 564)	Det kan det finnas, men det ska inte skapa hinder. (Bilaga 4 stycke 109)
26. Finns potentiella genvägar anställda kan ta för att effektivisera sitt arbete?	Inga specifika. (Bilaga 3 stycke 627)	Ja. (bilaga 4 stycke 111)
27. Anser ni att anställda bör lämna feedback för att förbättra informationssäkerhetspolicy?	Ja. (Bilaga 3 stycke 419)	Ja.(Bilaga 4 stycke 83)
28. Hur är er generella syn på hur effektiviteten är och mäter ni effektiviteten på ett speciellt sätt?	Säkerhetsavdelningen mäter inte effektiviteten. IT-bolaget mäter sin egen effektivitet (nertid, snabbhet vid service etc.)(Bilaga 3 stycke 346, 383)	Effektivitetsmätning sker på IT och på säkerhet. (Bilaga 4 stycke 27)

Tabell 4.5. *Övriga frågor*

4.4. Enkätundersökningen

Enkätundersökningens frågor var utvalda specifikt för att besvara uppsatsens frågeställning. Frågorna grundar sig i litteraturgranskning och från resultatet av expertintervjuerna.

4.4.1. Enkätundersökningens resultat

Alla frågor som presenteras är direkt tagna från enkätundersökningsformulären i bilagorna, och alla frågor kommer i kontinuerlig ordning utifrån original enkätformuläret som skickades in till Företag B. Resultatet från respektive företag presenteras bredvid varandra för att en tydlig jämförelse ska vara möjlig.

De rangordnade svaren presenteras i tre nivåer. Den första nivån presenterar antalet respondenter för att få en överblick för att se om bortfall förekommit. På Företag A var det 53 respondenter som svarade på enkäten och på Företag B var det nio respondenter som svarade på enkäten.

Den andra nivån är frekvens utryckt i procent. På den tredje nivån i tabellen presenteras medelvärdet och standardavvikelsen. Standardavvikelsen är uträknad enligt ”n-1”-metoden (Blom et al., 2005). Standardavvikelse är ett spridningsmått vilket är ett lämpligt verktyg för att visa hur mycket olika kapaciteter skiljer sig åt (Blom et al., 2005). Standardavvikelse och medelvärdet bör visas tillsammans (Jacobsen, 2002).

För att kunna beräkna standardavvikelse gavs varje svarsalternativ ett värde mellan 1-5 enligt följande:

- 5 - Instämmer helt
- 4 - Instämmer till stor del
- 3 - Instämmer till viss del
- 2 - Instämmer lite
- 1 - Instämmer inte alls

De angivna värdena användes vid uträkningarna av medelvärde och standardavvikelse vilka kan ses under Bilaga 9. Under Bilaga 9 kan även de formler som använts för uträkningarna ses. Formlerna är tagna från boken ”Sannolikhetsteori och statistikteori med tillämpningar” av Blom et al. (2005). Vid den standardavvikelse som presenteras nedan innebär noll ingen spridning i resultatet, och en standardavvikelse på strax över två innebär maximal spridning i resultatet.

De kategoriserade svaren presenteras i två nivåer. På den första nivån presenteras antalet svarande och på den andra nivån presenteras frekvensen utryckt i procent.

Fråga 1 – Jag känner till reglerna som gäller mig i företagets informationssäkerhetspolicy.

	Företag A	**Företag B**
Antal svarande	53	9
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Instämmer helt	17	44
Instämmer till stor del	69	56
Instämmer till viss del	13	0
Instämmer lite	2	0
Instämmer inte alls	0	0
Mätvärde		
Medelvärde	4,00	4,44
Standardavvikelse	0,62	0,53

Tabell 4.6. *Enkätfråga 1 (Question1, Bilaga6; Fråga1, Bilaga8)*

Fråga 2 – Känner du att ditt arbete innehåller för många säkerhetsregler, då du ska utföra vissa uppgifter?

	Företag A	**Företag B**
Antal svarande	53	9
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Ja	6	56
Nej	94	44

Tabell 4.7. *Enkätfråga 2 (Question3, Bilaga6; Fråga2, Bilaga8)*

Fråga 3 – Jag anser att min chef har påverkat mitt säkerhetsmedvetande i stor utsträckning.

	Företag A	**Företag B**
Antal svarande	52	9
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Instämmer helt	4	0
Instämmer till stor del	31	22
Instämmer till viss del	28	33
Instämmer lite	25	22
Instämmer inte alls	2	22
Mätvärde		
Medelvärde	3,10	2,56
Standardavvikelse	0,89	1,13

Tabell 4.8. *Enkätfråga 3 (Question2, Bilaga6; Fråga3, Bilaga8)*

Fråga 4 – Har du mer än ett användarkonto? (vid inloggning av olika system och applikationer på företaget)

	Företag A	**Företag B**
Antal svarande	53	9
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Ja	51	56
Nej	49	44

Tabell 4.9. *Enkätfråga 4 (Question19, Bilaga6; Fråga4, Bilaga8)*

Fråga 5 – Jag anser att det är tidskrävande att hantera olika användarkonton.

	Företag A	**Företag B**
Antal svarande	30	9
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Instämmer helt	3	11
Instämmer till stor del	27	0
Instämmer till viss del	47	0
Instämmer lite	23	56
Instämmer inte alls	0	33
Mätvärde		
Medelvärde	3,10	2,00
Standardavvikelse	0,80	1,22

Tabell 4.10. *Enkätfråga 5 (Question20, Bilaga6; Fråga5, Bilaga8)*

Fråga 6 – Jag anser att det är tidskrävande att logga in i de olika systemen.

	Företag A	**Företag B**
Antal svarande	53	9
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Instämmer helt	9	22
Instämmer till stor del	24	0
Instämmer till viss del	40	22
Instämmer lite	26	34
Instämmer inte alls	0	22
Mätvärde		
Medelvärde	3,17	2,67
Standardavvikelse	0,94	1,50

Tabell 4.11. *Enkätfråga 6 (Question4, Bilaga6; Fråga6, Bilaga8)*

Fråga 7 – Jag anser att det är tidskrävande att byta lösenord.

	Företag A	**Företag B**
Antal svarande	53	9
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Instämmer helt	10	11
Instämmer till stor del	26	22
Instämmer till viss del	26	11
Instämmer lite	30	34
Instämmer inte alls	8	22
Mätvärde		
Medelvärde	3,00	2,67
Standardavvikelse	1,13	1,41

Tabell 4.12. *Enkätfråga 7 (Question5, Bilaga6; Fråga7, Bilaga8)*

Fråga 8 – Jag anser att det är tidskrävande att hämta nytt lösenord då jag glömt mitt gamla.

	Företag A	**Företag B**
Antal svarande	51	9
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Instämmer helt	8	11
Instämmer till stor del	17	11
Instämmer till viss del	22	11
Instämmer lite	49	34
Instämmer inte alls	4	34
Mätvärde		
Medelvärde	2,76	2,33
Standardavvikelse	1,05	1,41

Tabell 4.13. *Enkätfråga 8 (Question6, Bilaga6; Fråga8, Bilaga8)*

Fråga 9 – Jag anser att det är tidskrävande att följa säkerhetspolicy vid dokumenthantering.

	Företag A	**Företag B**
Antal svarande	53	9
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Instämmer helt	0	0
Instämmer till stor del	13	0
Instämmer till viss del	32	44
Instämmer lite	47	22
Instämmer inte alls	0	34
Mätvärde		
Medelvärde	2,51	2,11
Standardavvikelse	0,82	0,93

Tabell 4.14. *Enkätfråga 9 (Question7, Bilaga6; Fråga9, Bilaga8)*

Fråga 10 – Jag anser att den utbildning jag fått gällande informationssäkerhet har gjort så att jag på ett effektivare sätt kan utföra mitt arbete.

	Företag A	**Företag B**
Antal svarande	52	9
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Instämmer helt	4	0
Instämmer till stor del	29	11
Instämmer till viss del	27	33
Instämmer lite	36	22
Instämmer inte alls	4	45
Mätvärde		
Medelvärde	2,92	2,11
Standardavvikelse	0,99	1,17

Tabell 4.15. *Enkätfråga 10 (Question8, Bilaga6; Fråga10, Bilaga8)*

Fråga 11 – Har det hänt att du ”hoppat över” regler från säkerhetspolicyn för att effektivisera din arbetsuppgift?

	Företag A	**Företag B**
Antal svarande	53	9
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Ja	32	34
Nej	68	66

Tabell 4.16. *Enkätfråga 11 (Question9, Bilaga6; Fråga11, Bilaga8)*

Fråga 12 – (Om svaret är Ja på fråga 11, besvara fråga 12) Jag går ofta runt säkerhetspolicyn för att effektivisera mina arbetsuppgifter.

	Företag A	**Företag B**
Antal svarande	26	4
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Instämmer helt	0	0
Instämmer till stor del	0	0
Instämmer till viss del	23	0
Instämmer lite	65	50
Instämmer inte alls	1	50
Mätvärde		
Medelvärde	2,12	1,50
Standardavvikelse	0,59	0,59

Tabell 4.17. *Enkätfråga 12 (Question10, Bilaga6; Fråga12, Bilaga8)*

Fråga 13 – Har du någon gång fått påverka förändringar i informationssäkerhetspolicyn?

	Företag A	**Företag B**
Antal svarande	53	9
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Ja	9	22
Nej	91	78

Tabell 4.18. *Enkätfråga 13 (Question11, Bilaga6; Fråga13, Bilaga8)*

Fråga 14 - Anser du att ert arbete skulle effektiviseras om ni hade chans att påverka informationssäkerhetspolicyn?

	Företag A	**Företag B**
Antal svarande	47	9
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Ja	40	78
Nej	60	22

Tabell 4.19. *Enkätfråga 14 (Question12, Bilaga6; Fråga14, Bilaga8)*

Fråga 15 - Använder du Internet sidor som inte är arbetsrelaterade mer än en timme om dagen?

	Företag A	**Företag B**
Antal svarande	53	9
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Ja	8	11
Nej	92	89

Tabell 4.20. *Enkätfråga 15 (Question13, Bilaga6; Fråga15, Bilaga8)*

Fråga 16 - Känner du till hur du bör hantera information med hög säkerhetsklassificering?

	Företag A	**Företag B**
Antal svarande	53	9
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Ja	80	66
Nej	20	34

Tabell 4.21. *Enkätfråga 16 (Question14, Bilaga6; Fråga16, Bilaga8)*

Fråga 17 - (Om svaret är Ja på fråga 16, besvara fråga 17) Jag anser att det är tidskrävande att hantera information med hög säkerhetsklassificering.

	Företag A	**Företag B**
Antal svarande	52	6
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Instämmer helt	4	0
Instämmer till stor del	19	0
Instämmer till viss del	36	33,33
Instämmer lite	38	33,33
Instämmer inte alls	4	33,33
Mätvärde		
Medelvärde	2,81	2,00
Standardavvikelse	0,93	0,89

Tabell 4.22. *Enkätfråga 17 (Question15, Bilaga6; Fråga17, Bilaga8)*

Fråga 18 - Jag anser att jag har tillgång till information som har högre säkerhetsklassificering än vad jag använder.

	Företag A	**Företag B**
Antal svarande	53	9
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Instämmer helt	15	0
Instämmer till stor del	64	0
Instämmer till viss del	11	11
Instämmer lite	8	22
Instämmer inte alls	1	67
Mätvärde		
Medelvärde	2,17	1,44
Standardavvikelse	0,85	0,73

Tabell 4.23. *Enkätfråga 18 (Question16, Bilaga6; Fråga18, Bilaga8)*

Fråga 19 - Jag anser att jag har access till irrelevant information när jag gör sökningar i olika databaser på företaget. (sökningar resulterar i för mycket information som måste granskas för att finna det jag söker)

	Företag A	**Företag B**
Antal svarande	53	9
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Instämmer helt	4	0
Instämmer till stor del	15	0
Instämmer till viss del	34	44
Instämmer lite	41	22
Instämmer inte alls	6	34
Mätvärde		
Medelvärde	2,70	2,11
Standardavvikelse	0,93	0,93

Tabell 4.24. *Enkätfråga 19 (Question17, Bilaga6; Fråga19, Bilaga8)*

Fråga 20 - Sker det ofta automatiska uppdateringar på din arbetsstation under arbetstid (vilket medför att datorn måste startas om o.s.v.)?

	Företag A	**Företag B**
Antal svarande	--	9
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Ja	--	78
Nej	--	28

Tabell 4.25. *Enkätfråga 20 (Fråga20, Bilaga8)*

Fråga 21 - Jag anser att automatiska säkerhetsuppdateringar ofta tar lång tid att genomföra.

	Företag A	**Företag B**
Antal svarande	53	9
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Instämmer helt	9	34
Instämmer till stor del	28	0
Instämmer till viss del	15	55
Instämmer lite	40	11
Instämmer inte alls	0	0
Mätvärde		
Medelvärde	2,92	3,56
Standardavvikelse	1,17	1,13

Tabell 4.26. *Enkätfråga 21 (Question18, Bilaga6; Fråga21, Bilaga8)*

Fråga 22 - Använder du Internet för att effektivisera ditt vardagliga arbete på företaget? (via ex wikis, forum m.m.)?

	Företag A	**Företag B**
Antal svarande	53	9
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Ja	87	34
Nej	13	66

Tabell 4.27. *Enkätfråga 22 (Question21, Bilaga6; Fråga22, Bilaga8)*

Fråga 23 - Jag upplever att säkerheten generellt bromsar mitt effektiva användande av IT-system.

	Företag A	**Företag B**
Antal svarande	50	9
Svarsalternativ	***Frekvens, %***	***Frekvens, %***
Instämmer helt	2	0
Instämmer till stor del	9	34
Instämmer till viss del	32	11
Instämmer lite	57	21
Instämmer inte alls	0	34
Mätvärde		
Medelvärde	2,48	2,44
Standardavvikelse	0,68	1,33

Tabell 4.28. *Enkätfråga 23 (Question22, Bilaga6; Fråga23, Bilaga8)*

5. ANALYS & DISKUSSION

I detta avsnitt diskuteras och analyseras undersökningen och intervjuunderlagen kopplat till det teoretiska ramverket.

Det teoretiska ramverket och det empiriska materialet kommer att analyseras på flera nivåer. Jämförelser och analys kommer att ske mellan:

- Enkätresultat på Företag A och Företag B.
- Expertintervjuer på Företag A och Företag B.
- De enskilda företagens expertintervjuer och undersökningens teoretiska referensram.
- Enkäterna och undersökningens teoretiska referensram.
- Företagsspecifika frågor gällande enkäter.
- Företagsspecifika frågor gällande expertintervjuer.

Vid genomförandet av förintervjun på Företag A fick vi reda på att en av faktorerna som de anställda ansåg som mest effektivitetshämmande gällande informationssäkerhet var uppdateringar av systemen. Frågor kring uppdateringar kom därför till i expertintervjun och enkätundersökningen. Effektivt användande kopplat till uppdateringar presenteras således som ett eget avsnitt nedan.

Då avvikelser från medelvärdet i enkätstudien diskuteras, uppskattar vi själva vad som är stor respektive liten standardavvikelse. Vi utgår från de resultat som presenteras i empiri kapitlet.

I de kommande avsnitten diskuteras de teorier och resultat som tidigare presenterats i uppsatsen. I varje avsnitt analyseras hur respektive teori påverkar det effektiva användandet av ett informationssystem.

5.1. Företagen

Både företag A och Företag B har verksamheter lokaliserade i södra Sverige. Företagen har försäljning av produkter världen över. Under expertintervjuer berättade informanterna om företagens organisationsstruktur. Ett företags organisationsstruktur kan påverka implementeringen av en informationssäkerhetspolicy enligt Karyda et al., (2005). Informanterna på Företag A beskrev sin organisationsstruktur som en matrisorganisation med inslag av hierarkisk organisation. Företag B beskrev sin organisation som en ren matrisorganisation (Tabell 4.1). En stel och fast hierarkisk organisationsstruktur kan ha negativ påverkan på implementeringen av informationssäkerhetspolicyn medan en matrisorganisationsstruktur har positiv effekt, då informationssäkerhetspolicyn ska nå ut till de anställda. Företagens informanter var övertygade om att båda organisationerna var av flexibel karaktär, vilket Karyda et al., (2005) anser vara nödvändigt för att optimalt kunna implementera en informationssäkerhetspolicy.

Chefens roll gällande informationssäkerhet blir allt tydligare. Ett nytt synsätt är att chefen ska ha nära kontakt med slutanvändarna samt vara den person som ser till att en effektiv informationssäkerhetspolicy skapas och efterlevs (Tabell 2.2). Vi valde således att undersöka hur stort antal som ansåg att deras chef på något sätt påverkat deras säkerhetsmedvetande. Ökat säkerhetsmedvetande leder till effektivare användande av informationssäkerheten (Tabell 2.2). På både Företag A och Företag B ansåg majoriteten att chefen på något sätt påverkat deras informationssäkerhetsmedvetande (Tabell 4.8). Chefernas stora betydelse på informationssäkerhetsmedvetandet kan ha medfört en ökad effektivitet på båda företagen, vilket visas genom att ett minde antal respondenter anser att deras effektivitet bromsas av företagets informationssäkerhet (Tabell 4.8).

I båda företagen var informationssäkerheten uppbyggd enligt ISO 27000. Ramverken företagen använder hade ytterligare anpassats efter företagens behov (Tabellen 4.1). När enkätundersökningen byggdes upp behandlades de tre avgränsningsområden som hanteras i ISO/IEC 27000:2009E. De tre termer som fungerade som grundpelare i undersökningen var integritet, ansvar och sekretess.

5.1.1. Informationssäkerhet

Oberlaender (2010) skriver att de tre grundpelarna vid hantering av informationssäkerhet är säkerhet, funktionalitet och kostnad. Det är hela tiden en avvägning vilken eller vilka av faktorerna som blir lidande vid utformandet av en effektiv informationssäkerhet (Tabell 2.2). I de flesta fall är säkerhet motsatsen till funktionell bekvämlighet. Enligt respondenterna är det tydligt att säkerheten på ett eller annat sätt bromsar deras vardagliga arbetsprocesser (Tabell 4.28). Majoriteten av de anställda svarade att säkerheten generellt hindrar dem i deras vardagliga arbete. Det kan bero på att företagen där enkäterna genomfördes satsar mycket på säkerhets- och kostnadsaspekten, vilket gör att funktionaliteten blir lidande.

Vid genomförandet av enkätundersökningen bad vi respondenterna uppge om de kände till de informationssäkerhetsregler som gäller vid deras arbete. Majoriteten anser att de kände till vilka regler som bör följas i deras arbete (Tabell 4.6). Det var ett antal respondenter på Företag A som instämde till viss del att de kände till alla säkerhetsregler. Det var endast ett fåtal personer som inte kände till de exakta regler som gällde deras arbetsprocesser. Resultatet visar att företagen i stor utsträckning lyckats nå ut till de anställda gällande diverse säkerhetsaspekter. Alltså är de metoder som används för utbildning i företagen välutvecklade, vilket även framkom under expertintervjuerna. Detta medför i sin tur att en mer välanpassad informationssäkerhet skapats, där användarna är medvetna om de konsekvenser som deras handlingar medför. De "mänskliga faktorernas" påverkan minimeras även då en organisation har en välutvecklad säkerhetskultur (Van Niekerk & Von Solms, 2010). En god säkerhetskultur leder även till en mer effektiv informationssäkerhet (Van Niekerk & Von Solms, 2010).

På frågan om de anställda ansåg att de hade för många säkerhetsregler då de skulle utföra vissa arbetsuppgifter svarade respondenterna på Företag A och Företag B något olika (Tabell 4.7). På företag A svarade majoriteten att de inte ansåg att det var för många säkerhetsregler. På Företag B svarade drygt hälften av respondenterna att de ansåg att vissa av deras arbetsuppgifter innehöll för många säkerhetsregler. Skillnaden kan bero på det låga antalet respondenter från Företag B samt att undersökningen utförts på olika typer av avdelningar i respektive organisation. Generellt anser inte respondenterna att de har för många säkerhetsregler, problematiken ligger troligtvis i de processer som måste utföras för att hantera informationssäkerheten.

5.2. Informationssäkerhetspolicy

Informationssäkerhetspolicys är det verktyg som används för att hantera informationssäkerhet i en organisation (Gonzalez & Sawicka, 2002). De expertintervjuer vi genomfört visar tydligt att informationssäkerhetspolicyn utgör en central del i företagen.

Det är viktigt att säkerhetspolicyn är väl förankrad bland de anställda för att upprätthålla ett högt säkerhetsmedvetande (Tabell 2.2). Den första frågan på enkäten gällande huruvida respondenterna kände till de regler de bör följa i informationssäkerhetspolicyn svarade en stor andel att de var medvetna om säkerhetsreglerna. Det var endast ett litet antal på Företag A som instämde lite, dock ingen som inte alls instämde på att de kände till informationssäkerhets-reglerna (Tabell 4.6). Det är alltså ett relativt högt säkerhetsmedvetande i båda företagen vilket medför att svaren som presenteras gällande effektivt användande och informationssäkerhet blir trovärdiga. Hade de anställda inte känt till informationssäkerhetspolicyn hade det varit svårt att göra en analys på hur säkerhetsreglerna påverkar deras effektivitet.

Dutta & Roy (2008) beskriver att medvetenhet är effekten av olika aktiviteter som exempelvis utbildningar. Att säkerhetsmedvetandet är så högt kan alltså finna sin grund i att båda företagen har en rad olika aktiviteter och utbildningar för att öka säkerhetsmedvetenhet (Tabell 4.2). För att skapa en effektiv informationssäkerhetspolicy nämner Karyda et al. (2005) att det är viktigt att användare utvärderar informationssäkerhetspolicyn. Simms (2009) nämner vikten av att användare är delaktiga vid framtagandet av en informationssäkerhetspolicy. Ramverket PFIERS (Tabell 2.2) betonar tyngden av att användarna ger feedback under hela informationssäkerhets-policyns livscykel. På enkäten svarade en stor andel av användarna av informationssystemen, på både Företag A och Företag B, att de inte fått påverka förändringar i informationssäkerhets-policyn (Tabell 4.18).

En stor andel användare i båda företagen anser att deras arbete skulle effektiviseras om de fick möjlighet att påverka informationssäkerhetspolicyn. Det var dock en skillnad, då majoriteten på Företag B ansåg att arbetet skulle effektiviseras om de fick påverka informationssäkerhetspolicyn medan majoriteten på Företag A inte ansåg att deras vardagliga arbete skulle effektiviseras (Tabell 4.19). Skillnaden kan bero på att enkäten genomfördes på olika avdelningar inom

organisationen, där de anställda på Företag B jobbar närmare informationssäkerhetspolicyn än de anställda på Företag A.

Vid expertintervjun nämndes att användarna av informationssystemen i respektive företag är delaktiga och lämnar feedback för att förbättra informationssäkerhetspolicyn (Tabell 4.5). Då resultatet påvisar att en stor andel anser att deras arbete skulle effektiviseras om de fick möjlighet att påverka informationssäkerhetspolicyn kan det vara lämpligt för en organisation att se över om den metod som används för att hantera feedback verkligen täcker av alla typer av användare som har kontakt med informationssystemen.

Det är viktigt att utbilda och träna anställda gällande informationssäkerhet för att skapa en effektiv informationssäkerhet (Tabell 2.2). Då de anställda skulle ange om den utbildning de fått gällande informationssäkerhet medfört att de kunnat utföra sina arbetsuppgifter effektivare var det något skilda svar från Företag A och Företag B.

På Företag A instämde majoriteten att den träning de fått mer eller mindre medförde att de kunde utföra sitt vardagliga arbete effektivare. Resultatet kan bero på att Företag A har kontinuerliga utbildningar med de anställda gällande informationssäkerhet (Tabell 4.2).

På Företag B var det avvikelse i resultatet, där en stor andel inte alls instämmer att den utbildning de fått gällande informationssäkerhet medfört att de kunnat utföra sitt arbete effektivare (Tabell 4.15). Utbildning sker också på Företag B (Tabell 4.2). Intressant är dock att de inte i lika stor utsträckning lyckats nå ut till de anställda med faktorer som medför att arbetet kan effektiviseras. Anledningen till skillnaden kan bero på att utbildningarna inte är utformade på samma sätt i Företag A och Företag B. Karyda et al. (2005) menar att efter en informationssäkerhetspolicy har implementerats, är det viktigt att få ut budskapet till de anställda. En andel respondenter på Företag A och Företag B svarade att de inte ansåg att den utbildning de genomgått kring informationssäkerhet har påverkat deras effektivitet positivt (Tabell 4.15). Det kan det bero på att företagen snarare förespråkar säker användning än effektiv användning av informationssystem. Simms (2009) nämner att det är viktigt att få anställda att förstå vilka konsekvenser deras handlingar kan medföra.

Enkätundersökningen visar att de anställda är i behov av att kunna arbeta effektivare, men att olika säkerhetsregler begränsar dem. En tredjedel av de anställda på respektive företag har någon gång hoppat över säkerhetsregler för att kunna effektivisera sitt arbete (Tabell 4.16). Det är en stor andel vilket medför ökade risker att information kommer till skada eller missbrukas inom organisationerna. Enligt det svar respondenterna lämnat på enkätundersökningen, så sker det dock inte särskilt ofta att de anställda bryter mot säkerhetsreglerna (Tabell 4.17). Att användarna hoppat över säkerhetsregler kan i sin tur bero på att de inte i tillräckligt stor utsträckning fått vara med och påverka säkerhetspolicyns regler. Arnesen & William (2007) menar att om informationssäkerhetspolicyn ligger i de anställdas intresse skapas även ett större ansvarstagande mot informationssäkerhetspolicyn.

5.2.1. Användarkonton & tillgång till information

I litteraturen fann vi att det är viktigt att hitta en balansgång mellan skydd av information och tillgång till information. Viktig information eller information som är potentiellt skadlig för organisationen bör begränsas till dem som verkligen har ett behov av informationen. Detta sker med hjälp av bland annat användarkonton. Båda företagen använder sig av användarkonton men varken Företag A eller Företag B använde en single sign-on lösning (Tabell 4.3). På enkät-undersökningen var det däremot nästan hälften av respondenterna som svarade att de endast hade ett användarkonto. Antingen har frågan missuppfattats, eller så har de anställda endast tillgång till ett system, då företagen inte tillhandahåller en single sign-on lösning (Tabell 4.9). Anställda på båda företagen använder sig av minst ett användarkonto och alla användarkonton är individuella (Tabell 4.2). Vidare visade vår enkätundersökning att en stor del anser att det var tidskrävande att hantera olika användarkonton samt lösenord, vilket bekräftar vår litteratur som menar att det bland de anställda anses viktigt med single sign-on (Tabell 4.10 & 4.11).

Denemark et al. (2005) menar att en viktig aspekt vid riskreducerande strategier är att skydda kritisk information. För att skydda information och begränsa den till det den är ämnad åt så klassificerar man information i olika sekretessklasser. En organisation bör minimera tillgången till information, endast till dem som verkligen behöver den. Företag A påtalade även detta i intervjun, där de menar att slutanvändarna snarare har för mycket access än för lite (Tabell 4.3). När enkätundersökningen genomfördes, bekräftades detta än en gång, där en majoritet av Företag A:s informanter ansåg sig ha tillgång till mer information än de behövde (Tabell 4.23). Företag B ansåg sig däremot i en avsevärt mindre utsträckning ha tillgång till mer information än nödvändigt.

Intressant i detta sammanhang var att många på Företag A upplevde att de hade access till irrelevant information då de utförde sökningar i olika databaser på företaget, medan Företag B var mindre benägna att hålla med påståendet. (Tabell 4.24) Det visar att en ökad tillgång till information och ökade accessrättigheter inte nödvändigtvis effektiviserar arbetet, utan i värsta fall kan det ha motsatt effekt.

Kamel et al., (2007) menar att större organisationer som är fysiskt belägna på olika platser ofta vill fungera som en helhet gällande kunskapsspridning. Vidare bör organisationer underlätta både det horisontella och vertikala informationsflödet, för att förverkliga organisationens övergripande mål (Daft, 2008). Om strukturen inte passar de krav på information som finns i organisationen kommer de anställdas effektivitet minska på grund av antingen för lite eller för mycket information. Under expertintervjun visade det sig att Företag A inte använde sig av ett gemensamt dokumenthanteringssystem. Det fanns däremot önskemål från de anställda att implementera ett sådant system, men det ansågs vara för kostsamt i dagsläget (Tabell 4.3). Enkätundersökningarna visade även att en stor andel respondenter från respektive företag anser det tidskrävande att följa säkerhetspolicyn vid dokumenthantering (Tabell 4.14). Majoriteten på både Företag A och Företag B vet hur de ska hantera information med hög säkerhetsklassificering

men det ansågs vara en tidskrävande process (Tabell 4.21 & Tabell 4.22). För att relatera detta till ”The magic triangle of informations security” blir det tydligt att Företag A låter kostnad väga tyngre än funktionalitet, gällande dokumenthantering.

En annan tidskrävande procedur är att byta lösenord samt att hämta nytt, då det förlorats eller glömts. Layton (2007) menar att det bör tas fram en formell policy och en uppsättning tillvägagångssätt för hantering av lösenord. Båda företagen har procedurer som ska följas, men trots att de skiljer sig åt, visade enkätundersökningarna att de i princip uppfattas lika tidskrävande. I enkätundersökningen fann vi även att ett byte av lösenord uppfattades mer tidskrävande än att hämta helt nytt lösenord (Tabell 4.12 & 4.13). Vid intervjun med företagen fick vi uppfattningen att det var en klart mer tidskrävande procedur att hämta ett nytt lösenord än ett rutinmässigt standardbyte (Tabell 4.3). Anledningen till resultaten kan bero på olika faktorer, vi vet exempelvis inte hur många av informanterna som någon gång har förlorat eller glömt sitt lösenord och som då vet hur tidskrävande det är att hämta nytt. Standardbyte av lösenord sker däremot regelbundet för samtlig personal (Tabell 4.3).

5.2.2. Internetaccess

Med ökningen av Internetanvändningen bland anställda som Doherty & Fulford (2006) påpekar, var det intressant att ställa en specifik fråga kring det på enkätformuläret. Frågan var om anställda upplevde att deras arbetsuppgift kunde effektiviseras med Internetanvändning. Majoriteten av de totalt svarande på Företag A ansåg att Internet kunde effektivisera deras arbete. På Företag B svarade en tredjedel att de kunde effektivisera sitt arbete med Internet (Tabell 4.27). Den typen av effektivitet, som de anställda ansåg påverka sitt arbetsutförande positivt, är vad Alter (2006) beskriver som "speed". "Speed" är en ”performance indicator”, där en helhet räknas ut för att få ett medelvärde från start till avslut (Tabell 2.2). Formen av effektiviteten kan räknas då som att anställda med hjälp av exempelvis Wikipedia, kan hitta en lösning snabbare. På så sätt reduceras medelvärdet av tiden från start till avslut. På expertintervjun framkom det även att båda företagens informanter ansåg att Internet är en bra tillgång och att säkerhetsreglerna som berör Internetaccess inte ska vara effektivitetshindrande (Tabell 4.4).

En enkätfråga var på huruvida anställda använde Internet mer än en timme om dagen till icke-jobbrelaterade hemsidor. På båda företagen var det endast ett litet antal som svarade ja (Tabell 4.20). Om resultatet jämförs med vad Websense (2006) skriver, där han menar att 60 % av Internetanvändningen går åt privat surfning, kan vi anta att det inte stämmer in på de företag vi analyserat. Det är dock inte mer än ett antagande, då vi inte vet hur mycket Internet utnyttjas av de anställda. Det är svårt att säga hur stor del av den totala användningen av Internet 60 % är. Under expertintervjun visade det sig att båda företagen tillät de anställda en "rimlig" användning av privat surfande på Internet. (Se tabell 4.4)

Brodkins (2008) skriver inte bara att nätverksprestandan kan påverkas i negativ bemärkelse, men också hur Internetanvändning kan ineffektivisera produktiviteten för anställda vid användning av

de allt mer populära sociala medier så som Facebook och Youtube. Brodkins (2008) undersökning påvisar att anställda som har full tillgänglighet till Internet löpte en större risk att drastiskt minska sitt arbetsutförande. Det kan vara en av anledningarna till varför informanterna på respektive företag enbart tillåter ”rimlig” användning av Internet (se tabell 4.4).

Förutom reducerad effektivitet i form av privat användning av Internet och e-post, kan det även påverka företagskostnader, då bandbredd går åt till fel ändamål. Det kan innebära att viktig information blir lidande när det ska skickas eller tas emot. Ökade kostnader vid internet-användning kan i hög grad bero på framför allt ”streaming” av musik och filmer. Det kan påverka företags nätverksprestanda negativt enligt Sfakiyanudis (2008).

Dock menar Arnesen & William (2007) att ökad acceptans på Internetanvändning kan skapa ett förtroende mellan arbetsgivaren och anställda, och det kan i sin tur leda till ökad produktivitet. Arnesen & William(2007) menar vidare att ett framgångsrikt företag bör tillåta Internetanvändning i en rimlig mängd. Internet- och e-postanvändning bör vara reglerad men fortfarande tillåta en viss mängd användande, och i slutändan kan båda parter, arbetsgivare som anställd, tjäna på att Internetanvändningen styrs under rimliga regler.

5.2.3. Uppdateringar

En uppdatering kan sätta ett helt system ur drift under en period. Då ett system är ur drift påverkas dess uptime och det har då en direkt påverkan på effektiviteten (Tabell 2.2). Dutta & Roy (2008) menar att det är viktigt att fastställa hur uppdateringar ska släppas för att ta hand om sårbarheter och effektivt kunna införa dem i informationssystemen. För att undvika att användarna förlorar data på grund omstart, måste därför säkerhetsuppdateringar schemaläggas i förväg (Tabell 2.2). Både Företag A och Företag B har regler för hur säkerhetsuppdateringar ska införas, dock skiljer de sig åt. På Företag B krävdes det att alla stora uppdateringar skulle implementeras inom fem dagar efter släpp. Företag A gav en annan syn på deras regler, där fokus var att utbilda de anställda som berörs av uppdateringarna genom artiklar, Internet-tidning med mera. (Tabell 4.1)

Respondenterna blev tillfrågade på enkätformuläret om deras uppfattning kring uppdateringar på deras arbetsstationer. En av de två frågorna valdes bort från Företag A:s enkätformulär. Frågan löd: "Sker det ofta automatiska uppdateringar på din arbetsstation under arbetstid (vilket medför att datorn måste startas om o.s.v.)?". Vi ville ändå undersöka om frågan hade någon relevans genom att ställa frågan till Företag B och analysera deras svar. Svarsresultaten visade att en majoritet hade svarat ja på frågan (Tabell 4.25). Då majoriteten svarade ja på Företag B hade det varit intressant att undersöka frågan även på Företag A för att kunna jämföra utfallet. Anledningen att företag A inte valde att ställa frågan kan vara att de anser att uppdateringar är så pass kritiska att de måste utföras direkt på arbetsstationerna och därmed inte kan schemaläggas senare. Vi ville med frågan påvisa att det kan vara nödvändigt att granska vilket sätt det

effektivast införs en uppdatering på datorerna. En rad uppdateringar skulle exempelvis kunna schemaläggas innan de anställda påbörjade sin arbetsdag.

Nästkommande fråga som också gällde uppdateringar ställdes till både Företag A och Företag B. Svaren visade att majoriteten på båda företagen kände att automatiska uppdateringar kunde vara irriterande eller att de tar för lång tid att genomföra (Tabell 4.26).

Potter & Nieh (2005) skriver i sin artikel om hur organisationen som helhet kan påverkas negativt om IS-användarna väljer att inte genomföra uppdateringar på sina arbetsstationer. Det är inte ovanligt att system fortsätts köra med programvara som inte är uppdaterad långt efter en säkerhetsbrist har blivit välkänd (Rescorla, 2003). Det kan kännas som en tvingande process att behöva genomföra en uppdatering. Hyeun-Suk et al. (2009) menar att människan är en av de svagaste länkarna inom informationssäkerhetsområdet. Därför krävs en balansgång mellan kostnad och funktionalitet så att båda parter kan känna förtroende, det är vad "the magic triangle of information security" försöker illustrera.

5.3. Effektivitet

Alter (2006) menar att ett för stort informationsflöde kan påverka effektiviteten negativt. Det är inte först efter det att organisationer genomför någon form av selektion av informationen som det går att behandla den mer effektivt. Ett informationsflöde som inte selekteras, löper större risk att skapa ett negativt fenomen, som innebär att viktig information enbart bearbetas och inte används. I expertintervjun nämnde båda företagen att effektivitetsmätningar utförs inom organisationen (Tabell 4.5). Genom effektivitetsmätningar kan organisationen få reda på vilken information som kan selekteras bort för att de anställda ska kunna arbeta effektivare. De anställda anser att de har tillgång till för mycket information vid sökningar i databaser (Tabell 4.24). Alltså kan det finnas anledning för organisationerna att vidareutveckla de metoder som används för att mäta effektiviteten då den upplevda effektiviteten kan upplevas olika för användarna och cheferna.

Under expertintervjun berättade Företag A att de anställda inte använde sig av några specifika genvägar för att effektivisera sitt arbete (Tabell 4.5) Enkätundersökningen visade däremot att nästan en tredjedel av de anställda någon gång hoppat över säkerhetsregler för att effektivisera sitt arbete. Var tredje person uppfattar vi som ett stort antal, vilket än en gång bekräftar Hyeun-Suk et al.s (2009) tes, att informationssäkerhetens svagaste länk är den mänskliga faktorn. Intressant är även att säkerhetsansvariga på Företag A inte var medvetna om detta faktum. Företag B hade samma resultat, där en tredjedel någon gång hade hoppat över säkerhetsregler, de var däremot medvetna om detta och menade att de oftast upptäckte när anställda tar genvägar för att effektivisera sitt arbete (Tabell 4.16).

Frågan på enkäten om respondenterna upplevde att informationssäkerheten bromsade det effektiva användandet av IT-system, gav olika uppfattningar. Resultaten var avvikande men strax under hälften av respondenterna på respektive företag upplevde att informationssäkerheten

bromsade deras effektivitet (Tabell 4.28). Intressant i sammanhanget är att respondenterna trots den upplevda effektivitetsbroms som informationssäkerhet innebär, inte ansåg att deras arbete innehöll för många säkerhetsregler (Tabell 4.7).

Arnesen & William, (2007) menar att det ska finnas en harmoni mellan anställda och arbetsgivare och en policy ska vara skapad utifrån bådas intressen. Ligger informationssäkerhetspolicyn i användarnas intresse och de har förståelse över policyn, skapas ett större ansvar mot missbruk av policyn. Under expertintervjuerna menade båda företagen att feedback om informations-säkerhetspolicyn från de anställda var viktigt och något de bör ta vara på (Tabell 4.5). Enkätundersökningen visade däremot att en majoritet av respondenterna aldrig fått tillfälle att påverka informationssäkerhetspolicyn (Tabell 4.18). Arnesen & William, (2007) menar att förtroendet mellan anställda och organisationen är en kritisk faktor för att anställda ska vilja följa organisationens policy ansvarsfullt. För att upprätthålla en hög informationssäkerhets-medvetenhet måste användare ha en hög self-efficacy (Bandura & Jourden, 1991). En organisation som upprätthåller en hög self-efficacy hos användarna har även en stark informationssäkerhetskultur.

När användare blir utsatta för säkerhetsproblem såsom virus, spyware attacker och/eller offer för internetbedrägeri, sjunker deras self-efficacy markant (Tabell 2.2). För att bibehålla användares self-efficacy har säkerhetsansvariga ett ansvar att utbilda de anställda inom informationssäkerhet. På frågan om respondenterna ansåg att deras chef på något sätt påverkat deras säkerhetsmedvetande, var det stor avvikelse på svaren i båda företagen. (Tabell 4.8). Det kan betyda att det finns respondenter som inte får den utbildning de behöver. Det kan även bero på att de inte tar till sig informationen som tillhandahålls. Informanterna på Företag A menar att de är delaktiga i att förbereda IS-användarna på problematiska situationer i form av utbildning (Tabell 4.2).

6. SLUTSATSER

Slutligen presenteras slutsatsen där avsikten är att presentera våra data relaterat till vår problemdiskussion.

De slutsatser som presenteras bygger på den litteratur (Kapitel 2) och de resultat (Kapitel 4) som undersökningen presenterar. Slutsatserna som presenteras i detta kapitel är således begränsade till de resultat, begrepp och faktorer som presenterats tidigare i uppsatsen. Undersökningen har fokuserat på informationssäkerhetspolicyns påverkan på effektiviteten hos IS-användare. Påverkan kan delas upp i ett antal påstående som beskrivs nedan:

Förståelse av informationssäkerhetens påverkan av effektiviteten - Respondenterna instämde med påståendet att säkerhet påverkade effektiviteten. Det krävs alltså förståelse för regler om man ska kunna använda sig av dem och öka effektiviteten.

Underlätta användningen av säkerhetsregler inom användarkonto, hantering av information och Internetaccess - Säkerhetsreglerna är till för att användarna ska kunna genomföra arbetsuppgifter på ett säkert sätt för att minska chansen till att organisationen skadas. Således är det viktigt att skapa medvetenhet i form av utbildningar.

Förbättra arbetsförhållandena med fokus på säkerhetsregler - Informanterna har som huvudsyfte att se till att regler följs med rimliga medel. Människan är oftast den svagaste länken när det gäller informationssäkerhet. Arbetsförhållandena är viktiga för organisationerna lika så att säkerhetsreglerna följs. Det är en viktig balans och någon som ”The magic triangle of information security" visar, vilket i slutändan påverkar slutresultatet och ökar effektiviteten.

Det kan vara svårt att jämföra två organisationer rakt av gällande frågor som rör det effektiva användandet av informationssystem, då det är många faktorer som spelar in. Exempelvis så är organisationers säkerhetspolicy så väl anpassat efter den enskilde organisationen att det kan vara svårt att skapa en hundra procentig jämförelse. För att vidare analysera resultatet i undersökningen presenteras nedan de faktorer som tydligt ger svar på den valda forsknings-frågan:

Hur påverkas det effektiva IS-användandet av de säkerhetsregler som finns i en organisations informationssäkerhetspolicy?

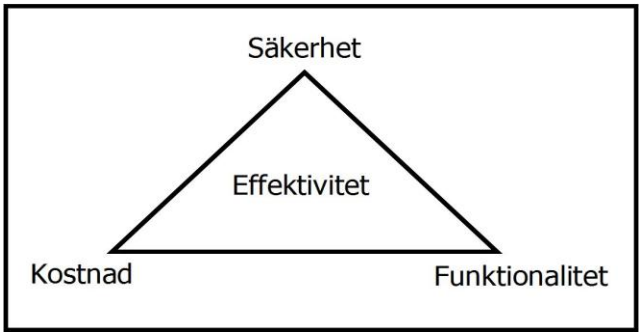
Det som i stor utsträckning utmärker resultatet på enkätundersökningen är att anställda påverkas av säkerheten, vilket bevisas enligt följande punkter:

- Anställda hoppar över säkerhetsregler för att effektivisera sitt arbete.

- Anställda känner att informationssäkerhet generellt bromsar deras effektiva arbetsutförande.
- Majoriteten av de anställda anser att deras arbete skulle effektiviseras om de fick möjlighet att påverka informationssäkerhetspolicyn.
- Anställda anser det tidskrävande att hantera flertalet användarkonto.
- Ett antal anställda anser att lösenordshantering är besvärande.
- Anställda anser att det i viss utsträckning är för mycket information att granska vid sökningar i databaser.
- En stor andel anställda anser att säkerhetsuppdateringar är effektivitetshämmande.

Punkterna påvisar inte att det direkt skulle resultera i ett effektivare arbetsutförande om förhållandet varit annorlunda. Med dessa punkter påvisas snarare att det finns många faktorer som en organisation måste beakta när de utvecklar, implementerar och underhåller informationssäkerhetespolicyn i organisationen. Säkerhetsansvariga måste kontinuerligt utbilda och skapa medvetenhet hos de anställda då de hot som sker mot IS ständigt utvecklas. Som tidigare nämnts, ansåg majoriteten att säkerheten generellt hindrar dem i deras vardagliga arbete. Men eftersom de flesta inte anser att deras arbete består av för många säkerhetsregler, finns det anledning att utvärdera om säkerheten är uppbyggd på rätt sätt.

För att förtydliga ”The *magic triangle of information security*" har vi valt att lägga till det begrepp som bör vara centralt vid utformande av informationssäkerhet, nämligen effektivitet. I figuren nedan presenteras en illustration över de begrepp som vi anser är centrala för att skapa en helhetlig informationssäkerhet i en organisation.



Figur 6.1. *Informationssäkerhetstriangel*

Triangeln hanterar balansen mellan de viktiga begrepp vi funnit som informationssäkerhet hanterar. Effektivitet är det centrala begreppet i modellen, vilket påverkas av övriga begrepp. För att uppnå de organisatoriska målen sker det en avvägning kring faktorernas prioritet . Vad som är tydligt i den utförda litteraturgranskningen, expertintervjuerna och enkätundersökningarna är att säkerhet, kostnad och funktionalitet i olika utsträckning påverkar effektiviteten.

6.1. Undersökningens begränsning

Undersökningen är begränsad i form av tid och rum. Tiden som undersökningen utfördes på var begränsad och medförde att expertintervjuer och enkäten endast kunde genomföras på ett par företag. Tidsramen var begränsad, så det fanns inte heller möjlighet att granska skillnader på olika fysiskt belägna platser, i och utanför Sverige.

Hade inte tidsaspekten varit avgörande hade undersökningen kunnat behandla fler punkter som en informationssäkerhetspolicy bör hantera, för att granska deras påverkan på det effektiva användandet av informationssystem.

6.2. Fortsatt forskning

Undersökningens genomförande påträffade ett behov av vidare forskning. Vidare forskning kan gå ut på att analysera skillnader inom flertalet nivåer på i en enstaka organisation. Intressant hade varit att analysera användare av samma informationssystem, men med olika grad av IT-kunskap för att se hur informationssäkerheten påverkar deras arbetsutförande. De anställda som svarade på enkäten kan generellt anses ha bra IT-kunskaper. Det hade då varit intressant att utföra undersökningen på anställda med lägre, respektive högre IT-kunskap. För att därefter kunna analysera skillnader utifrån olika typer av användares arbetssituation.

Modellen som presenteras ovan är framtagen ur det resultat som undersökningen genererat i förhållande till informationssäkerhet. Det finns olika sätt att mäta effektivitet på, men det som organisationer framförallt är i behov av är ett specifikt verktyg som mäter effektivitet i relation till informationssäkerhet. Trots organisationernas effektivitetstester, brister effektiviteten vid arbetsutförandet vid flertalet punkter som nämns ovan. En vidare analys och utveckling av den modell som presenteras ovan, kan bli en bra grundsten för utveckling av informationssäkerhet i organisationer. Det är viktigt att skapa en effektiv informationssäkerhet, då det i slutändan ligger i hela organisationens intresse.

BILAGOR

Bilaga 1 Förintervju utförd på Företag A

Introduktion av projekt
Går det bra att spela in mötet?

Vilka vi är, namn och bakgrund
Presentera gruppens kandidatuppsats och genomföra en presentation som beskriver vilka vi är och vad det är vi vill ska hända i framtiden. Framtida intervjuer och enkäter.

Presentera vad som är ändamålet med undersökningen

Vem har beslutat att undersökningen ska genomföras.
Vi tillsammans med gruppens handledare, Andres Svensson

Presentation av Case
Vi har tänkt göra en studie av relationen mellan effektivitet och säkerhet. Vi avser att avgränsa oss inom säkerhetspolicyn till vissa komponenter: hur personal hanterar viktig information och hur personal använder sin internettillgång. Effektiviteten som vi vill "mäta" är i vilken utsträckning personalen känner att deras arbete påverkas positivt/negativt av de säkerhetsregler som är satta. Det blir en undersökning baserad på personalens uppfattningar av och attityder till säkerhetspolicyn.

Avgränsningen kommer att ske utifrån ramverket, gjort av Dorthy & Fulford med elva komponenter av säkerhetspolicyn. De som är utvalda för att vi ska genomföra undersökningen utifrån är ”Disclosure of information”, ”Access Internet”, ”user access information”, ”mobile computing” och ”Encryption”.

Information om varje del så som vi tolkar den:

Disclosure of information - Hur personal kan få tillgång till stor mängd känslig data därför är det viktigt med strikta restriktioner.

Access Internet - Eftersom Internet användningen ökar allt mer med tiden och även på arbetsplatserna. Är det viktigt att policyn adresserar vilka bekymmer det uppstår med Internettillgång. Främst handlar det om vid Internettillgång att personal inte genomför någon anständiga sökningar eller till personligt bruk.

User Access Information - Det har notifierats att tillgången av information och företagsprocesser bör kontrolleras utifrån grundval av företaget och säkerhetskraven.

Mobil Computing - Det kan förekomma att man använder bärbara datorer utanför arbetsplatsen och detta kan leda till sårbarhet eftersom det är svårare att kontrollera och försvara mot angrepp. Därför bör policyn beskriva hur man användningen av arbetsdator bör hanteras så att inte någon företagsinformation kan äventyras.

Tidsram

Denna intervju går för vår del också ut på att klargöra vår problemformulering.

Anonymitet

Enkäter till anställda

Enkäters utformning – Webb- eller pappersforn. Web är att fördedra.

Säkerställa att anställda svarar inom vår tidsram?

Ytterligare en intervju med säkerhetsansvarig, eller person som känner till säkerheten i organisationen.

Intervju utformning – e-post eller möte. Möte är att föredra

Bilaga 2 Expertintervju, Företag A och Företag B

Dagordning

1. Presentation av dagordning

2. Oklarheter gällande Undersökningen

3. Vi går igenom våra frågor - Stickord som ska gås igenom

4. Presentation av 'typ' enkätfrågor

5. Öppen diskussion

6. De berättar vilka frågor de vill ha med i enkäten och vilka som bör undvikas

7. Övrigt synpunkter/ Mötet slut

1. Presentation av dagordning

Vid frågor som ni ej vill svara på så behövs ingen längre utläggning på vad det är varför ni inte vill svara. Mer för att effektivisera tiden.

2. Oklarheter gällande Undersökningen

Ska vi tillverka enkäten med era frågor eller gör ni det i ert egna system med våra frågor?

Enkäter skickas ut: 5 maj

Enkäter in: 17 maj

50 tal svarande användare

3. Stickord som ska gås igenom

Fokus på **Tillgång till information**, **Internetåtkomst**, **Hantering av Användarkonto**

Frågor gällande Organisationen

1. Hur är organisationen uppbyggd? Stora drag.

2. På vilket sätt har er organisationsstomme haft någon inverkan på implementationen av säkerhetspolicyn? matris, team, hierarkisk

2.1. Känner ni att er organisationstumme gör det enklare att nå ut med säkerhetspolicyn?

3. Hur arbetar ni med era anställda vid uppdateringar av säkerhetssystem?

3.1 Vid förändring av informationssäkerhetspolicyn får de utbildning/information om det nya regelverket?

4. Skulle ni påstå att ert företag är av flexibel karaktär?

4.1. På vilket sätt är organisationen flexibel resp. inte flexibel?

4.2 Om **företaget** är **flexibelt**, har det påverkat implementationen av säkerhetspolicyn positivt?

4.3. Om företaget **INTE** är **flexibelt**, ser ni några hinder som uppstod av under implementationen som är negativa?

5. Är er säkerhet uppbyggd enligt ISO 17799? Någon annan specifik modell?

6. Något att tillägga gällande organisationens uppbyggnad som påverkar utformning av säkerheten?

Frågor gällande Säkerhetspolicy

specifika frågor i nästa stycke, användarkonton, tillgång till information, Internet access

1. På vilket sätt reglerar ni användarkonto i er informationssäkerhetspolicy?

1.1 Är det vanligt att en person har flera användarkonton?

2. På vilket sätt reglerar ni/hanterar tillgång till information i er informationssäkerhetspolicy?

2.1. Social engineering, metoder för att öka lojaliteten hos anställda? utbildning, teambuilding etc..

3. På vilket sätt reglerar ni tillgång till Internet i er informationssäkerhetspolicy?

3.1 vad står det i säkerhetspolicyn som gör att personer inte får gå in på vissa sidor?

4. I en artikel vi läst ska har den säkerhetsansvarige en avgörande roll för hur bra förankrad

informationssäkerhetspolicyn blir vid en implementation. På vilket sätt är era informationssäkerhetsansvariga delaktiga i att implemetera informationssäkerhetspolicyn?

5. Vilken typ av aktiviteter utför ni för att säkra att de anställda är medvetna om säkerhetsreglerna i informationssäkerhetspolicyn?

6. På vilket sätt utbildas de anställda i säkerhetspolicyn?

6.1. Gällande tillgång till information

6.2. Gällande Internetåtkomst

6.3. Gällande Användarkonto

6.4. Är det bara fokus på säkerheten i utbildningarna eller tar ni upp på vilket sätt användarna bör använda säkerhetsreglerna och fortfarande kunna arbeta effektivt?

7. Bygger ni er informationssäkerhetspolicy efter något specifikt ramverk eller det är ett privat ramverk som enbart är uppbyggt för att vara anpassat åt ert företag?

7.1 På vilket sätt har ni genomgått faser för att implementera informationssäkerhetspolicy? ex planeringsfas implementationsfas

7.2 Är dessa faser något ni genomgår varje gång informationssäkerhetspolicyn har uppdaterats och ska implementeras?

8. Har IS-användare varit delaktiga med förarbetet av implementation av informationssäkerhetspolicyn, att de påverkar slutresultatet?

9. Hur ofta sker riskanalys för att utveckla säkerhetspolicyn? I vilken omfattning? Hur påverkar det de anställda ?

10. På vilket sätt tror ni att informationssäkerheten och reglerna i informationssäkerhetspolicyn påverkar effektiviteten?

10.1. Är det någon speciell del i informationssäkerhetspolicyn som ni ser begränsar effektivt användande mest?

11. Är det något ni vill tillägga som kan påverka effektivt användande i er säkerhetspolicy?

Hantering av Användarkonto och Tillgång/hantering till information

1. Vilka är de valda metoderna för inloggning i de olika delarna av informationssystemet? ex. Flera lösenord, inloggning med dosa (kan jobba även hemifrån)

1.1. Mellan olika system?

1.2. Logga in i olika program?

1.3. Har alla användare i organisationen anpassade konton och behörighetsnivåer, eller har en användare olika användarkonton för att få tillgång till olika delar av systemet?

2. Hur ofta byts lösenord?

3. Om en användare glömmer ett lösenord, hur hanteras det?

4. Hur skiljer sig de olika behörighetsnivåerna för användarna av systemet?

4.1. Olika behörighetsnivåer för anställda med snarlika uppgifter?

5. Har en anställd tillgång till flera olika system som gör att de måste ha fler lösenord än ett?

6. Hur arbetar ni proaktivt för att förhindra att information läcker ut och att anställda är lojala? Utbildning, teambuilding, hänvisning till säkerhetsregler?

7. Hantering av information är viktig aspekt och då man måste skydda organisationen mot externa och interna hot. Bygger detta förtroendet mest på de strikta reglerna av informationssäkerhetspolicyn? Eller bygger det på några andra principer?

8. Vet de anställda vilken information som är sekretessbelagd ex känsliga e-post m.m.

9.Vet de anställda hur e-post ska hanteras, och i så fall på vilket sätt.

Frågor gällande Tillgång till Internet

1. Utför ni förebyggande arbete med Internettillgängligheten?

1.1. Hur tar ni reda på vilka sidor som ska spärras? t.ex. Facebook?

1.2. Vilka slags sidor är spärrade?

1.2.1. Wikis

1.2.2. Google

1.2.3. Pornografi

1.2.4. Nöjes sidor

1.2.5. Sociala medier

1.2.6. Sharelinks

2.2.7. Privat mail

3. Problem med Internettillgängligheten utöver personlig Websökning och pornografi, finns det andra risker och problem som kan förekomma?

4. Vid uppdateringar, ges genomgång till anställda om Internet tillgängligheten?

5. Bygger säkerheten också på att användare är ansvarsfulla och medvetna om de säkerhetsrisker som finns?

6. Arbetar ni någon form av att öka medvetenheten eller hänvisar direkt till strikta regler som informationssäkerhetspolicyn?

6.1 Varför anser ni att er metod är det bästa?

6.2 I så fall hur arbetar ni för att motverka säkerhetsrisker och öka medvetenheten?

7. Vanliga risker med Internet tillgänglighet kan vara spam och virus, risker som många användare känner till. Utbildas personal för att förstå andra risker som botnets / zombies?

7.1 Anser ni att personal med högre medvetenhet kan påverka andra att bli mer medvetna?

8. Enligt ramverk vid implementation av informationssäkerhetspolicies krävs det feedback från användaren kontinuerligt. Är det något som ni använder er av att strukturera informationssäkerhetspolicyn? ex. Att feedbacken ni får låser sidor ?

9. Vilka informationssäkerhetsmoduler använder ni som anställda måste genomgå för att ansluta sig till Internet? Detta är till för att sen under enkäten fråga hur inloggning etc. påverkar deras effektivitet av arbetet om det är omfattande säkerhet.

Övriga frågor

1. Hur ofta servar ni datorerna gällande olika säkerhetsuppgraderingar och liknande?

1.1. Hur hanteras det? Arbetstid?
1.2 Blir personal informerade efter uppgraderingar och om regler ändras, hur de ska följas därefter?

3. I vilken utsträckning loggar ni era anställda och i så fall varför?

4. Hur arbetar ni för att förbättra informationssäkerhetskulturen?

5 Är det någon speciell del i policyn som ni ser begränsar mest?

6. Tror ni de anställda går runt informationssäkerhetspolicyn för att smidigare kunna utföra sin arbetsuppgift? I så fall på vilket sätt?

7. Hur är er generella syn på hur effektiviteten är?

8. Mäter ni effektiviteten på ett speciellt sätt?

9. Har informationssäkerheten en bromsande effekt av den uppmätta effektiviteten som företag kan märka skillnad av?

10. Arbetar ni utifrån feedback som anställda ger er för att strukturera informationssäkerhetsreglerna?

11. Vilka potentiella genvägar kan anställda ta för att effektivisera sitt arbete?

12. Hur upplevs en informationssäkerhetspolicy dels bland ledningen och dels bland de anställda? Finns det dokumentation som kan ge svar på frågan

4. Exempel på Enkätfrågor - Med fokus på effektivitet

Frågorna kommer att gälla:

1. Tillgång till information
2. policy
3. Internet Access
4. (Utbildning - kan hjälpa användare att hantera effektiviteten effektivare)
5. Användarkonto
6. övrigt

Exempel:

1. Känner du till företagets säkerhetspolicy

Graderade svarsalternativ, eller ja och nej

2. Upplever du att säkerheten (ibland) begränsar dig i ditt arbete?
(beroende på hur policyn ser ut, alltså vad vi får reda på under intervjuerna)

- att du inte kan nå alla sidor på Internet?
- att det krävs olika lösenord i olika system?
- att du inte har behörighet till all information?

3. Vet du om du har full tillgång till Internet?

4. Upplever du att du saknar någon hemsida som skulle kunna göra ditt arbete mer effektivt?

5. Vilken grad av kunskap har ni för att veta vilka restriktioner det finns för att skicka mail?

5. Öppen diskussion

6. De berättar om det är några övriga frågor de vill ha med i enkäten och vilka som bör undvikas

7. Övrigt synpunkter/ Mötet slut

Bilaga 3 Transkribering, Företag A, expertintervju

S = Student

A = Säkerhetsansvarig

B = Säkerhetsexpert

1. S: Första frågan. Vi vill veta hur organisationen är uppbyggd i stora drag?

2. A: "Företag A:s Organisation

3. S: Framförallt den delen av organisationen som vi kommer att skicka enkäterna till. Är det divisioner, hierarkisk organisationstumme?

4. B: Jag smilar lite för det är den största vi har.

5. A: Den består av något som heter "Enhet1" som är en global enhet varav då vissa sitter här. En 700-800 sitter här. Den ena, och sen så en annan enhet som heter "Enhet2" som är ungefär lika många, och som också finns ute i världen men den delen som sitter här, är den så att säga, 700-800. Sen legalt i Sverige är dom ett dotterbolag som heter "Företag A" -"Dotterbolag A", Men man kan väl säga att du är, jag tror du är ute efter den svenska delen av, "Enhet1" och "Enhet2",

6. S: Ok

7. A: Och hur den är uppbyggd? Hur menar du sen? Räcker det eller?

8. S: Ja, precis, detta är det som ska kunna ligga till grund.

9. A: Ni får säga till om det inte räcker.

10. S: Nä, det låter bra. Vi kan ta fråga nummer 2: På vilket sätt har er organisationsstomme då har haft någon inverkan på implementeringen av säkerhetspolicyn, eller har det haft någon inverkan? Vi har läst i artiklar om att har man en hierarkisk organisationsstomme så kan det påverka implementering på så vis att det kanske inte är lika flexibelt. Förstår ni vad vi menar.

11. A: Ja, det ska inte egentligen ha inverkat så mycket på det, utan de policys, procedures och guidelines som vi har i "Företag A" gäller överallt oavsett var de befinner sig, oavsett hur organisationen ser ut, och så finns det chefer på olika nivåer som har ansvar för att det här fungerar. Var det de ni hade tänkt er?

12. S: Ja, precis vi vill göra en jämförelse här med artikeln att det kanske inte just, även om dom skriver att det kan bli negativt om det är en hierarkisk organisationsstumme så behöver det ju inte vara så hos er. Då stämmer ju inte den för alla företag. Det dom skriver.

13. A: Man kan väl säga att, organisationen i Sverige den legala organisationen är mer hierarkiskt uppbyggd medan "Enhet1" och "Enhet2" i världen, eftersom de finns på andra ställen än här i Sverige, blir mer en matrisorganisation.

14. S: Ok

15. A: Det är både och.

16. S: Så "Företag A" kan bestå av både och, alltså ute i världen är det en matris, ok

17. B: mm

18. S: Men ni ser inte att det är någon skillnad på hur policyn följs, eller hur den, hur ni för ut budskapet om det?

19. A: Nu pratar vi för Sverige?

20. S: Ja, precis

21. A: Så här är det ingen skillnad, utan här ser vi ju till att föra ut det budskapet, och det är också de ansvariga chefernas ansvar att göra det. Men vi har ju utbildningar och sådant som förstärker det.

22. S: Ja, det kommer vi till. Då har vi ju svarat på 2.1. . Och Trean då. Hur arbetar ni med era anställda vid uppdatering utav era säkerhetssystem. Får dom..

23. B: Definiera säkerhetssystem.

24. S: Det är ju, informationssäkerhetssystemet

25. B: Antivirus, Backup och så eller?

26. S: Precis. Behöver dom..

27. B: Vad som händer praktiskt är att det är "IT-partner1" som är ansvariga för att både ta fram och se till så att de är i funktion, och testar alla våra säkerhetssystem. Sedan, oftast, så informerar dom antingen via E-post eller på ett annat sätt alla anställd hur man ska göra för att uppdatera det. Det kan vara en länk eller något som man ska gå in på för att uppdatera på sin egen dator. Men hur tänker ni på uppdateringar, hur man ska använda det?, eller hur tänker ni då?

28. S: Nä just säkerhetsuppdateringar. Men så då är det att.

29. A: Dom uppdateras.. Mycket av våra säkerhetsuppdateringar uppdateras automatiskt. Så fort du slår på datorn så gör den sin uppdatering.

30. B: Ja, en sms-tjänst där alla programuppdateringar kommer. Men i vissa fall måste vi aktivt gå in på någon länk eller aktivera så att det blir aktivt i varje klientmaskin

31. S: Och är det dom anställd som gör det då eller är det ni som går in och för det.

32. A: Man kan säga såhär om jag får tolka dig, Huvuddelen, nästan, alltså säkert över 90% av alla säkerhetsuppdateringar behöver inte användaren göra någonting utan det bara rasslar in i burken. Och då är virusdefinitioner uppdaterade och andra säkerhetspatchar eller vad det nu är för någonting. I vissa fall behöver användaren göra lite handarbete, och vid dom fallen så får man då ett mail med instruktioner hur man ska göra då.

33. S: Ja, okej

34. A: Men det är rätt sällsynt.

35. S: Och är det knutet till någon utbildning då? Vi kom in på det innan, att dom anställda vet om..

36. A: Nej

37. S: Dom bara får informationen och ni litar på ett dom kan hantera det?

38. B: Med instruktion, ja. Steg för steg med länkar och information, instruktioner hur man ska göra.

39. A: Men det handlar alltså om virusuppdateringar. Det handlar om andra säkerhetspatchar..

40. S: Ja, precis..

41. A: ..som vårat datorbolag måste ha in därför att det finns en brist någonstans och så har det kommit en patch och så kör dom ut den, tvingar ut den i systemet, men användaren behöver inte göra någonting.

42. S: Nä..

43. A: Sen skyddas ju datorn då, det är tekniska säkerhetssystem som körs in.

44. S: Okej.

45. B: Och det är ju då också att om dom nu skulle påverka att vi inte kan jobba med systemen, liksom driftavbrott, då får vi information före att den lördagen den och den tiden kan ni inte använda det systemet för det pågår någon form av säkerhetsuppdatering. Så vi får information före. Sen vi i vårt intranät som heter "Intranät1" där kan man också läsa att nu kommer vi t.ex. byta vårt backup-system, en integration kommer att ske vecka x, så det kommer för- information, och sen kommer det information när vi får det, hur ska vi göra. Så att det är information ut.

46. S: Så det var alltså på en sajt som era anställda regelbundet ska gå in och läsa på eller.

47. B: Ja, Precis

48. A: Byter man backup-system som vi gjorde här för ett antal år sedan. Då måste man ju gå ut till varje användare, så att varje användare får den här instruktionen hur man ska göra. Därför att, en sak är att få in det i datorn så att säga, en annan sak är hur man ska sen konfigurera det. Hur ofta man tar backuper och vad man klickar och vad man ska tänka på och vad dom inte tar backup på.

49. B: Så det är liksom olika kommunikationskanaler, så man gör det samtidigt, ni förstod.

50. S: Ja

51. B: Det kommer både till oss, men det finns ju någon annan stans, plus i vår dator finns alla manualer till olika program och säkerhetsprogram under startmenyn. Så vi har dom som en exe-fil där man kan läsa hur VPN och backup fungerar, så där finns instruktioner.

52. S: Har ni det i er någon slags säkerhetspolicy, hur ofta det här ska ske, uppdateringar. Sker det vart tredje år eller sker det varje år?

53. A: vilket?

54. S: som att ni uppdaterar ert backup-system..

55. A: Nä

56. S: Det sker efterhand som det är behov eller?

57. A Nä, när vårt databolag har kommit på en bättre lösning än vi hade innan.

58. S: okej..

59. A: Så driver man ut den lösningen och det är då man får den instruktionen, det är då den installeras i datorn.

60. S: Så okej, efterhand som dom utvecklar en ny, säkrare lösning kommer de.

61. B: Och det är dom som heter "IT-partner1", IT bolaget.

62. S: Ok, 3.1. då. Vid förändring informationssäkerhetspolicyn får de anställda utbildning och information om det nya regelverket?

63. A: Jag är rädd för att vi pratar om skilda saker här. På trean då pratar vi om IT-tekniska säkerhetssystem som pushas ut till den enskilda användaren. Och ibland med instruktioner

64. S: Ja, det blir lite lustigt där med 3 och 3.1 dom hänger inte riktigt..

65. A: Ja, säkerhetspolicyn är mer ett dokument om hur man ska förhålla sig som individ..

66. S: Ja..

67. A: Till vad som gäller..

68. S: Ja, ni har svarat rätt, men det står lite konstigt där med 3 och 3.1..

69. A: Men svaret på 3.1. blir väl då att det ändras inte så mycket, och i den mån det ändras så är det samma innan att respektive VD i dom här dotterbolagen har ansvaret att se till att det kommer ut till respektive organisation. Och till sin hjälp har han då Information Management Security Officers som ser till att det sker. Och sen har vi en mer koordinerande roll för Sverige . I våra utbildningar tar vi naturligtvis upp det som är nytt. t.ex. retention period och sådant som inte var i confidentiality policyn från början, eller vad det nu är.

70. S: Ja..

71. A: Men, det låter ju bra. Det ska ju också singla ner till siste man..

72. S: Precis, alla ska ju få ta del. Får Cheferna då själva bestämma hur de ska informera de anställda om det. Förstår jag det rätt?

73. A: Nja, dom har ju ansvaret för att applicera dom policy, procedurs och guidelines som finns, att dom följs i respektive dotterbolag..

74. S: Ja..

75. A: Då får man också fylla i en control self assessment i april-maj varje år. Om man gör det eller inte mot dom policyna och mot många andra policies. Så ansvaret har dom men, ska vi vara riktigt ärliga så funkar det inte 100 %, att det sipprar ner till siste man, det gör det inte.

76. S: Så dom har mer ansvar att det följs än kanske sprida det?

77. A: Nä, dom har ansvar för att sprida det också. Men med så stora organisationer blir det kanske inte alla som..

78. S: Nä, okej, men det är så det ska vara?

79. A: Men är det större och mer väsentliga förändringar är det ju lättare att få igenom det så att säga. Men det ändras inte så mycket, inte än i alla fall, tycker inte jag.

80. B: Nä, inte så. Och vi då i vår tur försöker då hålla, de Information Manager Security Officers, som finns i alla bolag, om vi pratar om Sverige, uppdaterade om vad som gäller. Vi ska vara experter på alla sådana här förändringar. För att dom i sin tur har ansvaret för att implementera det i sina bolag. Dom har fått det delegerat till sig, att dom ska göra det. Så att vi har olika källor hur vi gör detta. Det är ren utbildning som vi kan erbjuda bolagen, det är inte obligatoriskt, om vi inte bestämmer att det här är så viktigt att det ska vara obligatoriskt. Sen har vi då våra internttidningar, vi har olika. Vi har "tidning1" och "tidning2", som vi sprider om det är något viktigt, då skriver vi artiklar om det, vi kan också ha det som olika aktiviteter, d.v.s. skicka broschyrer eller ha det på våra tv skärmar som ni såg i korridoren eller andra aktiviteter för att sprida det ännu mer, att det här är viktigt. Men det är kanske mycket mer när det är påminnelser när det är någonting viktigt eller när det är nya saker.

81. S: Men ni har ändå lite olika sätt att få ut det..

82. A: Ja, Precis.Via oss då. Men primärt är det inte vårt ansvar. Utan det är VD:n i dotterbolagets ansvar.

83. S: Ert ansvar är att informera VD:n?

84. A: Nej, vårt ansvar är att vara experten som kan hjälpa till och stödja honom eller henne eller IMSO:n eller någon annan.

85. S: Okej..

86. A: Men rent generellt ligger inte ansvarsdelegeringen på oss. Att policy proceduers och guidelines i Företag A sköts utan det ligger på VD:n.

87. S: Okej, Ja..

88. A: Vi har många VD:ar här så..

89. S: Ja då är det fortsatt frågor generellt på organisationen här, skulle ni påstå att ert företag är av flexibel karaktär?

90. A: Du måste förklara vad du menar med det där.

91. S: Det var ju det jag sa innan, att vi hade läst någon rapport om, hur ska vi säga, att man har enkelt att ta till sig nya saker, att om någon förändring sker i en informationssäkerhetspolicy så är då organisationen flexibel att ta till sig de nya förändringarna. Som vi förstod det så har en flexibel organisation enklare att ta till sig säkerhetspolicyn.

92. A: Vad är motsatsen?

93. S: Ja det är väl en icke flexibel organisation, en hårt styrd organisation. Att dom inte har samma kontakt, så som vi förstår det nu har ni kontakt, ni sprider med tidningar och annat..

94. A: Ja, jag skulle vilja påstå att vi är en flexibel organisation.

95. S: Precis, men då är det en följdfråga, om det påverkat implementationen på säkerhetspolicyn positivt? Att ni är flexibla.

96. A: Jag menar, att ”Företag A” är inte centralt styrt uppifrån. Utan det är ett delegerat ansvar till alla möjliga. Då Vd:ar, marknads-VD:ar och neråt. Nu kommer det mer och mer centralstyrning därför att man tycker att vissa saker i corporate governance och måste vara strikt. Men om man tittar på Företag A här och i världen så är det flexibelt, det är inte toppstyrt.

97. S: Okej..

98. A: Utan det är ganska korta vägar mellan beslut och handling.

99. S: Du sa att det blir mer centraliserat. Är det på grund utav EU?

100. A: Det beror på de corporate governance som vi tar till oss, allt möjligt, som bland annat är regelverk i EU, men även annat. Vi har gått från en väldigt decentraliserad organisation, med ännu kortare beslutsvägar, så är det så pass stort nu, och det finns så många regelverk som vi måste följa. Och då måste man styra upp det så att det finns kontroll på det uppifrån.

101. S: Okej, Ja de var bra svar..

102. B: Ja, och där kan jag nog bara lägga till också att det är också en av våra grund värderingar ”G1”, så att vi har ju policys och procedures och guidelines som är mandatory, som är obligatoriska, men man har rätt att göra på olika sätt hur man implementerar den, det är ju inte bara one-way så vi måste göra, exakt det här ska alla göra, utan man kan anpassa det efter målgruppen, efter landet eller efter hur man gör det bäst, man tycker att det här är det bästa för oss. Om det förklarade någonting.

103. S: Ja, Absolut. Då behöver vi inte ta 4.3. men 4.2., Men vi har diskuterat det redan kanske.

104. A: Vi kan ju säga såhär på 4.2. så får du(B) plussa på. Vi fick t.ex. en confidentiality policy..

105. B: 2005

106. A: 2005, och då går vi till min chef som är VD Företag A, moderbolaget Sverige, och säger att här krävs det ett change management för att få igenom detta annars så blir det ingenting av det. Och så förankrar han det i VD gruppen som han har med Vd:arna att vi hjälper till att få change management, att få den här policyn och göra vissa saker för att dom själv ska kunna jobba efter den på ett bra sätt, vilket du(B) jobbade med i..

107. B: 2 år

108. A: i ett par år ja, det är ett sätt att alla bolagen behöver inte jobba med det själv utan nu blir det så att man gör ju likadant i dom bolagen vilket underlättar.

109. S: Okej, så ni kan anpassa samma grundmodell

110. B: Ja, samma process, samma sätt

111. A: man fick i policyn globala matriser på vilken övergripande information som skulle ha vilken klass..

112. B: Dess informationsklassificering..

113. A: Det har man gjort på koncernledningsnivå, och där får du inte ändra på det utan vidare, men all information finns inte med där, utan vi i vår avdelning här kan då förhålla oss till mycket av den här informationen, vi har också annan information, och då måste vi hantera, eller förhålla oss till hur ska vi hantera den informationen som vi har här, i det dagliga arbetet, i den där matrisen, så att alla är överens om att är det nu är ett sånt här papper, så ska det märkas och klassificeras på det sättet. Och det var workshops lite överallt som B då höll i.

114. B: mm, och det som jag skulle lägga till där är också att vi har väldigt nära till bolagsledningen, så att det är inte sån här, högt upp till högsta, utan vi har ju nära kontakt till alla bolags ledningsgrupper, så då, man kommer snabbt till om man vill implementera någonting. Så det är inget konstigt, som tar jättelångt tid att förena, inte massa politik och sådant som måste snurra runt utan man kommer direkt till VD.

115. S: Okej, ja det är bra. Vi kan gå vidare till 5:an. Är säkerheten uppbyggd enligt ISO 17799 eller är det någon annan specifik modell som kanske ni har grundat er informationssäkerhetspolicy på?

116. B: Svaret är ja, det är IT-Partner1 som har skrivit policyn, dom har ju grundat den på den

117. A: men heter den inte 27001 nu?..

118. B: ja, nu ja, den heter 27001, men den hette så tidigare.

119. S: Vi har hittat litteratur på, punkter som vi har valt att avgränsa oss på, men vi kommer till det senare.

120. A: Vår policy är uppbyggd kring den.

121. B: Precis. Och 17799, om ni inte har studerat den, det är en gammal variation som den nya heter 27000..

122. S: Ja den nya har vi inte sätt, men den gamla har vi sett exempel från..

123. B: Och den bygger på en ISO standard som är 7799 så den är nästa steg då.

124. S: Okej. Ja, är det något som ni vill tillägga gällande organisationens uppbyggnad? Och utformningen av säkerheten?

125. B: Nej

126. S: Så det här är det grundläggande.

127. A: Även om det här kan låta bra, det här som vi har sagt nu, så är det inte helt enkelt att nå ut till användarna med dom här policyna och sen att dom gör som det står där. Det är inte helt enkelt, varken för oss eller för någon annan, att tränga igenom där, och få det att bli som det står där. Nu försöker vi ju bland annat genom ett antal saker som B har sagt men också utbildningar och så, träningar. Men det är inte helt enkelt.

128. B: Det är ju gemensamt för alla företag, det är inte så lätt att kontrollera håller, att man gör så. Jag kan inte sitta åtta timmar bredvid dig och se till att du gör som du ska..

129. S: Nä, precis..

130. B: Vi kan bara göra intervjuer och prickkontroll, sådana här stickprov och annat. Men det finns ju ingen som kan kontrollera att man gör exakt som man ska. Och det är ju samma för alla.

131. A: Vad vi gör där, jag tror inte vi har sagt det, vi gör Gapanalys på bolagen i förhållande till den där standarden om 10 kapitlen där vi ställer frågor, öga mot öga, eller via webenkäter, till dom, och då tar vi bolag för bolag. Och i bolagen kan det vara olika befattningshavare, det kan vara ledning, det kan vara personalchefer, eller personalavdelningen, det kan vara säkerhet och IT inom bolaget, det kan vara vanliga användare. Och då får man olika frågor, Och dom frågorna gör ju då att vi mäter hur stora gapen är i förhållande till att ha 100 % uppfyllandegrad i dom 10 kapitlen i standarden.

132. S: Ja..

133. A: Och det har vi gjort med alla bolag, och vi har gjort det flera gånger med vissa. Och där mellan har man förbättringsarbete för att få upp det, stänga gapet. Och det gör vi kontinuerligt så det kommer vi att fortsätta med. I år ska vi göra det med tre bolag?

134. B: Ja.

135. A: Och där är varierande framgång hos bolaget. Där är dom som ligger över 80 % uppfyllandegrad och där är ett bolag som ligger under 70 %.

136. S: Då är det ändå ganska..

137. A: Ja, 69 har de tror jag, och så ligger dom där emellan. Har man 69 är det rätt mycket människor som känner till dom saker som man ska känna till. Där är 31 % gap.

138. B: Och vi har då 12 bolag, eller det kanske du sagt..

139. S: Okej..

140. B: ”Bolag1” som ni ska göra enkäten till är bara ett av dom, men det är det största.

141. S: Ja, vi kommer att gå vidare här nu med frågor gällande säkerhetspolicys, det ska gälla informationssäkerhetspolicys, dom tre specifika frågor som kommer senare är, det vi vill inrikta oss på är hantering av användarkonto, tillgång till information och internetaccess. Det är de delar vi vill undersöka och de vi tycker kan påverka effektiviteten. Det kommer mer om det sen, och det kan va så att frågor går in i varandra så ni kan också hjälpa oss med att vara uppmärksamma på sånt som vi tycker att vi har svarat på. För det är bättre att vi för en öppen diskussion, så som vi har gjort. Men vi tar den första här då. På vilket sätt hanterar ni användarkonto i er informationssäkerhetspolicy?

142. B: Tänker ni policymässigt

143. S: Ja, policymässigt

144. B: Policymässigt, det är naturligtvis hur den ska konstrueras och vad man får göra med den, att man inte får upplåta en till någon annan, att det ska, lösenordens ska hålls krypterat och att man inte får avslöja till någon annan. I vissa olika, är det mot Internet?

145. A: I största allmänhet?

146. S: Ja, i största allmänhet.

147. B: Okej, för i vissa applikationer och system sa har man ju olika säkerhetspolicys där det gemensamma är att vi har ett antal tecken på hur de ska konstrueras. Men byten av lösenord är ju olika beroende om det är "system1" så måste det bytas oftare än om det är eller vanligt-"system2" konto så är det ju på ett annat sätt.

148. S: Okej..

149. B: Ok var man kommer till, accessen, ingår det med användarkontot?

150. S: Ja

151. B: Vi har ju accesser till massa olika applikationer och filservrar vilket vi nu tittar på?..

152. S: Det är mer den generella synen, som fråga 1.1...

153. B: Om jag säger så här, i den perfekta världen finns ju någon ansvarig som ser till att man får rätt rättighet genom sitt konto. För det är som ett passerkort som man får massa accesser till det. Så att det finns ett behörighetssystem hur man styr..

154. S: Okej..

155. B: Och vi har då active directory inom, där vi styr våra rättigheter, vad gäller där. Det finns separata system som har olika sätt hur man sätter dit användarkonton, beroende på vad det är. Men inga gemensamma konton. Det finns regler om det är lånekonto, hur man byter dom hur man reviderar dom, hur man tar bort dom. Allt sådant finns.

156. S: Så kan man säga att varje konto är anpassat för en anställd eller finns det vissa typer av konto så att en anställd kan ha flera olika konton?

157. B: Du kan ha flera olika beroende på om det är stand-alone system, eller om du har dom, som filservar finns det ju gemensamma strukturer hur man bygger upp det, men om det är separata, då är det helt annat, och det är ju systemägaren som ansvarar hur det kontot byggs upp. Var det svaret på frågan?..

158. S: Ja?..

159. B: För dom styrs inte centralt, alla system styrs inte centralt via IT-bolaget...

160. A: Alla system som är verksamhetskritiska går genom vårt IT-bolag. Men det kan ju finnas andra system, t.ex. säkerhetsavdelningen, vi har valt att ha vissa av våra system utanför IT-systemet. Så vi har ett eget nätverk till

våra..

161. S: Okej.

162. A: Och då har vi andra inloggningsförhållanden där. Och användarkonton.

163. B: Och sen är det ju då accesserna, hur man ger dom, då är den som äger systemet eller applikationen som sätter upp om det är rollbaserat, det kan va rollbaserat, eller det kan vara vilken del i systemet, hur mycket man släpper in. Det beror på vad du jobbar med, om du är anställd konsult o.s.v. Så man styr det på dom olika, men jag kan inte ge något generellt om ni inte säger att ni vill veta..

164. S: Nä, det låter bra, det kommer delar sen när vi tar lite mer exakta frågor.

165. A: Man kan ju också säga att normalt sätt det användarkontot som anställda har ger tillgång till det mesta som de anställda behöver. Eller hur?

166. B: Ja. Så det regleras, du får den rättigheten.

167. S: Okej. Då har vi täckt av 1. och 1.1.. Då är det tillgång till information, hur relegerar ni det i er informationssäkerhetspolicy. Den hör ju lite ihop med föregående fråga om konto.

168. B: Det är ju kanske något jag kan säga här för att komplettera, I informationssäkerhetspolicyn finns ingenting om vilken information man ska ha tillgång till däremot i confidentiality policyn som handlar om informationsklassificering står det mer om att handlandet av restricted eller highly confidential eller internal, då styr man där. Att man klassificerar informationen istället och sen ska man rätta accessen till det.

169. S: Okej..

170. B: Gav det förklaring på det?..

171. S: Ja..

172. B: Så att om man har en information som är restricted måste dem skyddas så att det bara är vissa som får tillgång till den i systemen. Men det står inte i informationssäkerhetspolicyn. Och säkerhetskoppling till confidentiality policyn, att det är klassificering som gäller.

173. S: Ja..

174. B: Så det är enligt vår klassificeringsmodell som vi styr vad man ska få tillgång till. Alltså hur känsligt det är.

175. S: Ja, det är bra. Det kommer mer specifika frågor på tillgång till information senare så vi kan gå vidare.

176. S: Hur ser ni på det med social engineering, upplever ni det som ett problem?

177. S: Till exempel kan någon ringa in och säga att jag har glömt mitt lösenord, kan ni skicka det?

178. A: Det gör vi inte.

179. S: Finns det liknande luckor?

180. A: Kallar du det social engineering?

181. S: Ja, alltså hur man använder människans svaghet för att komma in i systemen.

182. A: Vi skulle aldrig ge ut ett lösenord på det sättet och det har funkat på lång tid här.

183. S: Om man till exempel är ute och reser och har blivit av med sina lösenord så kan man ringa in och be om nytt lösenord?

184. A: Nej, det gäller att hålla tag i sina lösenord när man är ute och reser. Datasupporten lämnar inte ut lösenord till någon som ringer och säger att ”Jag sitter i Frankfurt och jag ska gå in via secure ID remote access hit och har glömt mitt lösenord.”

185. B: Däremot har vi något som heter selfservice så man kan resetta sina lösenord. Vi har en mjukvara för det. Ni vet när man matar in olika intressen, man fyller i en sån där tablå, till exempel förra pojkvännen osv. Sen får man upp random fråga som man ska svara på.

186. S: För att få ett nytt password då alltså?

187. B: Ja.

188. S: Social engineering... hur ser ni på...

189. A: Det förekommer på ett annat sätt här. Inte gentemot IT-systemet, man ringer in och vill prata med en utvecklingsingenjör och luskar om vad de håller på med. Nu har de lärt sig att inte svara på det.

190. S: Är det något som ni har ni lärt upp dem?

191. A: De har lärt upp sig själva men vi sprider det budskapet till alla andra. Alltså man ringer in utifrån och utger sig för att vara anställd i det här företaget, då kan man nyckelord till någonting och så försöker man luska. Då drar dem öronen åt sig och nu är svaret man får ”Du, jag har inte tid nu men får jag ditt telefonnummer så kan jag ringa upp dig” och under den tiden däremellan så kontrollerar man om den här personen dels finns i företaget och dels har rätt till informationen.

192. B: Men att öka lojaliteten ligger i mjuka värdena, att vi har en bra personalpolitik, att man känner att man har bra utvecklingsmöjligheter, att lönenivåerna är bra... allt det där runtomkring, det mjuka. Det är där man bygger lojaliteten. Det kan man inte utbilda någon till och säga ”nu ska du bli jättelojal!” men däremot att utbilda som dem, som A säger med saker som inträffat, då kan man förebygga att man inte gör ett misstag bara för att man är blåögd.

193. S: Nä, precis.

194. A: När vi diskuterar detta på våra kurser, om våra anställda är lojala så har jag inte varit med en enda gång när någon sagt att vi inte är det.

195. B: Nej och en sak som man kanske kan tolka att vi kanske är lojala är att vi brukar fråga om vi hur länge man har jobbat på företaget. I just det här bolaget har vi två personer som har jobbat i 43år, så det visar att man trivs på ett sätt i alla fall.

196. A: Men medel anställd tiden på företag A globalt är 12år.

197. S: Det är rätt länge.

198. A: Mm, men det kommer nog ändras. Det handlar om att samhället ändras och ungdomar som ni byter oftare än oss gamla.

199. S: Det kanske hänger samman med det vi pratade om där ute med att ni anställer framför allt internt och mindre externt, så man känner att man kan...

200. A: Vi anställer externt också men det finns jobbrotation internt också. Men jag menar nog att lojaliteten här kommer från att företaget är ett privatägt företag med starka ägare som är långsiktiga och det går bra för företaget och har gått bra. Det finns massa förmåner som den anställda kanske inte ser varje dag, men de finns där och det är ingen som har synpunkter på det utan den här friheten med ansvar/frihet.. och som du sa bra personalpolitik och bra utvecklingsmöjligheter.

201. S: Familjekänsla?

202. A: Ja, även om det har blivit stort så finns det där någonstans.

203. B: Här är det många som är släkt med varandra också som jobbar här. Man jobbar inte vid sidan om varandra men att man är familjär på det sättet också.

204. S: Är det så vid rekrytering också?

205. A: Nej, vi ska anställa den bästa personen.

206. B: Det finns en process som följs.

207. A: Men det handlar om att till exempel båda jobbat här, så har de gift sig och fått barn och så har barnen glidit in på ett bananskal så snart är hela familjen här... det är inte så många, men det finns.

208. S: Som vi tänkte där var att social eningeering och lojalitet har ett samband, ni säger att ni har en väldigt lojal kultur här men ni har inte ett så stort problem med social engineering?

209. A: Det förekommer hela tiden att det händer, det jag beskrev.

210. S: Men det är inget stort hot?

211. A: Vi har på sista delen på vår informationssäkerhets utbildning 15 frågor där de själva får skatta hur bra vi är på företaget från dålig till mycket bra och den sista frågan är ”om någon extern frågar dig om företaget A:s konfidentiella saker, svarar du då?” Då är det alltid ett högt svar, på den, alltså man är försiktig om någon obehörig frågar. Frågan innan är något i stil med om man pratar högt på offentliga miljöer så som flygplan, tåg, taxi och så vidare och där tycker man att man är rätt dålig.

212. S: Okej, så det är inte medvetet då?

213. A: Precis, så då gör vi ett litet skämt av det, precis som du nu säger så är vi på sista frågan medvetna om på frågan innan är vi ju så att säga medvetslösa. Så det gäller bara att koppla på medvetandet när man är på flygplatsen eller vart man nu är, så funkar det också, likadant med det här att prata högt i telefon när man är på offentliga platser... där har vi en del att göra, men det har många andra företag också.

214. B: Jag tolkar inte riktigt inom oss att det här med social engineering går ihop riktigt med lojaliteten hos oss. Utan det handlar om att man är omedveten, inte om att ”jag är inte lojal och jag vill berätta allting.” Det är så jag upplever det.

215. A: Jo, men så till vida kan man säga att det går ihop alltså är man lojal så är man ju lite försiktigare i den här.. där man inte kan inse att det är social engineering. Är man medveten om att det är det, då är man jätteförsiktig, då är alla ljusen röda.

216. S: Men hur hög grad av omedvetenhet tillåter ni, om ni skulle få reda på att 50 % pratar högt ute på gatorna, då är det väl ganska allvarligt? Hur skulle ni hantera det, tar ni till stora åtgärder då?

217. A: Vi pratar om det ständigt på våra utbildningar och vi har skrivit om det i vår interntidning och vår före detta koncern chef har skrivit om det. Det är inte så att det är ett jätteproblem, inte värre än hos nån annan men vi vill tackla problemet.

218. S: Och det sker hela tiden?

219. A: Ja.

220. B: Jag vet inte om jag berättat hur mycket vi utbildat, men vi har gått igenom 3000 som vi har utbildat.

221. A: Jag tror inte vi haft 3000, lite mindre.

222. S: Ok, då kommer vår tredje...

223. A: Nej, vi har ingen tillgång till Internet alls.

224. S: Ni har ingen tillgång alls?

225. B: Nä, han bara skojar.. vi gör det enkelt för oss...

226. A: Men faktum är att det inte bara är ett skämt.. vi fick inte använda Internet förrän 1998.. 1997 eller 1998. Anledningen var att våra säkerhetssystem inte var tillräckligt bra för att hantera det. Alltså säkerhetssystemen var bra, men inte för att hantera Internet. Så där för väntade vi tills det var på innan vi släppte på Internet. Alltså brandväggarna och allt sånt måste vara riktigt bra innan vi släppte på det... och det är rätt sent, 97, 98. Innan fick man ha två datorer, en stand-alone som inte gick på nätverket som man i så fall hade Internet på och en som gick på nätverket.

227. S: Var det en jobbig övergång då?

228. A: Nej, inte alls.. men policyn var att vi inte fick vara på Internet samtidigt som vi var på företagets nätverk därför att alla säkerhetsgrejer som skulle vara på plats inte fanns på plats.

229. S: Okej.

230. B: ...Tillgång till Internet i informationssäkerhetspolicyn.. Vi har tillgång till Internet och det som styrs är hur mycket man får vara privat, och sedan är det då vilka sidor man inte får besöka, dem är diskriminerande och olagliga, så som porr och sånt får man inte besöka, det är förbjudet men annars får vi använda Internet...

231. A: och så står det lite om risker i största allmänhet med nedladdning och sånt här.. säkra sidor och inte säkra sidor...

232. B: Sen däremot om man nu utgår ifrån policyn så har vi en teknisk lösning som vi har, filtrering som gör att man inte kan komma åt vad som helst. Det finns en filtrering som gör att man inte kan komma åt porrsiter, man kommer inte in på vissa saker men man kan ju ändå komma åt det på nåt sätt å vis och det får man inte göra men vi har en sån spärrning så att säga.

233. S: Det är lite samma sak som det där med social engineering, är man medveten vad man inte får göra så..

234. A: Bland 20 000 finns det alltid någon som inte kan låta bli vissa sidor.. men då kan de inte för att det är spärrat

235. B: Då får de bara ett meddelande att de inte kommer åt det.

236. S: Ok.. där står det 3.1an också..

237. B: Ja, precis.

238. S: Nästa är då: I en artikel vi läst ska har den säkerhetsansvarige en avgörande roll för hur bra förankrad informationssäkerhetspolicyn blir vid en implementation. På vilket sätt är era informationssäkerhetsansvariga delaktiga i att implementera informationssäkerhetspolicyn?
239. Jag vet inte om vi kanske täckt den när vi pratat om organisationen.. alltså er delaktighet i det här med att ni tar det vidare till cheferna..?
240. A: Ja, vi är i allra högsta grad delaktiga genom den utbildningen och Gapanalysen och sånt vi har. Gapanalysen visar ju på brister att de inte är utbildade och sen så får de utbildning.

241. S: Precis...

242. B: Och dom IMSO:rna som vi nämnt tidigare, alltså dom här information management security officers som vi har i alla bolag, dom är jätteviktiga för dom är i sin egen verksamhet hela tiden, dom träffar på Calle, Pelle, Nisse, Lena hela tiden.. Det gör inte vi utan vi kommer dit lite då och då och gör utbildningar och sen träffas i andra projekt, så det är jätteviktigt med IMSO's engagemang.

243. A: Men då kan jag tycka att IMSO:rna där ute, dom kan vara mycket välkända i bolaget och alla vet att dom ska kontakta den personen, men det kan också finnas IMSO:n som inte är så kända och då blir dom mer okända, organisationen vet knappt att dom finns.

244. B: Så det är upp till dem att driva det på ett bra sätt och synas. Men vi fångar också det i våra gap analyser så är de osynliga ser vi till att de blir synliga på olika sätt.

245. S: Okej.

246. B: Vad var det mer... säkerhetsansvarig... om A är avgörande...

247. A: Ja, det är väl du och jag..

248. B: Men har vi svarat på det? Ja, det är jätteviktigt, att man har nån som driver.

249. S: Ja, precis..

250. B: Vår ambition är väl ändå att säkerheten ska vara en del, inte någonting man lägger till utan det ska vara en del i verksamheten.

251. S: Japp... och vilken typ av aktiviteter.. det hade vi också..

252. A: Där ser ni en (pekar på broschyrer)

253. B: Där ser ni en ja, det är några broschyrer vi gjort.

254. S: Tidningar också va?

255. A: Vi skriver i "Tidning 2"... artiklar om... inte varje gång men då och då om det och andra... det kan vara...

256. B: det kan vara öppet hus i säkerhet som vi arrangerar med utställare som en minimässa internt.

257. A: Hackattacker och knäcka lösenord snabbt som ögat och så går man runt där och så finns det biometriska kortläsare och... you name it..

258. S: är den obligatoriskt?

259. A: Nej, alltså det är öppet hus. Man har det en dag mellan till exempel 10 och 2, så kommer de som har tid och lust in där.

260. B: Sen håller vi i det här IMSO-nätverket, vilket gör att vi ger dem extra mycket utbildning, vi träffar dem mellan två till fyra gånger per år för att de ska ha spetskompetens.. vi gör alla möjliga såna här saker då.. tar fram saker man kan dela ut med säkerhetsbudskap.

261. A: ja, broschyrer gör vi ju.

262. B: Broschyrer gör vi och dom har vi också här.

263. A: Alltså vi formulerar ibland om policyn till mer broschyraktig utgåva som är lättare att ta till sig. Där har vi till exempel om man ska ta in konsulter som ska jobba i företaget As nätverk med vår kärnverksamhet. En quickguide, vad ska man tänka på innan man kommer hit, under tiden den är här och efteråt.

264. S: Är det till konsulten?

265. A: Nej , till den som tar in den.

266. S: Okej.

267. B: Den här är för informationssäkerhet.

268. A: Det är informationssäkerhetspolicyn i huvuddrag, alltså kan man det som står där så kan man Det som man behöver kunna.

269. S: Den här som är orange?

270. A: Japp.

271. S: Skulle vi kunna få en sån?

272. A: Nej!

273. S: Nähä, det får vi inte...

274. A: Och det här confidentiality policy, den policy som handlar om klassificering och konfidentiellitet, ansvar och hur det ska hanteras och så vidare..

275. S: okej.

276. A: Och sen den är för säkerhets-arbetsmiljö och säkerhetsordning skrifter, mest för entreprenörer... byggare, rörläggare och vad det nu är för nånting men även för konsulter, att de inte får vara här vilka arbetstider som helst.

277. S: Okej.

278. A: Jo… vi kan väl överväga om ni ska få titta i dom...

279. B: Ja, ni kan se sen...

280. A: Hur är den klassad?

281. B: Den är internal.

282. S: Okej, så ni klassificerar alla broschyrer?

283. B: Ja precis, därför kan vi inte bara lämna ut, utan sekretess avtal.. ja ni kan få läsa sen...

284. A: Men ni kan få ett par såna på svenska

285. S: Ja, det vore väldigt intressant för rapporten.

286. A: Ja, det är ju inget hemligt, våra policys är inte hemliga.

287. S: Finns den för allmänheten?

288. A: Nej, men de är interna, vi har ju klasser som är värre än det.

289. S: Jaja.

290. A: Men vi har rätt att ge er det om det är internt under förutsättning att vi tar ansvar.

291. S: Okej... Nästa fråga har vi väl lite börjat på, men vi kan ta underfrågorna. På vilket sätt utbildas de anställda i säkerhetspolicyn men underfrågan nu då, gällande tillgång till information, Internet åtkomst och användarkonton. Är det några specifika grejer när det gäller dem, eller är det generella...?

292. A: Menar ni gällande vilka accesser de har?

293. S: Ja, vissa anställda kanske har tillgång till viss information för att kunna arbeta som kanske ändå är för känslig för dem, men för att kunna arbeta effektivt så når de den?

294. A: Ja, så har vi det.

295. S: Okej.

296. A: Alltså vi har en rätt bred åtkomst beroende på vart man jobbar nånstans, det är ju inte så att alla har åtkomst till allt men jobbar du nu i det bolaget som jobbar med utveckling och sånt så har du en rätt bred åtkomst till information.

297. S: Precis och då har dom anställda då någon tuffare utbildning vad som gäller säkerhetsmässigt?

298. A: Den är samma.

299. S: Är det samma för alla?

300. A: Det här företaget i Lund består rätt mycket av tjänstemän så det spelar ingen roll om man är där eller någon annanstans. Men dom som jobbar med våra nya projekt tänker hela tiden på sånt på ett eller annat sätt för att skydda. De förstår hur viktigt det är att till exempel skydda en ny maskin som tagit kanske 5-6år att utveckla. Så de har mer awareness i sitt jobb, tycker jag. De får inte specifik utbildning av oss, men de kan ju väldigt mycket mer för de är ofta inne med juristerna i patentfrågor och sånt, och i och med det får de en utbildning också hur viktigt det är att inte klanta innan patentansökan är färdig.

301. S: Okej...

302. B: I våra filservrar, om vi tittar bara på det så finns det två nivåer, det är då publik och så finns det restricted och under restricted kan man ha flera olika restricted folders så att det styr man. Det är någon som äger och tar ansvar för det att vem som ska komma åt det. Man kan sätta projektspecifika mappar om man har projekt A, B, C och D så är det bara projektmedlemmarna som kommer åt dem. Men viss information vill alla komma åt.

303. S: Ja, precis...

304. B: Och i systemen så ger man då...
305. (B stänger av sin telefon som ringer)
306. B: ...applikationerna var det då beroende på vilken information man ska komma åt. Om det till exempel är ritningar så får man accessrättigheter till dem. Systemen kan man ju styra lättare än filservrarna.

307. S: Okej.

308. A: Det förekommer ju projekt överallt här och tillhör man då till exempel "Enhet 1" som är det bolag säkert har mest projekt så ligger det i grunden liksom lång tid tillbaka att man måste kunna dela mellan olika projekt, den kunskap man får till sig som är ny, för att hela tiden förbättra. Så man är ganska öppen med vissa saker, att dela med sig av det som är bra till kollegorna som i ett annat projekt kommer stöta på igen för att inte göra om det, lägga tid på samma problem en gång till. Men sen är det också som du säger att vissa saker håller man striktare på.

309. S: Så då har ni någon slags stor databas med alla tidigare projekt dokumenterade?

310. A: Nja, jag vet inte hur de håller på.

311. B: Det här är väldigt komplext, men om dom har ju... till exempel om det skulle vara innovation eller annat sånt här så delar man och kan söka och sånt inom den gruppen som jobbar med sånt, så man ska få extra mycket ideer och förslag och så. Men det är också restricted access till dem som ska jobba med det, så man vet vem som har varit inne där och man styr vad som får skrivas ut och så.

312. S: Okej.

313. A: Vi har till exempel inget gemensamt dokumenthanteringssystem som vi kan lägga olika säkerhetsnivåer på. Vi har inte det va, utan vi jobbar mycket mot filservrar och på det sättet. Det är många som vill ha ett dokumenthanteringssystem, men det får vänta för vi har hållit på med mycket annat och under många år implementerat ett system till stora kostnader så det är nog inte läge just nu att komma med ett dokumenthanteringssystem. Det kanske kan tyckas lite konstigt, men så är det.

314. B: Vad man tittar då på från globalt håll är sharepoint.

315. S: Okej.

316. B: Det känner ni till?

317. S: Japp.

318. A: Men sexan var information då?

319. S: Ja, precis, det handlar om utbildning i de här tre specifika...

320. A: Alltså vi utbildar inte i hur de får tillgång till information utan det utbildas de på internt. Jag tror inte de utbildas på det utan man får vissa rättigheter beroende på vart man är placerad i organisationen.

321. S: Så de har bara tillgänglighet till det dem...

322. A: De har inte klagat på det.

323. S: Men ändå har ni en ganska bred åtkomst också..

324. A: Japp.

325. S: Gäller det på alla tre punkterna? Internet åtkomst och användarkonton, det är ingen speciell utbildning på det heller?

326. B: Nej, man får väl det och så får man läsa igenom policyn om man inte går på våra utbildningar.

327. A: Men vi har ingen speciell utbildning på Internetåtkomst eller användarkonton.

328. S: Så att de inte ska gå in på de här sidorna och sånt här...?

329. B: Ja, men det säger vi när de är nyanställda.

330. A: Vi har utbildning för nyanställda men då får dem alla de här. (broschyrer) Här står det bland annat hur man ska bete sig på Internet.

331. S: Så det är framför allt genom broschyrer?

332. A: Ja, den utbildningen vi har för vi kopplar den till att vi har PowerPoint slides och så som stödjer det.

333. S: Men det är alla anställda som måste genomgå det för att få lov att använda systemet?

334. A: Nej, man blir anställd här, sen har man naturligtvis en introduktion av sin chef och kollegor runt omkring sig. Sen fångar vi upp dem och har två timmar utbildning med dem efter 3-4 månader senast. Då går vi igenom allt, från brandsäkerhet, utrymning, till arbetsmiljö, till informationssäkerhet och annat. Vi går alltså inte igenom denna (broschyr) utan vi pekar på faran att göra fel kan man säga och kopplar det till realistiska case som har hänt.

335. S: Okej.

336. A: Dagens industri till exempel ringer till oss och säger att ni har en medarbetare som är ute och chattar på dagens industri, skriver saker som vi inte tycker är lämpliga och det tycker säkert inte ni heller. Då letar vi upp den personen och har ett allvarligt samtal med honom och stoppar det. För han skriver ju faktiskt i Företag A:s namn när han är där.

337. S: Precis...

338. A: Eller det är klart att det förekommer att folk har varit för mycket på porrsidor och där är det att de får varning för det, sen kan anställningen ifrågasättas om det fortsätter
339. S: Ja, så det kan förekomma att det tar upp till fyra månader innan de känner till säkerhetsreglerna? Alltså får de lov att använda systemet under de fyra månaderna?

340. A: Nej, det är inte riktigt sant.

341. B: Chefen har ett ansvar, men dem introduceras direkt när man kommer in som nyanställd. Så det är dem som introducerar som har ett ansvar, vi vet inte om de gör det 100 % rätt, men det finns ingen sån här ”du får inte tillgång innan du gjort det här”.

342. A: I samband med anställningen gör man den här interaktiva utbildningen och där är ett kapitel som handlar om säkerhet. Det handlar om brandsäkerhet och det handlar om informationssäkerhet. Det är att medvetande göra dem att hemligheter vi har är viktiga, kan man säga. Sen är det chefen och kollegornas som får se till att det fungerar i vardagen. Men vi kan inte fånga upp alla den första dagen, utan det blir då efter ett par månader.

343. S: Japp, vi kan... 6.4..

344. B: Jag protesterar mot formeringen.

345. S: Är det bara fokus på säkerheten i utbildningarna eller tar ni upp på vilket sätt användarna bör använda säkerhetsreglerna och fortfarande kunna arbeta effektivt?

346. B: Det är därför jag inte gillar den, för det är ett påstående, men det är väl okej att ni påstår.

347. S: Vi skulle kunna stryka det fösta där, är det bara fokus på säkerheten och snarare fråga om ni på nåt sätt pratar om att de även kan arbeta effektivt och samtidigt följa reglerna? Vi tänker framför allt vid en uppgradering, alltså systemen kanske blir mer och mer låsta ju mer tiden går.

348. A: De blir mer och mer?

349. S: Vi tänker att oss det kommer fler och fler hot och vid en uppgradering då, så måste de kanske göra de här grejerna också, för att det ska vara säkert. Har ni då någon utbildning...

350. A: Du har ju utbildning i krypteringsverktyget... till exempel... Jag för står inte riktigt frågan. Det enda jag har märkt under de utbildningar vi haft säger de främst att det tar för lång tid att starta datorn på morgonen och komma in i systemen för det är så mycket som ska uppdateras där, om det nu ska uppdateras. Jag säger inte att det timmar, men ni vet hur det är när man vill på det på det direkt på morgonen så tar det 5-10minuter.

351. S: Ja, precis...

352. A: Det har tagit ännu längre tid i vissa fall, då har man haft någonting i systemet som gjorde att det gick långsamt. Det har man klagat på. Man säger gärna också ibland att det finns alldeles för många lösenord att hålla koll på. Jag vill inte skämta bort det, men här på företag A har vi inte speciellt många lösenord. Det kan var ett par stycket beroende på vad man nu har access till. Men om man nu inte kan hålla reda på tankkort och så vidare så är det ju inte vårt problem. När vi gör gap analyser har vi fått ganska höga staplar på access till datasystemen.

353. B: Ja, det är nästan så att man tycker att de har för mycket access, det är ju det man vill styra. Anledningen till att jag protesterar är att ni här skriver att säkerhet betyder att man jobbar ineffektivt. I vissa fall, som kryptering, det är klart att det krånglar till det.. eller inte krånglar till det men det blir mer arbete för att man måste kryptera filer eller E-post eller annat. Eftersom vi inte har ett dokumenthanteringssystem så då rekommenderar vi hur man ska göra och hur man ska klassificera men tills vi inte har något annat, så måste vi guida dem hur de ska göra manuellt, alltså i systemen. Man får alltså inget tekniskt stöd för att märka eller något sånt. Jag vet inte riktigt något annat här.. det som det klagas mest på är bristen på dokumenthanteringssystem

354. S: Okej… Ser du att säkerhetspolicyn till och med kan göra att de arbetar mer effektivt?

355. B: Om man gör för strikt säkerhetspolicy så stänger man och det krävs mer av varje användare. Det som är viktigt är att om man skriver en säkerhetspolicy måste man ha tekniken som stöttar en. Till exempel med vårt krypteringsverktyg så säger policyn att vi ska kryptera allting om vi nu har det via E-post på hårddisken eller servern som är highly confidential, den högsta klassen. Då är verktyget vi har inte riktigt optimalt för att dela dokument på servern och det gör att det kan bli väldigt tidskrävande och då är det inte effektivt längre. Då tittar vi efter ett annat verktyg så jag tror att det är viktigt att man tittar på vilket verktyg man har när man ska skriva en policy så de anställda inte bryter mot policyn för att det blir för jobbigt, för att det tar för lång tid.

356. A: Sen är det så här att bekvämlighet och säkerhet inte går ihop, antingen har man det enda eller så har man det andra. Det kan handla om rotationstimmarna, ID-korten eller vad du vill, så är det ju. Det tycker jag nog att man förstår här. I början tycker jag nog inte att man förstod det, långt före min tid, då blev de jätteupprörda när man införde rotationstimmar här. Då kom man inte in med resväskor.

357. S: Ja, precis.

358. S: Effektiviteten bromsar säkerhet?

359. A: Nej, Jag säger bara att det inte är självklart att säkerhet och bekvämlighet går ihop. Jag sa bekvämlighet!

360. S: Aa jo, jag hörde inte riktigt och det var därför jag frågade.

361. A: Jag sa inte effektivitet.

362. S: Skulle jag bara kunna sen ställa en fråga. Mäter ni effektiviteten på något sätt?

363. A: Vi mäter inte det.

364. A: nej.

365. A: Säkerhetsavdelningen mäter inte det, men man mäter säkert det där ute.

366. B: Det enda gången man tar upp, tror jag, eller kanske inte men den gången man tar upp effektiviteten gällande datorn. Är om man vill göra någon förändring i IT-miljöer eller ta något nytt system så måste man ta fram något som heter här ”Systemnamn” och i ”Systemnamn” kan man oftast ta hur mycket tid varje användare kan spara genom när man tar fram ett nytt system. Så det kan i sin tur att vi kan spara såhär mycket tid då det här systemet gör det så här mycket effektivare.

367. B: Då är detta direkt kopplat till effektivitet och pengar kan man säga.

368. B: Så det är ett sätt att visa att vi har sparat tid här.

369. B: om nu vi svarat på frågan.

370. B: Nu kan man beräkna med sådan tid när det gäller effektivitet eller?

371. S: Men det låg utanför er, ni fokuserar bara på att göra det så säkert som möjligt?

372. B: Det är fel formulerat. Vi försöker inte göra något så säkert som möjligt utan vi försöker göra det till en möjlig risknivå.

373. S: en rimlig risk nivå?

374. B: eller till den risknivån som vi har är acceptabelt.

375. B: Nu är det lite så ord.. Vilket vi ska säga. Vi försöker inte göra detta till Fort Knox.

376. A: Vilket hade varit hur lätt som helst.

377. S: Men då hade också effektiviteten försvunnit.

378. B: Ja, vissa risker måste vi kunna ta.

379. A: Men vi mäter alltså inte effektiviteten av säkerhetsåtgärder. Det är policy och vägledning som styr det och riskvärdering m.m.

380. A: Utan då funderar vi på att vi inte kan göra det hur jobbigt som helst för våra olika användare för olika saker.

381. A: Men det är inte det som mäter effektivitet utan bolagen mäter effektivitet på allt möjligt. De mäter alltså tidplaner, kostnader och allt möjligt, inte kopplat till IT speciellt.

382. S: Men ni har alltså inga egna kontroller på att mäta effektivitet? alltså ni väljer när ni gör er riskanalys..

383. B: Nej, inte vi. IT bolaget mäter sin egen effektivitet (nertid, snabbhet vid service desk etc.)

384. S: ...för att se att nu har vi satt lite för hög säkerhet och det tar alldeles för lång tid att utföra vissa uppgifter?

385. B: Ja

386. S: De accepterar det?

387. B: Jag ska förklara.

388. B: De vi frågar är det att om de känner till vilka regler som finns...

389. B: ...och sen frågar vi om de följer dem, regelverken. Och då kan man få kommentarer och då kan vi fråga: Varför gör ni inte det?

390. B: Så där får vi veta lite men inte exakt om effektivitet.

391. A: Men det är inte vi som ger ut policy alltså, den som ger ut policyn får i så fall fundera på det.

392. A: Men jag är rätt säker på att det är så att man ser på om detta kommer att störa alla användare.

393. A: Jag är också rätt säker på att man gör tester i grupp först innan man implementerar det till alla.

394. A: Så först en testperiod av både det ena och det andra och sen implementerar man. Har man bestämt sig för att det ska vara kryptering då gör man på det sättet. Utvecklar verktyget sen implementerar det i en testmiljö och sen till alla.

395. A: Och utbildning.

396. S: På det sättet regleras det genom att ni har en testperioden först och användare klaga, att vi tycker det här går för långsamt.

397. S: Okej då har vi kommit fram till det vi tänkte.

398. S: Ja vi kanske kan börja detta är en fråga som vi kan hoppa över och ta nästa iaf. Sjuan: Bygger ni er säkerhetspolicy efter något specifikt ramverk?

399. S: Det har vi kanske redan pratat om.

400. A: Ja det är ISO standard.

401. S: Det är ISO standard?

402. S: Åttan?

403. S: Ja vi tog åttan nog att om de är delaktiga vid implementationen av säkerhetspolicy och hur det påverkar slutresultatet och då har ni någon slags testperiod först...

404. A: Inte vi.

405. S: Inte ni men någon annan. Det finns en testperiod.

406. A: Ja

407. B: Ja Jag nämnde lite där om kryptering innan att det är ett verktyg som inte var helt...

408. A: Är vi inte på sjuan?

409. B: ja det enda jag har tänkt säga är att det finns vissa fall som man hade önskat sig att det hade gjorts lite bättre.

410. B: När IT-avdelningen tar med sina testgrupper. Då hade kanske kunnat ta med lite fler av vanliga användare än att enbart konsultera med sina datakollegor som är lite mer dator vana.

411. S: Så det är dem på avdelningen som gör tester också?

412. B: Ja de gör testerna och går det som det ska har de en användargrupp som är lite mer ovana.

413. B: Men just i krypteringsfallet så fanns det en viss brist.

414. S: ”Svammel”

415. S: Det med feedback från personal, skulle ni anse det vara en stor faktor till att det blir en bra säkerhetspolicy eller ett bra förarbete till en säkerhetspolicy?

416. B: Ja. absolut på hur det funkar eller inte . Det står i policyn att om man har synpunkter så ska man framföra det så att man kan göra förbättringar av policyn.

417. S: Vi har just läst det att feedback är bland nyckelfaktorerna för säkerhetspolicyn.

418. B: Absolut. Om ingen säger något utan alla bara håller tyst så blir det inget förbättringsarbete.

419. A: Den där. Det är den som gäller alla användare. Policyn och proceduren är på 50 sidor. Det är ingen vanlig användare som läser den. Utan den är också en sådan som vänder sig till mig som användare i IT-avdelningar eller till IT-systemen ute i världen.

420. A: Och hur de ska hantera det ena och det andra. Det sagt så menar jag. Jag förstå att det är bra med feedback. Om man bygger upp det under en viss tid så måste man få in det ganska snabbt också. Därför att vad ska vi säga Det är faktiskt inte så länge sedan, mitten av 80 talet fanns det knappt några datorer, höll jag på att säga, sen allting rusar iväg och då rusar också problemen iväg, säkerhetsproblemen och då måste du se till så att du får plats på alla dessa 50 sidorna

421. A: I tekniska system och annat. Du kan inte gå ut och fråga varje man om vad de tycker. Det kommer så fall i nästa generation.

422. A: För i början har man nästan ingenting.

423. A: Och sen upptäcker man nej här finns säkerhetsluckor överallt. Och jag vet inte vilket år vi är då på men då kommer vi med dessa 50 sidorna och det är det här som gäller. Man går inte ut och frågar alla även om jag inser att det är bra.

424. A: Men också tror jag faktiskt att det har med lojaliteten att göra. Man klagar inte helt enkelt

425. A: Kanske ni kommer fram till något annat

426. B: Men tänkte bara säga att IMSO:na har också en roll som information manager security officers

427. S: Ja vi hoppar lite för vi har lite andra viktiga frågor som vi vill gå igenom. Men vi kan ta elvan först också. Om det är något ni vill tillägga som kan påverka effektiviteten. Effektivt användande av säkerhet.

428. B: Ett dokumenthanteringssystem hade det underlättat, bättre krypteringssystem och att man kan dela krypterade filer med varandra på servern.

429. A: Och dokumenteringshanteringssystem som gör att man inte kan release det du har gjort om du inte har klassificerat det.

430. A: Bättre accessrättigheter, kunna göra dem mer differentierade.
431. B: Ja

432. A: Det är för tungt att göra differentiering till olika grupper med olika accesser.

433. S: Det är saker ni arbetar med för att effektivisera

434. A: Nej det gör vi inte, det gör vårt IT-bolag.

435. S: Då hoppar vi till hantering av användarkonto. Dessa är lite mer specifika frågor, kanske lite snabbare frågor. Mer hur det fungerar praktiskt, vi har säkert gått in på det en del.

436. S: Vilka är de valda metoderna för de olika inloggningarna av informationssystemet? - flera lösenord?

437. S: Ja inloggning med en slags dosa om man har någon sådan säkerhetsdosa?

438. B: Hemifrån på distans.

439. A: Lösenordet måste också väljas enligt policyn.

440. B: Ja

441. A: Även om du byter det får du inte välja vad som helst. Utan du måste välja ett som består av siffror, tecken, gemener

442. B: Åtta tecken. specialtecken, stora och små bokstäver

443. A: stora och små bokstäver, tre av dem och åtta av de andra. Är det inte det så tar inte systemet emot det.

444. S: Men de får själva ändå välja sitt lösenord?

445. B: Ja.

446. B: Det är till filserverna. Hemifrån är det med Secure ID,en VPN lösning som är krypterat med engångslösenord och användarnamn. Alltså användarnamn och lösenord.

447. A: Ja och programvara i datorn

448. B Så det måste vara den datorn de loggar in med.

449. S: Har ni krav på att de har olika lösenord mellan och i olika system eller de kan använda samma lösenord hela tiden?

450. B: Olika.. vi har ingen "singel sign on", här i Sverige i alla fall.

451. S: mm okej, är det likadant på en lokal dator om man sitter på en klient om de har tillgång till olika system till ex. ett ekonomisystem eller någon annan del eller har ni olika lösenord där också?

452. A: Nej, samma.

453. S: Samma i en klient?

454. A: Ja det är inte riktigt sant, det beror på vad du menar med ett ekonomisystem?

455. S: Alltså om de loggar in på en klient så loggar de bara in på med ett lösenord och då har man tillgång till vissa grejer.

456. A: men om vi hör med ”intervjuperson B”, om jag loggar in på min dator så har jag det lösenordet för att komma in ”användarnamn” sen ett lösenord, det är som jag sa innan. Sen har jag vilket också andra kan ha att jag har även lösenord till andra säkerhetssystem där jag har en annan inloggning, och med ekonomiuppföljning har jag med ett annat lösenord. Jag har till ”system1”

457. S: och de, stängs de av efterhand om du inte är aktiv? ex. om du inte är aktiv efter fem minuter loggas du ut då?

458. A: två av dem, säkerhetssystemet och ”System1”. ”System1” blir lösenordet ogiltigt om jag inte har varit inne på tre månader.

459. S: Ja, det var en fråga här också så ja. tvåan: Hur ofta byter ni lösenord?

460. B: till nätverket ”system2” så är det inte tvingande lösenordsbyte, man rekommenderar att man byter det när man misstänker att någon har fått ta del av det.Det är då lösenord som ”intervjuperson A” sa innan och sitt lösenord.

461. B: Till ”System1” är det oftare. Jag tror det är en gång i månaden. eller?

462. A: Ja en gång i månaden. Vi är en av tron, även den som skriver globala policyn, IT, i alla fall han som gjorde det innan. Att det är bättre att ha ett bra lösenord och hålla tyst om det än att byta lösenord en gång i månaden för då blir det bara en åtta eller nia i slutet.

463. A: Så tror vi.

464. A: därför så är det så.

465. B: Så det är väldigt olika, om man tittar på tvåan och inte byts. Eftersom ni inte vet hur det ser ut och vi bara pratar om några stycken, men vi har hundratals system och applikationer. Därför kan vi inte säga det exakt just nu. Så tänk på sen att när ni formulerar frågorna ni måste vara rätt specifika med vad ni är ute efter det allmänna. De får frågan och svarar för ett helt annat system och då kan det vara svårt och sammanställa det. Eller så väljer ni något specifikt som ni vill fokusera på som ni tror att alla har.

466. B: Eller ni kan maila mig era frågor om det är något ni är osäkra på. Så det inte blir att den ena svarar för det ena systemet och en annan för ett annat.

467. S: Ja då om en användare glömmer ett lösenord, hur hanterar ni det då?

468. B: Man kontaktar alltså vårt IT-bolag där man har vissa rutiner för att få tillbaka sitt lösenord

469. S: Är det även där man ringer in och har möjlighet att svara på de frågor som du sa innan. de frågorna som är personliga?

470. B: Ja precis, man kan välja vilken man vill så hjälper de en. Så blir det en motidentifiering så det är inget man bara ringer in och säger att man vill ha, utan det finns en hel procedur som måste följas.

471. B: Så det är säkert

472. S: Kan det ta lite tid då?

473. A: Nej det tror jag inte, de tar det direkt. Nu vet jag inte om de kan ta över datorn om de behöver hjälpa till.

474. B: Nej jag tror inte de behöver det för de har redan det nersparat på servrarna.

475. S: Vilka behörighetsnivåer har ni?

476. S: Sexan kan vi stryka, den har vi redan gått igenom. fyran också

477. B: Är fyran av de olika.

478. S: femman också har vi diskuterat. Om anställda måste ha flera lösenord

479. B: Det har vi svarat på sexan! att vi har mycket utbildning

480. S: Och sjuan också.

481. B: Ja åttan är kopplat till den gröna informationsklassificering som är obligatorisk

482. S: De får dem genom utbildningar?

483. A: Det får man hela tiden...

484. S: Är det något man själv måste ta av eller är det utskick?

485. A: Av dem?

486. A: Alla får dem på våra utbildningar, nyanställda får dem och de kan ta här då det finns en hel bokhylla fylld.

487. S: Då kan man i alla fall inte säga att man inte sett dem

488. B: Nej, och dem finns på vår hemsida

489. S: om man tänker till nyanställda får de, som ni sa har ni många med lång erfarenhet i företaget. Får de nyutbildning och blir kallade på något sätt?

490. B: Ja

491. S: för att uppdatera sig..

492. A: Dem får nyheter med broschyrer. Nyanställda får alltihopa och får ta hem och läsa över helgen.

493. A: Men all informationssäkerhet är det mer, workshop liknande historier där man blir engagerad i det.

494. S: Du sa något där via vardagen? sen hörde jag inte riktigt vad du sa, ni skickar information...

495. A: Ja i vardagen sitter man och kollegor emellan och diskuterar, inte varje dag men då och då. Nu har vi detta dokumentet till detta projektet och vad vi ska klassificera det till

496. A: Och så blir man överens om att det här är "highly confidential"

497. B: Ja

498. A: Så funkar det också och det är också en form av utbildning.

499. S: Så sen är det nian om mail men det går också lite in i Internet.

500. B: Ja det finns e-post policy även en svensk e-post policy kopplat till den globala. Vi har även en specifik policy för Sverige. Den tar upp mer praktiskt att man inte ska skicka det mitt i natten eller helgen och lite sådana saker, mer arbetsmiljö.

501. S: tas det här upp på utbildningar eller bara via.. ?

502. B: Det tas upp, vi har en speciell e-postutbildning som inte vi håller i, där det går igenom och lär hur man ska hantera Outlook. En Outlookutbildning

503. S: Kan vi gå in på tillgång till Internet?

504. S: Ettan handlar då om vilka sidor som är spärrade.

505. S: Vilka är era förebyggande arbeten med Internet användningen men det har nu redan svarat lite på?

506. B: Hur tar ni reda på vilka sidor som är spärrade? Det får man reda på när man söker annars blir användarna informerade om de inte vet in vilka som är spärrade.

507. S: Vi tänker mer på er del, hur vet ni om att t.ex. Facebook ska vara spärrat, för anställda använder det för mycket?

508. A: Det är inte vi som bestämmer om vilka sidor som ska spärras. Det är vårt dotterbolag som bestämmer i den frågan.

509. S: Dem bestämmer vilka sidor som inte får användas?

510. A: Än så länge får vi vara på Facebook. Det handlar främst om att pornografi och annat som användarna inte får gå in på. Det är de sidorna som är spärrade.

511. S: Hur uppdaterar ni alla spärrningar av hemsidor?

512. A: Det är en tjänst som man köper där man får en uppdatering av sidor som ska vara spärrade.

513. S: Men det är inte några sociala medier som är spärrade? alltså sidor som inte är kränkande på något sätt.
514. A: De är inte spärrade än. Vi har precis fått nya guidelines till delar av organisationen.

515. S: Nyhetssidor och liknande är de spärrade?

516. A: Dagens industri och nyhetssidor får vi vara inne på i en rimlig omfattning så det inte påverkar arbetet.

517. B: Sidor som Flashback och liknande är inte tillåtet.

518. S: Är de spärrade?

519. B: De är spärrade.

520. S: Är det tillåtet att gå in på sin privata Hotmail och sådana sidor?

521. B: Det är tillåtet

522. S: Hur ser då den säkerhetsrisken ut när anställda öppnar sina email, sin privata mail?

523. B: Då finns det många olika antivirus program som dels finns på Internet Gateway och dels på klienterna. Det finns program som är oberoende och består av en mängd olika filter som filtrerar data (informationen går genom 7 filtreringar).

524. S: Det finns ingen risk då för det täcker av om någon skulle öppna ett privat mail?

525. B: Ja. Sen så styrs hanteringen av mail från säkerhetspolicyn som säger att man ska hantera mailen på rätt sätt och framför allt inte öppnar mail som kommer ifrån okända personer.

526. B: Vad menar ni med sharelinks?

527. S: Det vi menar med sharelinks är exempel på Twitter, Facebook och Youtube.

528. B: Sociala medier är som sagt okej att använda men det är inte tillåtet att använda sig av nedladdningsprogram som torrents. Allt som har med att nedladdning där man måste dela med sig av sin hårddisk är inte tillåtet.

529. A: Men sidor som Facebook kommer troligen att förbjudas.

530. S: Det är något vi kan tänka oss att det kan ta mycket arbetstid från era anställda.

531. S: Så ingen form av nedladdning är tillåtet?

532. B: Nej, ingen nedladdning är tillåten. det är bara administratören som kan tillåta en sådan sak och allt går igenom ”IT-partner 1” och det är där ifrån vi också beställer vår mjukvara som ska vara godkända. Sen görs det också av-checkning där man går igenom och så man ser så inte någon har installerat något som inte får finnas eller har licenser.

533. A: Detta körs igenom varje morgon och ser över så att det inte finns något felaktigt program.

534. B: Är det någon extern som kommer med sin dator så skannas den.

535. S: Finns det andra risker med Internet?

536. B: Det finns så klart virus och det gäller också att man inte skriver någon information om företaget när man besöker sociala medier.

537. S: Hur är det med uppdateringar, man upptäcker själv att man inte kan gå in på en hemsida?

538. A: Det beror på men troligtvis går man ut med informationen om det är något som berör flera.

539. S: Så endast vid stora besökta sidor och där man inte kan vara säker på om de är spärrade?

540. A: Ja, alltså vid förändring så går man ut och förklarar varför.

541. S: Nu kommer en sidofråga, loggar ni era anställda?

542. A: Alltid, i allt de gör så loggas dem.

543. S: Så ni vet om det är någon som försöker komma in på en sida flertalet gånger?

544. A: Vi loggar allting men det vi kontrollerar vid användning av internet är vilka som är de mest besökta sidorna. Så om det vore att något inte är bra så går vi inte på individnivå utan det blir mer ett problem för alla.

545. S: Så om ni upptäcker någon?

546. B: Vi kan om vi vill om det finns någon misstanke.

547. A: Förekommer det någon olaglighet så finns där procedurer att då tar man in facket och jurister som löser problemet.

548. S: okej. men så det är något mer ur en juridisk synpunkt att ni som ett företag måste logga era anställda?

549. B: Det måste vi inte men det kan också vara en trygghet för de anställda som inte begår något fel. Då kan de känna sig fria om vetskapen att de inte har gjort något fel.

550. A: Vi ser inte på den enskilda individen utan vi ser enbart till hur mönstret ser ut på Internet.

551. S: Ser ni bara på loggarna om ni misstänker att någon gör något fel?

552. A: Om det finns en stark misstanke om att någon begår olagligheter eller om något inte är förenligt med ”företagsnamn”. Kan man gå in med vissa procedurer.

553. A: Det är faktiskt information som tillhör ”företagsnamn” och det är inte något som tillhör den enskilde.

554. S: Vi hoppar till nästa fråga för vi har ont om tid. Åttan, Enligt ramverk av implementationen av säkerhetspolicy krävs det feedback? Detta är något som vi har läst från litteratur att det är något som krävs vid en säkerhetspolicy. Går ni ut till användaren och fråga dem?

555. A: Det är något vi är dåliga med.

556. S: Ni tycker inte att ni har tillräckligt mycket kontakt med dem?

557. A: Nej det tycker jag inte.

558. B: Nej, men det är inte vi som skriver policyn.

559. A: Inte för att vi vill beskylla dem för det men jag personligen tycker inte att man kan ha för stor feedback från användaren.

560. A: Det kan bli så att om man får in en mängd problem i form av feedback om någon inte får sitt svar besvarat kan det leda till något negativt. Alla vill troligtvis som skickar in få svar på sitt problem. Därför kan jag tycka att det inte är bra. Det är så att många tycker samma sak.

561. S: ”går igenom frågorna och upptäcker att vi har reda fått dem besvarade i tidigare frågor, så vi går vidare till övriga frågor”

562. ” slutligen hittar ”intervjuperson B” en fråga som inte har blivit besvarad tidigare ”

563. B: Är det någon del i er policy som begränsar mest? Det är då informationsklassificering det nya sättet som gör att det blir mer byråkratiskt. Man måste tänka på det och då kopplas stor del av säkerheten åt det. Till exempel access rättigheter, hur man får sprida det med sekretessavtal och märkning.

564. B: Det gör att man inte kan göra vad man vill.

565. ”går vidare till en annan fråga om det händer att anställda går runt säkerheten för att öka tempot i arbetet”

566. B: Det kan hända man kanske inte märker att man gör det.

567. A: Jag tror inte att man går runt den för att det är smidigare, utan det är i så fall mer av okunnighet än att man gör det för att det är smidigare.

568. B: Eller för det kan förekomma att man är slarvig och vill att det ska gå fortare.

569. S: Kanske att det är mer bekvämt?

570. A: Ja.

571. B: Även att saker och ting går väldigt fort och man kanske måste svara inom en timme eller rent av inom tio minuter. Då kanske det händer att man inte kommer ihåg vilka regler som gäller.

572. S: Sjuan och åttan har vi redan fått svar på.

573. B: Tian: det vi gör är att vi har våra utbildningar där vi har ”metodnamn1” och berättar vad policyn står för men det är inte vi som skriver reglerna. Vi kan bara ge dem feedback till dem som skriver policyn. Ex. att man säger att det här fungerar eller det här fungerar mindre bra.

574. S: Okej. Jag tror vi har gått igenom alla frågor nu.

575. A: Något som jag inte nämnde sist vi sågs var att ”företagsnamn” tekniska system är alldeles utmärkta. Jag tror inte heller att de stör användarna i någon bemärkelse. Det är något som de får svara på men jag tror inte det. De är hur bra som helst medan policyn, de mer mjuka ex. klassificeringen. De stödjer inte att vi har gått ut med policyn innan vi har teknik som stödjer det. Och där har vi ett antal som genomskådat det av dem anställda. Att de kanske tycker, menar man verkligen allvar med den här policyn så måste man också ha ett tekniskt system bakom som kan underlätta för oss att följa den. Ex. på system då kan vara att man ska kunna enklare klassificera och dokumenthantering.

576. B: Ja

577. A: Alla system går inte att klassificera i efterhand.

578. S: Okej.

579. A: Då kan man säga att det läggs rätt mycket i knäet på användaren. Dels kan det vara så att en användare får arbeta med något som den tycker är rätt jobbigt till förhållande vad som skulle kunna finnas. Det kan göra så att man i vissa lägen tar en annan väg som är smidigare om det nu är så att man har bråttom.

580. S: Okej, ja då kan vi titta på exempel på enkätfrågor. Detta är på ett ungefär vad de ska handla om och hur vi har tänkt att de ska se ut.

581. A: Varför tycker ni att Internet access är så viktigt?

582. S: Det kan handla om saker som den anställda inte är riktigt säker på hur de ska göra eller betyder eller handlar om. Ex. om man är ny så kan jag tänka mig att det kan vara bra ex. om man vill kolla på på Wikipedia.

583. A: Så då blir det specifika frågor. ex. men så står det bara Internet access så kan ja tolka det som att på arbetstid kan jag surfa på Internet. Frågorna måste vara lite arbetsrelaterade som ni ställer.

584. A: jag är helt medveten om att man kan ha nytta av olika translation’s och Wikipeda, man kan ha nytta av väldigt mycket men det finns också mycket annat som man inte har nytta av.

585. A: Det läggs nog också en hel del tid på det och det är något som vi inte ska ta fram här.

586. A: Vi ska inte understödja att det läggs arbetstid på saker som inte tillhör arbetet.

587. S: Nä precis. Det ska vara arbetsrelaterade frågor

588. ”Diskussion mer om vilka sidor som kan vara okej att vara inne på men det är sådant som redan har diskuterats tidigare.”

589. S: Det vi vill fråga är mer hur de upplever det med Internet access.

590. A: Kommer ni nämna effektivitet? Man kan ha olika uppfattningar på hur man mäter effektiviteten. Vi gör det inte men It bolaget mäter troligtvis effektiviteten på många sätt.

591. S: Visst finns det många sätt att mäta effektiviteten på.

592. A: Så det kan vara bra någonstans i formuläret att ni beskriver vad ni menar med effektiviteten.

593. S: Alltså introducerar vad vi tycker att effektivitet är för något..

”Vidare är avslutning av mötet”

Bilaga 4 Transkribering, Företag B, expertintervju

S = Student

A = Informationssäkerhetsansvarig

1. A: Till en början har ni valet att välja att företaget ska få vara anonymt men det bidrar att kan lämna mer öppen information än om det är så att företaget kommer presenteras i er uppsats.

2. S: Det vi har valt är att hålla allt anonymt för vi använder oss av fler företag och det är den bästa lösningen för att kunna skriva om mer detaljerad information i uppsatsen.

3. A: Det är helt okej med oss att vi är anonyma. Men om vi börjar med ert underlag så ska vi se hur vi ska lägga upp intervjun.

4. S: Vill ni att vi gå igenom våra intervjufrågor först?

5. A: Det kan vi göra om ni inte vill ha en liten presentation av vad "företag B" sysslar med och vad vi är för ett företag? Det jag gör är att jag sitter på "Enhet 1" där jag arbetar med de länder som tillhör norden och Polen. Sen finns det personal som mig, som skriver runt med papper och datorer. Min roll är då att vara en corporate information manager på "Företag B" och arbetar under företagets CIO.

6. S: Okej då har vi fått det grundläggande om er. Vi har gjort en dagordning men det är inte säkert att vi behöver hålla fast vid den. Är det några oklarheter gällande undersökningen som vi har tänkt göra?

7. A: Jag har fått lite information, jag har hört att ni var systemvetare? Samma som mig och läste i Lund liksom ni och läste kandidat och master.

8. S: Det vi har tänkt är att vi gör en intervju med dig här och nu och sen på en lämplig avdelning som du tycker är bra. Om vi kan lämna ut enkäter som gäller effektivt användande.

9. A: Det är alltid en balansgång mellan säkerhet och effektivt användande. Har ni hört om triangeln där man ser hur säkerhet, kostnad och funktionalitet påverkar varandra. Lite beroende på vilka preferenser man har, men i mitt fall så sätter man säkerheten högst upp. Skulle det vara personal från ekonomiavdelningen skulle kanske kostnad vara det främsta. Utifrån triangeln kan man se att hög säkerhet kostar både pengar eller funktionalitet. Det blir alltså begränsningar av användarna vill göra. Kanske också ska nämna att jag inte sitter på IT, utan jag sitter på "Riskavdelningen". Det vi gör är att stå för alla kostnader om det skulle hända något och detta är något man kan göra om man är stor och har gott om resurser. Vi tar alltså väldigt allvarligt på om det skulle uppstå problematik eftersom företaget själv tar på sig kostnaderna. Detta gör att om något skulle hända blir det väldigt konkret i kassan. Alltså vi försäkrar både hårdvara och de "mjuka delarna" än andra företag som enbart försäkrar hårdvaran och man ser bara till riskerna på dem.

10. S: Frågorna vi har gjort har vi markerat med fetstil de som vi tycker är viktigare än de andra, ska vi gå igenom de först eller börja från början med organisationen?

11. A: Vi har alltså då en vi är en global organisation som finns i många länder i Europa med ett huvudkontor. Vi ligger just nu i ett transformationsskede vi går från en geografisk organisation till den funktionella organisationen. Jag arbetar inom den geografiska organisationen och allt som har med det geografiska inom norden och Polen ska gå igenom mig. När vi går över till funktionella så innebär det att man arbetar mer

med funktioner oavsett om det ligger i norden, Polen etc. så tillhör det samma organisation och distributionen. Delar av de länder som företaget är i är med elhandeln och när det väl kommer till oss vet jag inte vad som kommer hända. Något som är speciellt med vår organisation är att den är väldigt lagstyrd och lagreglerad. T.ex. kan man säga att tillståndet att bedriva/köra kärnkraft finns inte här men på själva kärnkraftverket. Det är alltså de som tillhör kraftverket och då kan man inte flytta styrningen till huvudkontoret då de inte får styra själva kraftverket. Det är lite andra områden som är liknande där har man då behållit det sättet att styra. Det kommer alltid finnas ett behov av lokalstyrning och därför tror jag att vi kommer finnas kvar här i Sverige. Min uppgift är ju att säga till huvudkontoret att de här lagarna fungerar här men inte dessa. Alltså de lagar som funkar för den svenska marknaden behöver att skrivas in i den globala policyn för företaget.

(informationssäkerhetsansvarig visar upp en pärm som tydligen innehåller företagets globala policy)

12. S: Kan man då säga att organisationen har en antydan på en hierarkisk organisationsstomme?

13. A: Jag skulle snarare vilja säga att den är en matrisorganisation, just nu. Sen har vi IT som är ett separat bolag. Det vi gör är då att vi sitter och ställer krav på IT-organisationen så de lever upp till dem. Så det är inte vi som köper in utan det är vi som säger vad som bör finnas i det som de köper in.

14. S: Är det form av utbildning ni har med dem?

15. A: Nej det vi gör är att ställa krav på dem ex. att det måste finnas en brandvägg eller det får inte komma in spam i användarnas brevlåder. Sen när vi kommit överens så säger jag åt dem att gå ut och köp systemet.

16. S: Men om vi ser till våra enkätfrågor. Är det någon specifik del i företaget som du tycker är mest lämpad för vi har avgränsat oss till olika delar?

17. A: Det kan vi ta upp senare när vi kollat över frågorna...

18. S: Ja, precis... det vi vill avgränsa oss till är att se ex. hur personal får sina uppdateringar på sina datorer.

19. A: okej. Om vi börjar med att det tas fram en gemensam policy för hela gruppen och författas på huvudkontoret. Sen kan man lägga till lokala regler som vi har här i Sverige. Dock får vi aldrig understiga de globala reglerna enbart överstiga dem. Detta är vad jag sysslar med, att skriva den nya säkerhetspolicyn eller tillägga. Det skriver jag till kommittén där vi sitter med informationssäkerhet tillsammans med alla andra riskområdena så som brandingenjör etc. För att sen utge den säkerhetsinformationen som uppges ifrån kommittén är det vi som skickar ut i organisationen. Vi har alltså ett intranät där alla regler publiceras även den globala policyn i sin fulla helhet. 20,16 Men detta dokument är knappas begripligt för någon som inte förstå IT termer dvs. en vanlig användare har inte så stor användning av den.

20. S: Har alla i företaget tillgång till dokumentet?

21. A: Alla har tillgång till det. Alltså alla personer i företaget har tillgång till den men skulle tippa att det är ungefär 10 personer som har läst den. Det vi inom företaget har varit överens om är att policyn ska vara så detaljerad som möjligt. Men jag har alltid hört att en vettig policy ska inte omfatta mer än en sida. Men i en verksamhet som är van att vara väldigt reglerad och detaljstyrd då fungerar det inte att komma med en övergripande viljeinriktning som säger att vi ska vara säkra. Det är ungefär vad man får plats med på en sida och då fattar de inte att de ska göra något. Vår policy följer ISO 27001 och den är organiserad på samma sätt. Så alla avsnitt som finns med i ISO finns också med i vår policy men det vi har gjort är att vi har skrivit in under alla rubriker hur vi gör i vår organisation.

22. S: Så ni har helt enkelt utvecklat policyn utifrån ISO standard till er egen?

23. A: ja, vår är också lika tjock som ISO men den är fylld av våra egna ord. Detta har vi gjort bara för att man ska känna igen sig i hur det brukar vara i styrande dokument utifrån verksamheten. Tar man och tittar på föreskriver som gäller elektriker så ser man att de är rätt detaljerade. Detta är ett problem inom informationssäkerhet då många tyckte att man inte såg att där fanns problem och man trodde inte att det fanns något problem i heller. Det var inget man behövde tänka på och då behövde man inte tänka på det ihäller. Denna är antagen av ledningen i norden och de förstår att som den är skriven kan inte en vanlig användare läsa och förstå. Den är skriven ungefär som en lagtext, för att förtydliga saken så, IT-personalen kan i regel läsa policyn och förstå den. Den är skriven för en redan utbildad och kompetent användare men de användare som den riktar sig mig då lyfter vi ut den informationen som är till för dem och skapar användardokument för dem.
Här gör vi många olika sätt för att användare ska förstå policyn, allt från PowerPoint, lat hundar, ex. vi har en bild som fångar hur man får lov att hantera USB-minnen. Den bilden behöver man inte ens vara läskunnig för att förstå de den då bilden visar massa streckgubbar mm. Vi har en befintlig användarutbildning. Jag har arbetat snart i två år för att ta fram denna utbildningen då det är format som ett datorspel där användaren rör sig i företagets lokaler och utsätts för olika uppgifter som man ska lösa på tid. I spelet blir man lurad av en lärling som ibland kan vara god och ibland inte lika hjälpsam. För att efterlikna verkligheten då ibland kan det förekomma att en medarbetare tror sig veta svaret till problemet men i själva verket inte gör det men ändå hjälper till. Lärlingen ska då ta rollen som en medarbetare. Detta spel är meningen med att alla samtliga medarbetare ska ta sig tid och spela igenom. Och det tar ungefär en timme för att spela igenom.

24. S: Vad händer då om någon inte klarar spelet?

25. A: Det är lite olika från land till land men här i norden har vi satt att de som inte klarar av spelet inte skulle få access till nätet men det var för hårt straff så om de inte klarar de kommer de inte få tillgång till fjärraccess. Så vill man ha möjlighet att sitta och arbeta på distans så ska man vara godkänd från våran utbildning. Detta gäller även alla konsulter och detta efterlevs. Ser ut som att detta kommer bli sanktion på den globala nivån. Sitter man internt men inte klarat det så får användaren påminnelse varje gång de går in på internet t.ex. Det är ju så, jag satt och spelade igenom spelet med min dotter och efter jag översatt engelskan så klarade hon många delar bara med sunt förnuft.

26. S: Vi kan fortsätta med frågorna fem och sex. hur är er generella syn på effektiviteten och hur mäter ni effektiviteten?

27. A: Vi har "effektivitetsmätning" både på IT och på rena säkerhet. Några av dem är jag inte så jätte lycklig över men man kan mäta på regelutfyllnad och vi mäter på insidenter. Inspektioner på alla stora anläggningar som får besök var tredje år men de lite mindre kanske det dröjer innan de får besök. vad man gör är att man utför fysisk kontroll av att det ser bra ut i lokalerna men också att man ställer frågor till anställda utifrån policyn. Från IT-sidan så får vi trafikljus rapporter månadsvis på incidenter som vi har delat upp i olika kategorier. sen mäter vi på patchar då alla viktiga patchar måste användaren uppdatera senast fem dagar efter den släppts. Sen kan man också göra stickprovs mätningar, där jag senast begärde ut för att se hur många datorer vi har det senaste operativsystemet och de senaste versionen. Det är mer att kontrollera våra användare för att man ska kunna ställa krav att skaffa fram den rapporten ex. har de bara ordning och reda efter de krav som vi ställer. Vi äger också vårt eget outsourcingbolag, det heter "outsourcingbolag" men de är form av leverantör åt mig och jag ställer krav och begär rapporter för att se så de har allt som de ska.

28. S: Där fick vi bra svar. Ska vi gå vidare till frågor mer gällande säkerhetspolicy? Det vi har valt att fokusera på inom säkerhetspolicyn är Internet access, användarkonto och informationshantering.
Då är fråga ett, på vilket sätt reglerar ni era användarkonton utifrån er säkerhetspolicy? Och en underfråga

till den, är det vanligt att en användare har flera lösenord till olika system?

29. A: Vi har alltså ingen "singel sign on" utan alla har att man kan ha olika användarkonto till olika system men man har bara ett användar-ID dvs. ett KID och det går igenom alla de system vi har där man behöver inloggning. Det finns bara ett system där man inte behöver ha inloggning och det är vår användarutbildning inom informationssäkerhet. Det har vi gjort för att alla ska ha kunna tillgång till utbildningen. Men annars är allt reglerat med kort där vi har PKI och där kan man säga att de känsligaste systemen ex. vårt "affärssystem 1" och några till, där måste man använda kortet och KID för att komma igenom och kod. Andra system som är mitt i mellan är det kortet och KID som gäller. Vi har faktiskt inte idag konverterat nätet till kortet än men det är på gång. Men vi säger att man inte helst använder samma lösenord i nätet som på sina system. Men däremot har vi sagt att heller att de inte skriver upp lösenorden och att där man använder samma lösenord i olika applikationer. Men vi vill inte att de använder samma lösenord i nätet som på applikationerna. Sen hur detta efterlevs är svårt att säga. Men tanken är att om snar framtid ska kortet vara till för att logga in på systemen. Reglerna för kortet är att man ska ha det för att komma igenom passagen och att man ska bära det synligt så att man alltid kan se det.

30. S: Hur hanterar ni om någon skulle tappa kortet?

31. A: Alltså ett kort kan vi få spärrat på mindre än tio minuter.

32. S: Men hur är det när den anställda ska få tillbaka sitt kort?

33. A: Det är en ganska rigid procedur att gå igenom tyvärr så tar processen för att få ett nytt kort alldeles för lång tid. Det är ett irritationsmoment för användare..

34. S: Ja..

35. A: Och dom är rätt så dyra så vi vill inte att folk ska slarva bort sina kort.

36. S: Nä, precis..

37. A: Prislappen på ett sådant här kort är ca 1500 kr.

38. S: Men du sa att ni tänkte bara använda kort i framtiden?

39. A: Ja, vi vill försöka gå över till att bara använda kortet, vi har en annan lösning, men vi vill gå över till tvåfaktor-authentisering överallt. Men vi har inte dem fullt ut. Vi har haft lite slitageproblem med chippen på dom här korten. Vi kallar det för "Företag B"-företags kort och det ska ju användas i många andra sammanhang än bara säkerhetssammanhang. Det är också det kortet som vi ska visa upp för att visa att vi är "Företag B"-personal när vi träffar kunder. Det är så hög trovärdighet hos det här kortet att det går att identifiera sig hos polisen.

40. S: Okej.. Och det fanns ett slags lösenord, eller pin-kod till kortet?

41. A: Ja..

42. S: Om man glömmer bort det, hur svårt är det att få ett nytt?

43. A: Då kan man få ett nytt vi service-desken. Det är begränsat vilka i servicedesken som är så kallade pin-admins. Alla pin-admins får sin behörighet av mig. Man kan inte bli pin-admin utan att det har passerat mig. Jag är den svaga länken i kedjan. Jag har förvisso blivit godkänd från högre ort att jag ska ha den rollen jag

har, men jag är ensam. Vilket betyder att om det händer mig någonting så är det inte så bra för "Företag B", då kommer det vara ett glapp för hur de ska få nya pki-administratörer och nya pin-admins.

44. S: Okej. Hur hanteras det om någon ringer in, som har hittat ett kort, och säger hej , mitt namn är det här och det här, jag vill ha ny pin-kod?

45. A: Om vi tar det riktiga senariot först. Om en användare upptäcker att dom inte kommer ihåg sin kod. Den är åtta tecken lång så den är lite tuff att komma ihåg. Då ringer dom service-desken som noterar ärendet, ställer motfrågor t.ex. enhet, närmsta chef etc. sen lägger man på luren. Sen ringer servicedesken till det förregistrerade telefonnumret, och det ska då vara samma person som svarar. Är dom minsta lilla osäkra så ringer dom till närmsta chef och frågar. Och får dom inte tag i närmsta chef då ringer dom oftast till mig och frågar vad dom ska göra, och då för jag göra en bedömning.

46. S: På vilket sätt blir det säkrare med det här korten än med bara användarnamn och lösenord.

47. A: Kortet är en förstärkning utav lösenordet. Istället för att ha bara att du anger ett lösenord så måste du ha kortet med certifikatet och pinkod.

48. S: Så det är som en tredje säkerhets variabel?..

49. A: Det är någonting du vet, någonting du är och någonting du har kan man säga. Eller inte någonting du är för det är biometri, vilket vi i övrigt också använder. Datorhallarna kommer man inte in i utan fingeravtryck.

50. S: Okej, Ja nästa fråga. På vilket sätt reglerar ni och hanterar tillgång till information i er informationssäkerhetspolicy? Som exempelvis att någon kan logga in på en klient och få tillgång till massa känslig information.

51. A: All inloggning ska ske i egen behörighet. Men några få undantag har vi. Det är till och med så här att när man gör IT-administration, så gör man det förfarande i egen behörighet. men det finns en del system som är väldigt gamla, framförallt på process IT sidan. Det kan skilja på kontors och administrativ IT och industriell IT. Där jag då har ansvar för båda delarna. På Industriell IT är systemen oerhört gamla, oerhört känsliga och där kan systemen många gånger inte hantera olika behörigheter. Så där finns det gruppkonto och grupplogins. Och då brukar vi istället vilja ha någon form utav logg, eller på annat sätt, så att vi kan identifiera vem som varit inloggad var, vid vilken tidpunkt.

52. S: Så ni loggar alls konto?

53. A: I nätet loggar vi alla. Alla system ska logga minimum alla systemhändelser, konfigurationsändringar och allting sånt, användare som är inloggade, det ska vara loggade med KID. Bara vi har ID så är det bra. Tidpunkt, tid för inloggning, tid för utloggning, och händelser, lite vad man gör. Och där är det lite varierande vad det är beroende på hur känsligt systemet är, vilken typ av händelser vi loggar. Vi loggar inte alla transaktioner, har du kommit in i ekonomisystemet loggar vi inte på den nivån, varenda liten tangenttryckning eller transaktionsändring. Även om man kan spåra det på annat sätt. t.ex. all surfning loggas, det sparas inte särskilt länge, men det loggas och kan vid behov plockas ut på individnivå, även om vi inte gör det utav PUL hänseende. Vi levererar statistik till verksamheten på begäran, det är inte alla som vill ha det, t.ex. vill kundtjänst avdelningen ha surfstatistik på alla kundmottagare, och det handlar egentligen om stöld av arbetstid kan man säga. Och det får dom inte ut på individnivå men däremot så kan dom få ut en topp10 lista på, PersonX har varit 6,3 timmar på Facebook denna månad. Och dom kan få ut total hur mycket tid man har varit på då top 10 listan, på sajter.

54. S: Vet dom anställd om att dom blir loggade?

55. A: Ja. Man skriver på användarföreskrifter, och det gör man innan man får ut en dator. Man får ingen dator annars. Vill du jobba här så skriver du på. Där står det vilka regler som ska följas, våran etiska policy, och att vi loggar. Där står till viss del vad vi loggar. När det gäller internetloggningen så har vi en liten fin skylt som talar om när man går någonstans, vilket jag får ganska ofta då det ingår i mitt jobb att testa "fula" sidor. Så jag får ganska ofta denhär skylten att min dator håller på att gå mot en sida som inte är godkänd enligt eran policy. Sedan kan man klicka upp policyn och då står det exakt vad som gäller.

56. S: Så sidorna är inte helt spärrade? Ni har bara en informationssida, att nu är det inte okej att gå in?

57. A: Vi har tre nivåer på det. Dom som man bara går igenom när det inte är någonting. Dom där man får upp den här varningsskylten men kan gå vidare. Sedan finns det dom som är helt blockerade. Vi har faktiskt ändrat inriktningen där. Tidigare blockerade vi kanske lite mer än vad som var absolut nödvändig, sådant som kanske inte har helt med arbete att göra. Vi blockade en del saker på önskemål från HR, bland annat tobak, alkohol och droger, vilka inte är någon säkerhetsrisk men vi hade ett verktyg och då tyckte dom det verkade bra. Det har man nu svängt och sagt att det är mer chefsansvar och därför är inte dom kategorierna blockade men man får den här lilla skylten att tänka efter om det här verkligen är arbetsrelaterat. För vi tillåter ju att man använder både våran utrustning och e-post privat så länge det inte har en påverkan på arbetets genomförande.

58. S: Så det kan vara så att en anställd kan gå in och kolla sin privata Facebook mail.

59. A: Just mail har vi en spärr på, webmail, det är på grund av att vi fick in för mycket skadlig kod.

60. S: Hotmail och liknande?..

61. A: Ja, för dom är inte tillräckligt väl skyddade. Genom riskanalysen kom vi fram till att genom ge de anställda den friheten att dom kan kolla sin privata mejl, visst är det ett mervärde i det, men nivån av skadlig kod vi fick in var faktiskt en ganska stor kostnad, i rensning, och vi har känsliga system. Vi får tänka på att om det sprider sig, om vi får ett massutbrott, då stänger vi ner halva Sverige, mer eller mindre om vi inte kan hantera det och inte leverera våran leverans. Så att där var vi tvinga att säga att värdet av att medarbetarna tycker det är trevligt att accessa sin privata mejl är för låg i förhållande till risken. Däremot ger vi dispans till konsulter att nå sina hemmaföretag.

62. S: Okej..

63. A: Vi anser att värdet för att dom kan nå sina hemmaföretag är högre, risken är mindre, förhoppningsvis jobbar vi bara med partners som har ett bra anti-virus skydd.

64. S: Okej, ja vi kan ta de mer övergripande frågorna och gå in på det övriga om det finns tid.

65. A: Ja, jag ser att ni har en fråga gällande social engineering.

66. S: Ja, berätta gärna hur ni hanterar social engenering.

67. A: Det är en sån fråga som ofta är väldigt bortglömd, att det finns. Jag vet inte om det är kopplat till lojalitet men vi har ju en del lojalitets program och inte så mycket teambuilding, men det förekommer väl en del. Men det är väl mer utav den anledningen att företaget har en ganska hög medelålder. "Företag B" har en kommande risk i att vi kommer att ha brist på medarbetare om några år. När vi haft stora pensionsomgångar. Och därför så är det viktigt för oss att alla medarbetare trivs och pratar bra om att det är

bra att jobba på "Företag B" så att vi har möjlighet att rekrytera när vi väl står där. Vi kan inte börja rekrytera, men vi har börjat så smått, men det är ju inte ekonomiskt försvarbart att man har dubbelt för länge. Vi måste ju vänta tills folk faktiskt har slutat. Men då är det ju väldigt viktigt vi kan rekrytera om man vill jobba hos oss. Vi har ju kanske inte alltid det bästa ryktet, det är vi väl medvetna om.

68. S: Okej..

69. A: Där kan jag ju säga att vi har en ganska bra förmånspolicy.

70. S: Men det här med social engineering, har ni något speciellt sätt som ni använder för att skydda er mot det?

71. A: Det har vi ju som en del i informationssäkerhetsarbetet. Det är med i det här spelet. Och det ingår även i de här lathundarna, en om usb. Där har vi en om social engineering, och framförallt om den här typen av phishing mail och även telefonsamtal. Det är så pass mycket medvetenhet så vi har incidenter i vårt incidentrapporteringssystem som är att medarbetare har blivit uppringda och tyckt att dom har gått konstiga frågor, så har man själv lagt in en incident på detta.

72. S: Vet dom anställda om att dom ska rapportera det, eller dom gör det om dom vill?

73. A: Vi har ju ett väldigt omfattande incidentrapporteringsarbete. Exempelvis så ska vi rapportera om det ligger en lös sladd i konferensrum, eller om vi ser en oljefläck. Och alla risker ska hanteras på samma sätt, så är det en informationssäkerhetsrisk kan man ju säga att om någon ringer och ställer konstiga frågor, vi säger då att om man ställer frågor gällande vårat säkerhetssystem så ska man hänvisa till någon av oss som jobbar med säkerheten. En "vanlig" anställd får inte besvara dom själv. Exempel IP-adresser, brandväggskonfigurationer och sådana saker är ingen information som vi ska dela med oss utav. Det är kvalificerad företagshemlighet.

74. S: Så utbildning kan man säga är för att öka deras awareness i företaget? Om att det förekommer..

75. A: Ja, Vi ställer ju högre krav på IT medarbetarna än vad vi ställer på de övriga 5800 anställda. Men det är ju också för att dom har högre behörigheter, och dom kan ställa till med mer saker.

76. S: Dom har tillgång till mer information, information som inte hör till deras arbete?

77. A: Ja. Bara en sådan sak som att servicedesk medarbetarna kan ta över, som en del av att dom ska kunna hjälpa användarna, vilket är väldigt viktigt att dom kan göra på ett snabbt sätt. Dom tar då över kontrollen på våra PC:s, och därmed får dom ju därmed tillgång till all den information som finns på den PC:n. Men dom kan inte göra det utan att användaren accepterar att låta servicedesken ta över. Man ska ha dom i telefonen samtidigt, så säger de jag har kid, och sen syns det att servicepersonal med visst kid tar över.

78. S: Då blir det någon slags vidare loggning?

79. A: Det loggas ja. Det loggas så att servicepersonal med kid har tagit över min dator, och så loggas det när dom tar över och när dom släpper kontrollen över datorn.

80. S: De flesta kommande frågor har vi diskuterat så vi kan gå vidare till nästa del.

81. A: Ja. Vi tillåter ju att man loggar in hemifrån. Vi har ett antal olika koncept kan man ju säga. Dels har vi je det som de flesta medarbetare utav oss har så att säga, vi har ju laptops, i princip allihopa. Vi har fler laptops än vi har stationära datorer. Och dom är alla med diskkryptering. Så dom är default alltid krypterade. Och vi har en remote access lösning där all trafik går i en krypterad tunnel. Tidigare hade den faktiskt den lilla

luckan att man som användare, om man satt t.ex. på SJ, var man tvungen att dissabla den lokala brandväggen för att få tag i SJ:s inloggningssida och därifrån öppna tunneln. Sen slog man på brandväggen igen, men den har vi faktiskt fixat så det går inte längre. Sen har vi virtuella klienter som ibland ger konsulter. Då skapar vi en "Företag B"-pc i deras pc som är helt logiskt skild från deras egna pc.

82. S: Men en sådan sak, hur får ni reda på det, får de anställda ge feedback på sådana säkerhetsbrister så att ni kan fixa till dom?

83. A: ja, de kan ju lämna det via det här incidentrapporteringssystemet. Och där rapporteras allt möjligt konstigt. Mycket av det är inte incidenter. Men om dom märker något konstigt så rapporterar dom det där. Men sådana saker det är ju tekniska personalen som undersöker och hittar dom. Vi driftsätter ju inte en tjänst utan att den är testad. Och till många tjänster hyr vi in penetrationstestare och hackers som hårdtestar systemen innan dom tas i drift. Så en lösning som tas i drift vet vi som regel om att den har det här och det här hålet. Men då har vi triangeln, säkerhet, kostnad, funktionalitet, verksamheten är geografiskt väldigt spridd. Vi finns över allt, mer eller mindre, långt ut på otillgängliga ställen. Därför finns det fjärrstyrningsmöjligheter till allting. Så därför är det väldigt viktigt att det är rätt person.

84. S: Okej, så ni har ingen sådan aktivitet där ni involverar användarna där de får påverka hur säkerheten är uppbyggd?

85. A: Nä, inte så mycket hur säkerheten är uppbyggd. Dom får ställa funktionskrav. Vad dom behöver. Det är oerhört få slutanvändare som ställer ett säkerhetskrav. Vad dom möjligtvis gör som är säkerhetskrav, är dom ställer krav på tillgänglighet. Annar är det ytterst sällan. Det är då vi som har rollen, informationssäkerhetsansvariga, som är verksamhetens förlängda arm, som ska ställa dom kraven så att dom också kommer med. För sekretess, tillgänglighet, spårbarhet, integritet och riktighet.

86. S: Okej, då kan vi gå vidare till frågor gällande användarkonto och tillgång till information. Hur ofta byts lösenord? Tvingas de anställda att byta lösenord?

87. A: På korten är det faktiskt vart annat år, eller något sånt. Eftersom där är det två delar. Man byter inte pinkod på sitt bankomatkort särskilt ofta. Det är viktigare att dom kommer ihåg så att dom inte skriver ner det. Men dom vanliga lösenorden, där man inte har någon form utav token, dom ska bytas var 90:e dag. Och det är kanske lite sällan, men det måste vägas mot att det är ännu värre att ha gula lappar över allt. Vi ställer krav på komplexa lösenord, dom lösenord som får lov att användas måste vara minst åtta tecken långa, det ska vara stora och små bokstäver, det ska vara specialtecken och det ska vara siffror.

88. S: Det har ni en automatisk check som gör då eller?

89. A: Det ska då byggas in i alla system. I testerna inför driftsättning sådan sak som ska testas. Att där finns valideringscheckar.

90. S: Men dom får välja dom här lösenorden själv?

91. A: Dom får välja lösenorden själva. Men de ska uppfylla dom kriterierna, och samma lösenord kan inte återanvändas, det kollas 13 gånger bak. Anledningen till att det är just 13 är för att undvika januari,01 februari,02 o.s.v..

92. S: Så om du fyller i ett lösenord som inte är giltigt får du respons?

93. A: Då måste du välja ett nytt. Då accepterar den inte lösenordet. I vissa system sätter administratören ett lösenord, när du har använt det en gång är det tvingande lösenordsbyte.

94. S: Är där någon slags spärr, att om man försöker logga in flera gånger så spärras kontot?

95. A: Ja, det är det. Och det varierar åter igen lite beroende på hur mycket systemen tillåter. Man kan säga att det går från tre till åtta gånger. Tre på de mer känsliga, som t.ex. krypteringen på våra laptops.

96. S: Okej, 4:an. Vet anställda vilken information som är sekretessbelagd? T.ex. känsliga e-post som kommer in och annan information.

97. A: Ja, Vi har ju informationsklassningsregler som innehåller exempel. Ni har ju som ni kanske förstår väldigt mycket information. Regeln säger att det är information ägaren som ska sekretessklassificera informationen. Vem är då informationsägaren?. Ett, så är det den som skapar informationen, och två, så är det den som får informationen utifrån, och tre, i vissa fall är det så här att det är någonting som man får med ett visst intervall och det kan vara olika handläggare. Och det är ju inte vettigt att varje handläggare ska sitta och informationsklassificera varje gång. Då är det chefen. Då är det avdelningschefen som har ansvar att informationen på hans avdelning är rätt klassificerad. Det där är så det ska vara, och hur det är en helt annan sak. Informationsklassning är ett område som är oerhört svårt, som ärligt talat folk blir sämre och sämre på. Om man tar fysiska dokument, så vet de äldre medarbetarna precis hur dom ska göra. Dom stoppar det i kuvert och häfta och stoppar dom det i ett nytt kuvert. Och sen tar dom samma information och skickar det i klartext via e-post. Det är ju utbildning som gäller.

98. S: Är det kunskap som saknas?

99. A: Jag har funderat jättemycket på det här. När samma individ är jätteduktig när jag ger ett pappersark, sen när jag ger dom en fil är det som bortblåst. Som jag sa, vi har en hög åldersprofil, man tycker det här med datorer är svårt, det är jobbigt, besvärligt och dom kan knappt själva öppna den här bifogade filen, och tanken att någon skulle kunna ta den på vägen när den är i någon sladd någonstans, den finns inte. Man har så svår att tänka sig att det skulle kunna gå. Mycket av min tid går ju åt att förklara att det är ju egentligen ganska lätt.

100. S: Det upplevs kanske lite väl abstract.

101. A: Det blir abstract. Vi brukar använda oss av en liten liknelse. Om man tar ett djungelfolk, och så sätter du dom på spåren där ute till stockholmslinjen, och så, gå du där, du ska i den riktningen. Kommer dom över huvudtaget taget att tänka på risken att man kan bli påkörd av ett tåg. För dom känner inte till konceptet tåg. Då kan man inte värdera risken. Lite där är vi i samma situation när det gäller informations/IT-säkerhet. Man har en infrastruktur som man glatt springer runt på men man har ingen aning om risken egentligen. Och man kan inte heller hålla på och skrämmas. En del säger då att ”jag vågar inte använda datorn” men det är klart de ska använda datorer, det vinner vi jättemycket på. Så man måste förklara men man får inte heller skrämmas.

102. A: Vi har möjlighet att kryptera e-post. Sekretessbelagt information ska vara krypterad både när den lagras och när den skickas. Det har vi ett system för. Vi använder också fyra sekretessklasser, öppen, intern, företagshemlig, kvalificerad företagshemlig.

103. A: Det vi jobbar mest med är sånt som är olagligt. Där sitter jag och tittar på en lösning som vi inte har än. Ett system som identifierar barnpornografiska bilder. Det är rikspolisstyrelsen som sätter en ”fingerprint” på bilden, sen så fort en sån bild dyker upp så går det ett larm till oss som och den sätts i en speciell form av karantän. Den printar en rapport, precis så som polisen vill se den. Fördelen med det systemet är att jag och

mina medarbetare som arbetar med incidentutredning slipper titta på det. Får vi den typen av indikation så gör vi en förutredning själva, för att se om det är någonting, sen kontaktar vi polisen. Ibland är det tvärtom att polisen kontaktar oss för då har de kanske fått upp ett spår på nån och så vill de att vi beslagtar företagsdatorn. Men tyvärr innebär det att vi är en del som får se saker som vi inte vill se.

104. S: Har ni någon slags extra kontroll för att se att det verkligen är en polis som kommer och beslagtar datorn?

105. A: Ja, det har vi. Vi har löpande och regelbunden kontakt med polisen.

106. S: Hur är det med forum och sånt där?

107. A: Vi har en policy för sociala medier och den är inte bara av säkerhetssjäl utan den ägs faktiskt av varumärke och kommunikation. Vi har dels regler för när man är I sociala forum I egenskap av "företag 2", för det har vi medarbetare som är. Då vi letar efter nya unga medarbetare så vart hittar man dom? Jo, dom hittar man på sociala forum oftast. Vi finns på både facebook och bloggar osv. Sen är det så att varje medarbetare agerar I sociala forum, då finns det en policy för vad man får säga och inte säga. Sen har vi ett internt bloggforum, där bland annat jag skriver om regler och vad som är aktuellt just nu och så.

108. S: Okej.. Här nere på övrigt har vi två intressanta frågor. Är det något speciellt i policyn som du tror begränsar folk i arbetet med informationssystem speciellt?

109. A: Målsättningen är egentligen att säkerheten ska vara så transparent som möjligt. Man ska inte behöva uppleva den som ett hinder, jag vet att man ibland gör det. Surfningen har varit en sån sak men på grund av ändringen nu så har den blivit ett mindre irritationsmoment. I viss mån har även remote access varit det. Det är stor skillnad mellan Sverige och andra länder. Vi här i Sverige vill gärna ha våran jobb-IT-miljö precis som hemma. Det är oftast inte av säkerhetsskäl utan av rena IT-policy-grejer. Vi har fått köpa in standarddatorer och det har man väldigt svårt att köpa av användarna. Går jag till mina kollegor i andra länder så ser man mycket mer att datorn är ett verktyg, vi tenderar att tro att datorn är vår personliga leksak. Det är mer missnöje i Sverige, det är till exempel många som vill köpa en Mac, det har vi inga... eller ja, bara en.

110. S: Vilka potentiella genvägar kan de anställda ta för att effektivisera sitt arbete? Finns det någon lucka du kan se, så som att de hoppar över något säkerhetssteg?

111. A: Ja, de försöker men vi hittar det mesta. Jag kan citera en av våra sommararbetare som satt och åt slutlunch eller något sånt "På företag 2 kan man inte göra någonting utan att de märker det". Så jag tror vi hittar det mesta, vi hittar Skype, vi hittar skadlig kod, oftast innan användarna själva är medvetna om att de har något.

112. S: Får ni inte använda MSN heller?

113. A: Vi använder MSN internt men däremot får man inte använda det externt, det är spärrat också. Det är en sån sak som människor tycker att de ska ha men jag tycker inte det varit någon konflikt än. Det är mer att man klagar över att datorerna är långsamma.

114. S: Men du tror då kort att de inte går runt några regler för att att öka effektiviteten, utan då är det mer kanske för att chatta med någon kompis eller så?

115. A: Då är det mer att man antingen inte vet om regeln, vi försöker ju se till att det inte ska vara ett effektivitetshinder. Ibland kan det vara det och när den är det så är det svårt att gå runt den.

116. S: Jag tänker som exempel att man sätter en kil i dörren när man ska gå in och hämta något. Detta är ett fysiskt exempel men i en dator då till exempel att folk struntar i att klassificera.

117. A: Ja, informationsklassificeringen är väl ett sånt exempel där det är lätt att göra fel och ett av de ställen där det går att göra fel.

118. S: Det finns inga andra liknande där man kan hoppa över...?

119. A: Nej, jag nämnde det här att man hade det här att man måste stänga av den personliga brandväggen och det lärde vi också alla användarna. Att när du ska ansluta mot vissa hotspots som kräver inloggning så måste du först stänga av den personliga brandväggen, sen öppnar du explorer och gör inloggningen. Sen öppnar du tunnelklienten och när du öppnar den så sätter den automatiskt på brandväggen igen. Det missbrukades lite men nu som sagt så är det inte möjligt. Alltså de allra flesta har inte.. inte ens jag är administratör på min egen PC. Vi arbetar efter den principen att det ska vara lätt att göra rätt och på så sätt begränsa möjligheterna att göra fel. Surfningen öppnade vi upp efter kritik så att det istället kommer statistik till cheferna. Vi spärrar det som är säkerhetsrelaterat och det som är olagligt, det kommer man inte åt. Filtrena bygger på reputation, dvs. siter som av någon anledning.. de kan ju vara hackade.

120. S: Men har ni det helst spärrat utåt eller egentligen eller förutom Internet...?

121. A: Internet är fullt öppet höll jag på att säga, förutom det som är olagliga sidor och ”extreme violence” osv.

122. S: Diskriminerande sidor?

123. A: Det är åter igen att det går till en policy och chefsansvarig-grej. Vi kan alltså inte säga att du inte får lov att titta på... alltså vi som arbetsgivare ska vi inte lägga oss i om du är nazist eller vad du nu vill vara. Sen kanske vi inte tycker om det och kan på annat sätt få dig att komma på bättre tankar. Men egentligen har vi inte rätt till det, man kan säga att det vi försöker få det till är att man inte ska använda sin arbetstid på det.

124. S: Jag vet ju att ni använder en tunnel för att komma in i företaget så det ganska lätt med sin webbläsare att använda proxy serverar för att komma ut på sidor som är spärrade. Har ni spärrat proxyservrar?

125. A: Alltså det där en en sån som är svår, jag kan inte säga att det är 100% löst men bland annat som sättet vi sorterar ut vår webbmail så är det oftast en krypterad inloggning. Då spärrar vi den, alltså enligt policy får man inte använda krypteringsteknik för att spärra ute företaget 2s från företag 2s information och utrustning. Så vi vänder på det kan man säga. Åter igen, är man inte administratör på klienterna så finns det inte så mycket man kan ställa in. Vi hade en incident där en person satte upp en fildelningsserver på vårt interna nät, den gapade ju ett litet tag innan vi fick tag på den rent fysiskt. Vi har ett rätt så aktivt incidenthanteringsarbete. Det låter kanske hemskt att säga, men vi har ju storleksordningen 500 incidenter per år som vi utreder. Kan vara mer om det sker någon virusgrej men storleksordningen 500. Det handlar om att vi aktivt försöker hitta och följa upp och utreda. Vi polisanmäler också en hel del grejer.

126. S: Men ni anser ändå att det är effektivare att ha ett öppet Internet och köra ”investigation” än att låsa allt och slippa undersöka om de anställda gör dumma grejer?

127. A: Man kan inte låsa att och samtidigt ha en fungerande verksamhet.

128. S: Nej, men mycket går väl att låsa?

129. A: Ja, mycket kan man men vi har nog låst ner det så mycket det går och ändå finns det ett flöde. Låt mig säga så här, har man inga incidenter på sitt företag så har man förmodligen inte ett speciellt bra uppföljande

informationssäkerhetsarbete. Jag skulle gissa på att man inte har koll. Jag säger, vi har trots det ganska höga antalet så är det ganska mycket som går under radarn. Vi har ett stort problem med skadlig kod för närvarande. Dom antivirusleverantören vi anlitar säger själva att de detekterar mindre än hälften, bland annat därför vi använder fler med förhoppningen att den ena hittar det den andra missat.

130. S: Du sa att de klagade på att burkarna var slöa, kan det bero på antalet virus program?

131. A: Det tror jag inte beror på det. Vi har överlag ganska gamla maskiner. Man köper gärna budgetmaskiner med lite internminne och lite processorkraft och sen lastar vi på med en förfärligt massa skipningar och packningar utav programvara.

132. S: Okej, så det är inte bara säkerhetsaspekterna som gör att de är slöa.

133. A: Nej, men sen är det åter igen det där med vad är slött? Jag har klockat min maskin och den har en uppstartstid på 2.55 minuter ungefär. Ja, vad gör man när man kommer till jobbet, startar upp datorn och hämtar kaffe osv och när jag är klar så är den uppstartad. Jag ser det inte som ett jättebekymmer egentligen men folk kan ibland vara lite gnälliga.

134. S: En kompletterande fråga där med uppdateringen. Sker den på morgonen eller sker den på arbetstid?

135. A: Den kan ske på arbetstid. Vi har en veckoscan på antivirusen varje tisdaglunch och den kan ju ibland komma väldigt olägligt. Det är meningen att den ska komma på lunchen men om man av någon anledning drar över så ”säckar” ju hela maskinen och det kan vara ganska irriterande. Vi pushar ju ut uppdateringar och vissa uppdateringar kräver att man startar om datorn. Är uppdateringen inte jättekritisk så schemalägger vi den till att den ska uppdateras antingen i början eller slutet av arbetsdagen. Är det lite mitt-emellan-kritiskt så pushar vi ut den och vill att den ska starta om inom 2 timmar men användaren kan senarelägga två gånger. Är det hyperkritisk så skiter vi i vad användaren säger och pushar ut den och startar om datorn. Ingen patch läggs på utan att den är testad på våra standarddatorer. Det finns vissa datorer som inte är standarddatorer där det kan uppstå problem.

136. S: Det är aldrig så att en anställd får utföra några steg för att installera en patch?

137. A: Allt det där händer innan, sen trycks den ut. Då kan det vara så att användaren får starta om datorn till exempel, men vi försöker skippa det också.

138. S: Så de behöver inte knappa runt för att installera... Använder ni ISO 27001?

139. A: Den har vi, sen har vi lite mer. Vi har även det här med industriella IT-system. Det finns ingen ISO-standard som är värd namnet på den, ingen reglering heller. Men i USA finns det en reglering och standard som heter nerc cip och där har vi ett beslut att vi ska följa den till 75 %.

Bilaga 5 Enkät, Företag A, internt enkätsystem

Survey name: Effectiveness versus Information Security

Purpose of bachelor thesis
We are three students at Lunds University, doing a survey for our bachelor thesis, on the impact of information security on the effective use of information systems. Efficiency can be defined as the degree of effectiveness in relation to the resources used. In this case, the use of resources consists of working hours. We want to measure to what degree information security is preventing you in your everyday work performance.
You will be anonymous in this survey; neither we nor anyone else will know who you are.
This survey should take about five minutes to answer. We appreciate your help.

Question 1. I know the rules that apply to me in the company's information security policy?

- Strongly Agree
- Agree
- Partially agree
- Disagree
- Strongly disagree

Question 2. I think my manager has affected my security awareness positively.

- Strongly Agree
- Agree
- Partially agree
- Disagree
- Strongly disagree

Question 3. Do you feel that your work has too many security rules, when you are performing certain tasks?

- Yes
- No

Question 4. I think it is time consuming to log into the different systems.

- Strongly Agree
- Agree
- Partially agree
- Disagree
- Strongly disagree

Question 5. I think it is time consuming to change my password.

- Strongly Agree
- Agree
- Partially agree
- Disagree
- Strongly disagree

Question 6. I think it is time consuming to retrieve a new password when I lost my old one.

- Strongly Agree
- Agree
- Partially agree
- Disagree
- Strongly disagree

Question 7. I think it is time consuming to comply with the security policies for document classification.

- Strongly Agree
- Agree
- Partially agree
- Disagree
- Strongly disagree

Question 8. I think the education I received about information security has made me able to perform my job more effectively.

- Strongly Agree
- Agree
- Partially agree
- Disagree
- Strongly disagree

Question 9. Has it happened that you skipped rules from the security policy just to increase your efficiency?

- Yes
- No

Question 10. It often happens that I skip steps from the security policy to increase the efficiency of the work assignments. (If the answer is Yes on question 9, please answer question 10)

- Strongly Agree
- Agree
- Partially agree
- Disagree
- Strongly disagree

Question 11. Have you ever got the chance to affect changes in the information security policies?

- Yes
- No

Question 12. Do you believe that your work would be more effective if you had the chance to affect the information security policies? (If you disagree with question 11, please answer question 12)

- Yes
- No

Question 13. Are you using non-job-related web pages more than one hour per day?

- Yes
- No

Question 14. Do you know how to handle information with high security classification?

- Yes
- No

Question 15. I think it's time consuming to manage information with high security classification.

- Strongly Agree
- Agree
- Partially agree
- Disagree
- Strongly disagree

Question 16. I think that I have access to information with higher security classification than I use.

- Strongly Agree
- Agree
- Partially agree
- Disagree
- Strongly disagree

Question 17. I think that I've got access to information that is irrelevant when I perform searches in different databases.

- Strongly Agree
- Agree
- Partially agree
- Disagree
- Strongly disagree

Question 18. I think that automatic security updates often take a long time to carry through.

- Strongly Agree
- Agree
- Partially agree
- Disagree
- Strongly disagree

Question 19. Do you have more than one user account (regarding login to different systems and applications)?

- Yes
- No

Question 20. I think it is time consuming to handle different user accounts. (If you agree with question 19, please answer question 20)

- Strongly Agree
- Agree
- Partially agree
- Disagree
- Strongly disagree

Question 21. Are you using Internet to make your everyday working more effective? (eg. through wikis, forums, etc.)

- Yes
- No

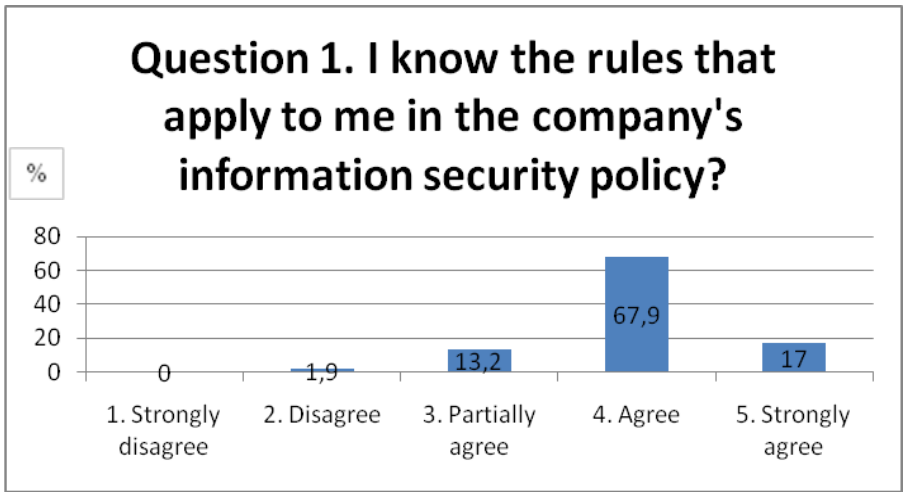
Question 22. I feel that the security in general slows me down when using IT-systems.

- Strongly Agree
- Agree
- Partially agree
- Disagree
- Strongly disagree

Bilaga 6 Resultat, Enkät, Företag A

Question 1

Question 1. I know the rules that apply to me in the company's information security policy?		
Current average: 4 of 5		
Alternative	**Answers**	**%**
1. Strongly disagree	0	0
2. Disagree	1	1,9
3. Partially agree	7	13,2
4. Agree	36	67,9
5. Strongly agree	9	17

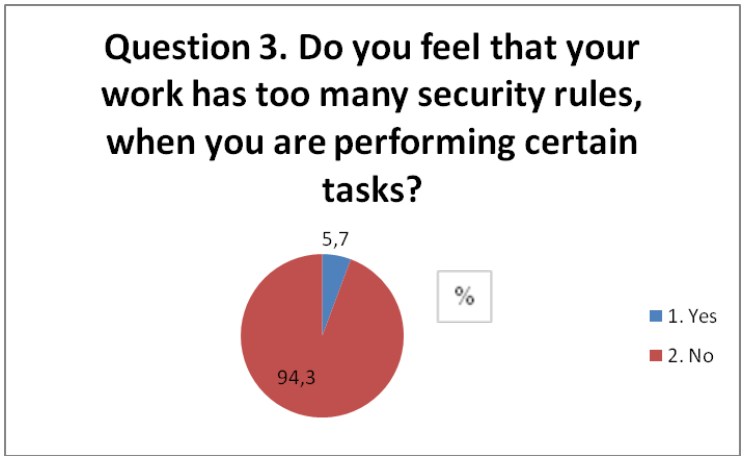


Question 2

Question 2. I think my manager has affected my security awareness positively.		
Current average: 3.1 of 5		
Alternative	**Answers**	**%**
1. Strongly disagree	1	1,9
2. Disagree	13	25
3. Partially agree	20	38,5
4. Agree	16	30,8
5. Strongly agree	2	3,8

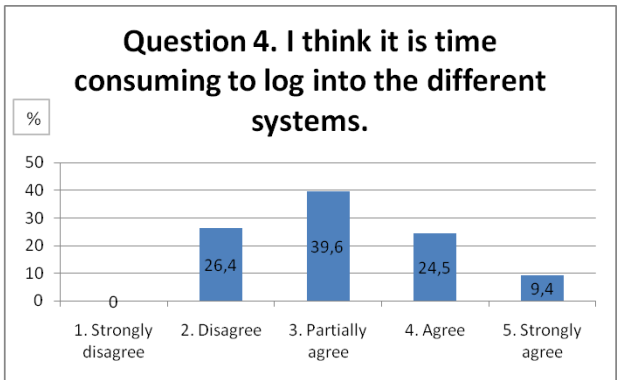
Question 3

Question 3. Do you feel that your work has too many security rules, when you are performing certain tasks?		
Alternative	**Answers**	**%**
1. Yes	3	5,7
2. No	50	94,3



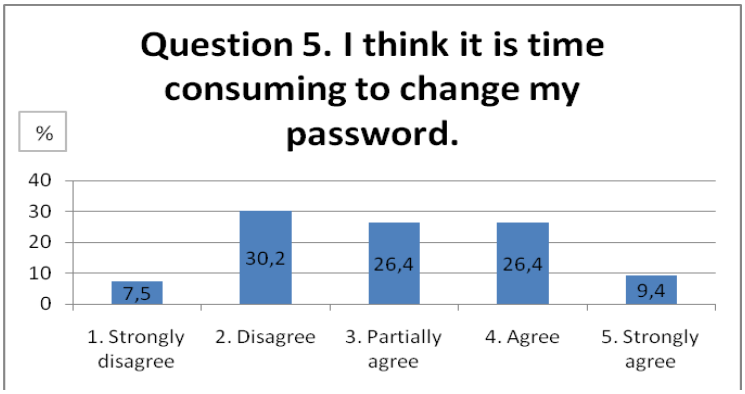
Question 4

Question 4. I think it is time consuming to log into the different systems.		
Current average: 3.17 of 5		
Alternative	**Answers**	**%**
1. Strongly disagree	0	0
2. Disagree	14	26,4
3. Partially agree	21	39,6
4. Agree	13	24,5
5. Strongly agree	5	9,4



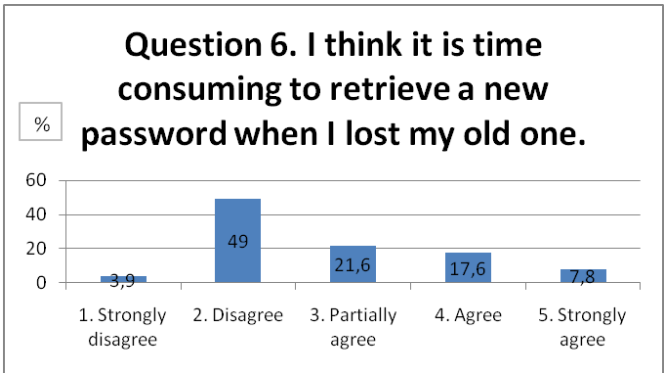
Question 5

Question 5. I think it is time consuming to change my password.		
Current average: 3 of 5		
Alternative	**Answers**	**%**
1. Strongly disagree	4	7,5
2. Disagree	16	30,2
3. Partially agree	14	26,4
4. Agree	14	26,4
5. Strongly agree	5	9,4



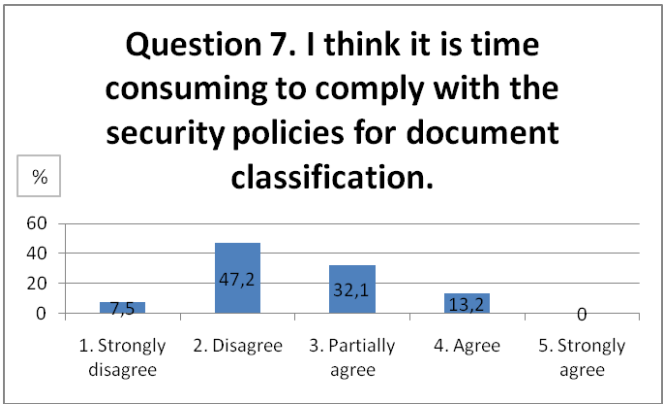
Question 6

Question 6. I think it is time consuming to retrieve a new password when I lost my old one.		
Current average: 2.76 of 5		
Alternative	**Answers**	**%**
1. Strongly disagree	2	3,9
2. Disagree	25	49
3. Partially agree	11	21,6
4. Agree	9	17,6
5. Strongly agree	4	7,8



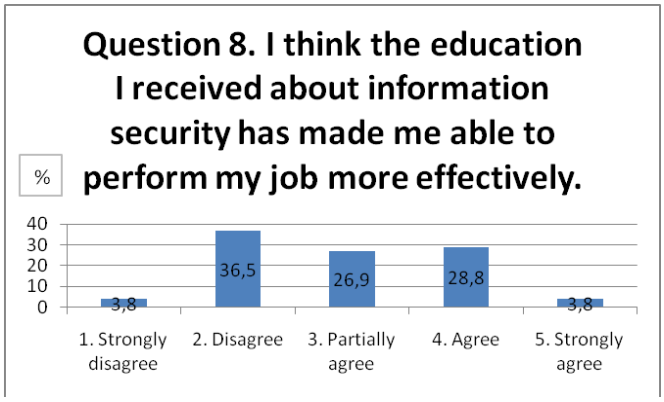
Question 7

Question 7. I think it is time consuming to comply with the security policies for document classification.		
Current average: 2.51 of 5		
Alternative	**Answers**	**%**
1. Strongly disagree	4	7,5
2. Disagree	25	47,2
3. Partially agree	17	32,1
4. Agree	7	13,2
5. Strongly agree	0	0



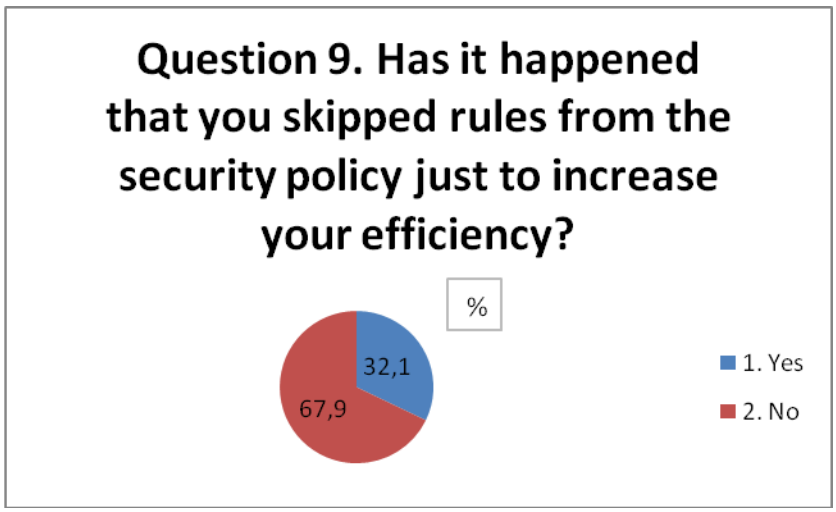
Question 8

Question 8. I think the education I received about information security has made me able to perform my job more effectively.		
Current average: 2.92 of 5		
Alternative	**Answers**	**%**
1. Strongly disagree	2	3,8
2. Disagree	19	36,5
3. Partially agree	14	26,9
4. Agree	15	28,8
5. Strongly agree	2	3,8



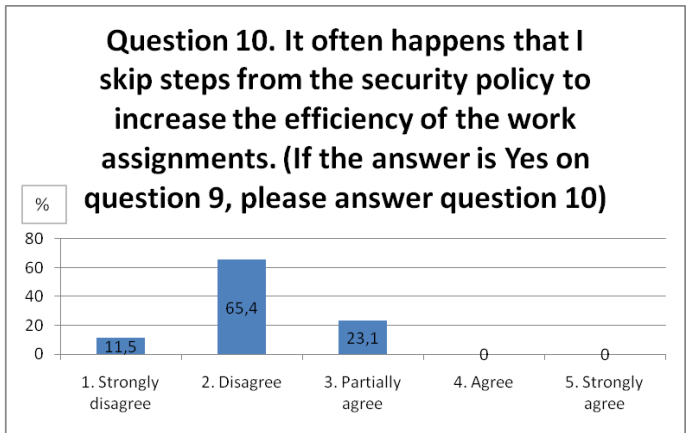
Question 9

Question 9. Has it happened that you skipped rules from the security policy just to increase your efficiency?		
Alternative	**Answers**	**%**
1. Yes	17	32,1
2. No	36	67,9



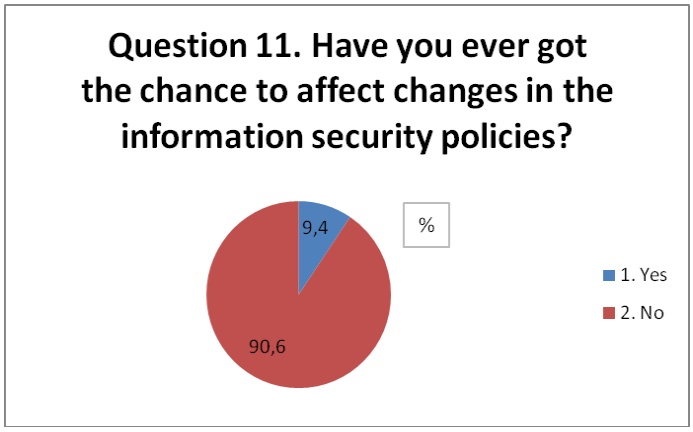
Question 10

Question 10. It often happens that I skip steps from the security policy to increase the efficiency of the work assignments. (If the answer is Yes on question 9, please answer question 10)		
Current average: 2.12 of 5		
Alternative	**Answers**	**%**
1. Strongly disagree	3	11,5
2. Disagree	17	65,4
3. Partially agree	6	23,1
4. Agree	0	0
5. Strongly agree	0	0



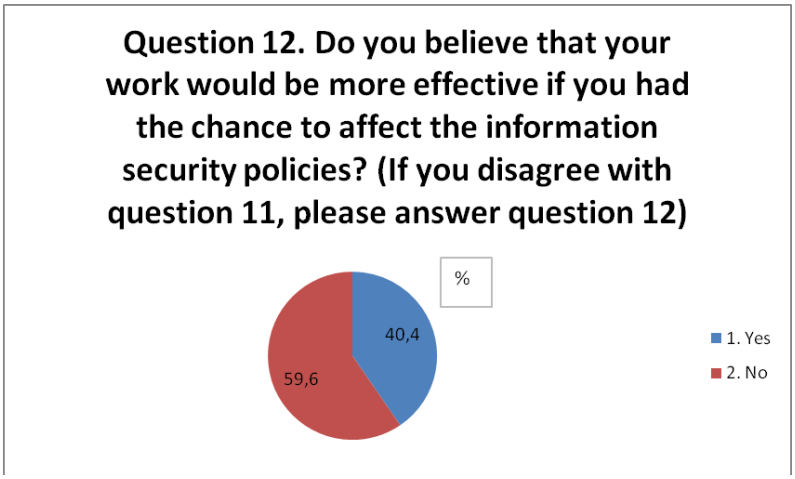
Question 11

Question 11. Have you ever got the chance to affect changes in the information security policies?		
Alternative	**Answers**	**%**
1. Yes	5	9,4
2. No	48	90,6



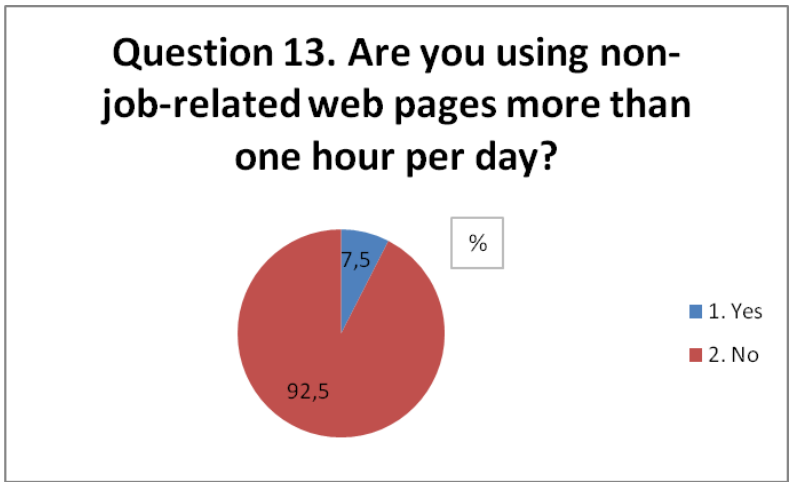
Question 12

Question 12. Do you believe that your work would be more effective if you had the chance to affect the information security policies? (If you disagree with question 11, please answer question 12)		
Alternative	**Answers**	**%**
1. Yes	19	40,4
2. No	28	59,6



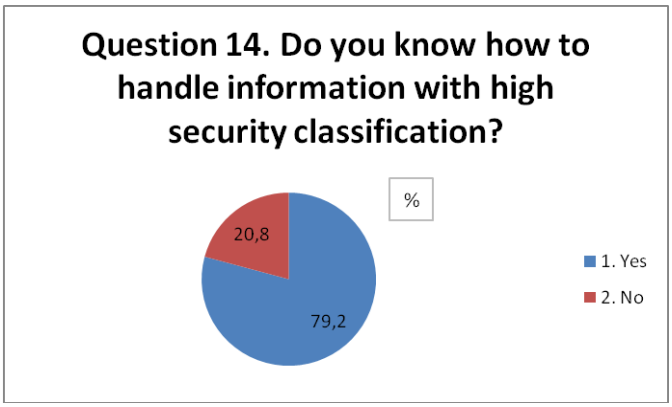
Question 13

Question 13. Are you using non-job-related web pages more than one hour per day?		
Alternative	**Answers**	**%**
1. Yes	4	7,5
2. No	49	92,5



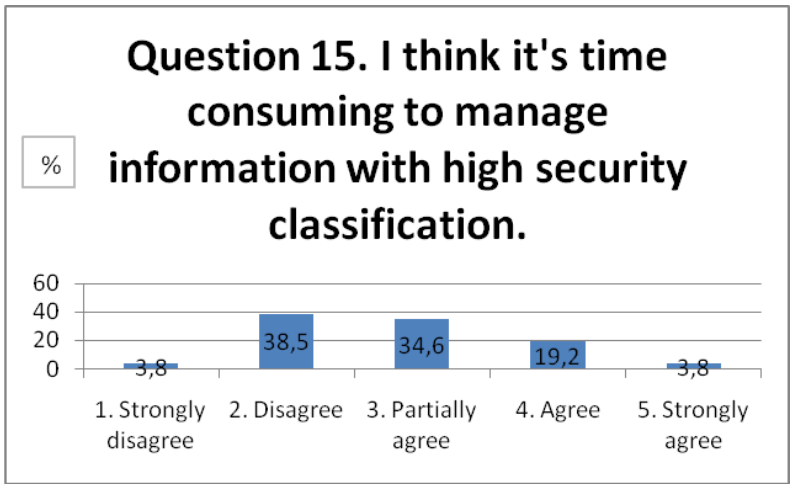
Question 14

Question 14. Do you know how to handle information with high security classification?		
Alternative	**Answers**	**%**
1. Yes	42	79,2
2. No	11	20,8



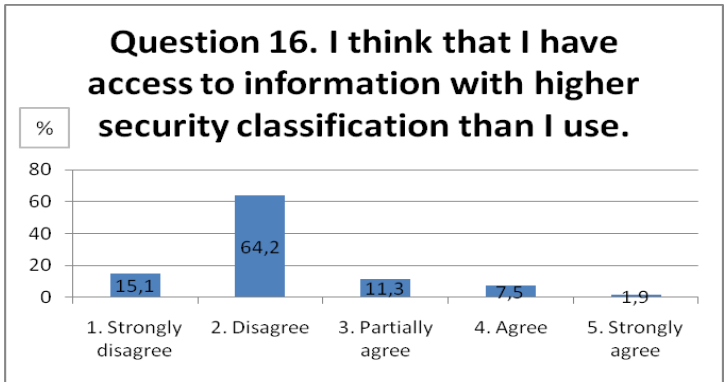
Question 15

Question 15. I think it's time consuming to manage information with high security classification.		
Current average: 2.81 of 5		
Alternative	**Answers**	**%**
1. Strongly disagree	2	3,8
2. Disagree	20	38,5
3. Partially agree	18	34,6
4. Agree	10	19,2
5. Strongly agree	2	3,8



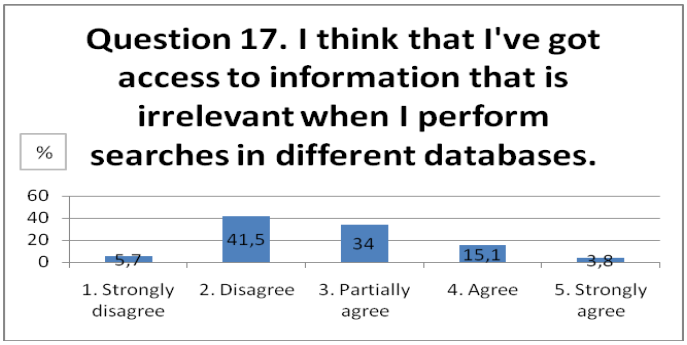
Question 16

Question 16. I think that I have access to information with higher security classification than I use.		
Current average: 2.17 of 5		
Alternative	**Answers**	**%**
1. Strongly disagree	8	15,1
2. Disagree	34	64,2
3. Partially agree	6	11,3
4. Agree	4	7,5
5. Strongly agree	1	1,9



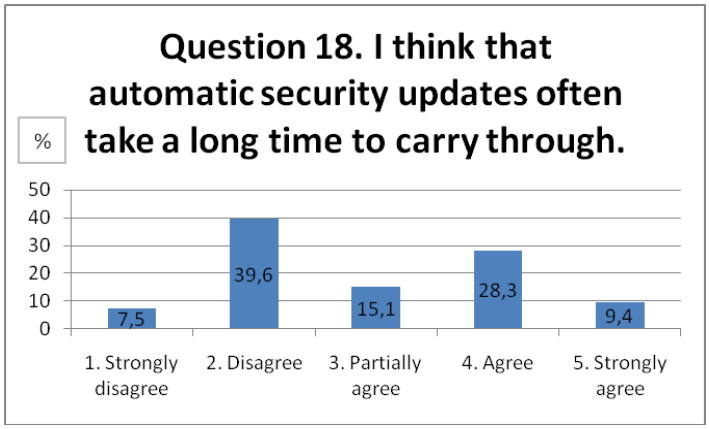
Question 17

Question 17. I think that I've got access to information that is irrelevant when I perform searches in different databases.		
Current average: 2.7 of 5		
Alternative	**Answers**	**%**
1. Strongly disagree	3	5,7
2. Disagree	22	41,5
3. Partially agree	18	34
4. Agree	8	15,1
5. Strongly agree	2	3,8



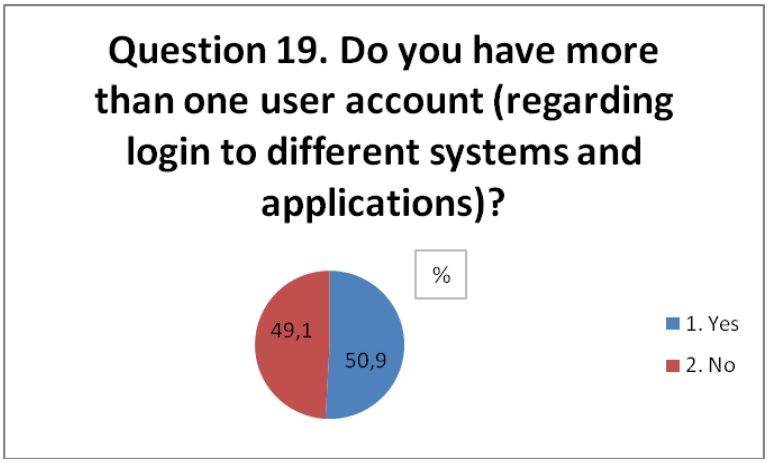
Question 18

Question 18. I think that automatic security updates often take a long time to carry through.		
Current average: 2.92 of 5		
Alternative	**Answers**	**%**
1. Strongly disagree	4	7,5
2. Disagree	21	39,6
3. Partially agree	8	15,1
4. Agree	15	28,3
5. Strongly agree	5	9,4



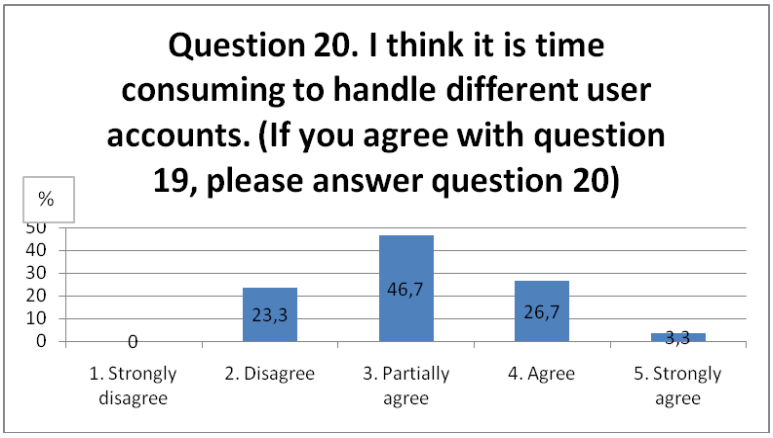
Question 19

Question 19. Do you have more than one user account (regarding login to different systems and applications)?		
Alternative	**Answers**	**%**
1. Yes	27	50,9
2. No	26	49,1



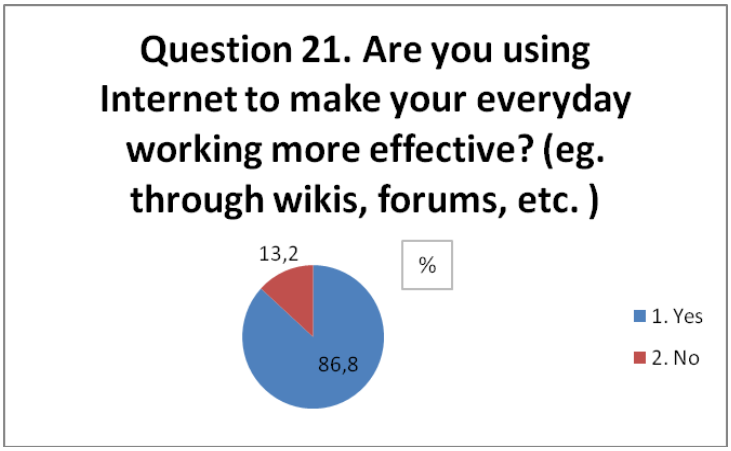
Question 20

Question 20. I think it is time consuming to handle different user accounts. (If you agree with question 19, please answer question 20)		
Current average: 3.1 of 5		
Alternative	**Answers**	**%**
1. Strongly disagree	0	0
2. Disagree	7	23,3
3. Partially agree	14	46,7
4. Agree	8	26,7
5. Strongly agree	1	3,3



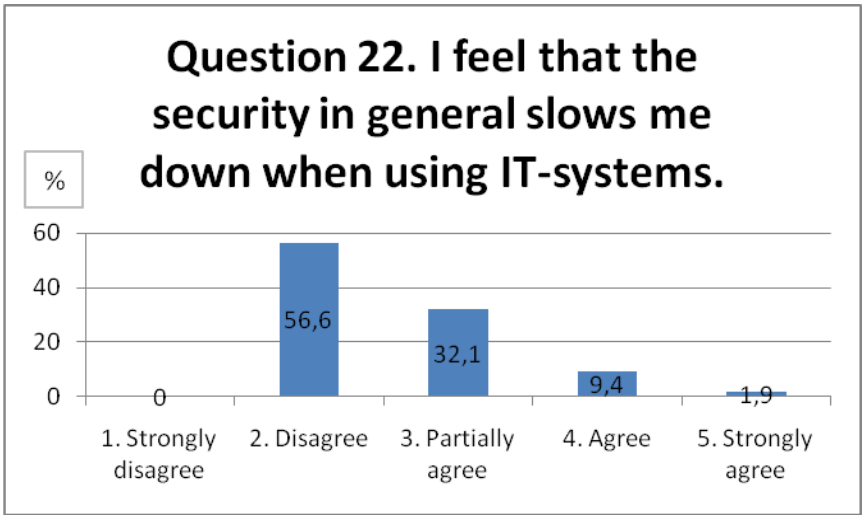
Question 21

Question 21. Are you using Internet to make your everyday working more effective? (eg. through wikis, forums, etc.)		
Alternative	**Answers**	**%**
1. Yes	46	86,8
2. No	7	13,2



Question 22

Question 22. I feel that the security in general slows me down when using IT-systems.		
Current average: 2.57 of 5		
Alternative	**Answers**	**%**
1. Strongly disagree	0	0
2. Disagree	30	56,6
3. Partially agree	17	32,1
4. Agree	5	9,4
5. Strongly agree	1	1,9



Bilaga 7 Enkät, Företag B, webbenkät

Effektivitet vs Informationssäkerhet

Syftet med Kandidatuppsatsen
Vi är tre studenter vid Lunds Universitet som ska göra en undersökning till vårt examensarbete på om informationssäkerhet påverkar effektivt användande av ett informationssystem. Effektivitet kan definieras som graden av måluppfyllelse i förhållande till resursanvändning.. I detta fall är användningen av resurser arbetstid. Vi vill mäta i vilken grad informationssäkerheten hindrar dig i ditt dagliga arbete med informationssystem.

Enkäten kommer att ta ca 5 minuter att besvara. Alla som deltar i undersökningen kommer att vara anonyma och varken vi eller någon annan kommer veta vem du är. Var vänlig att svara endast en gång på enkäten. Tack för ditt deltagande!

Fråga1. Jag känner till reglerna som gäller mig i företagets informationssäkerhetspolicy

- Instämmer helt
- Instämmer till stor del
- Instämmer till viss del
- Instämmer lite
- Instämmer inte alls

Fråga2. Känner du att ditt arbete innehåller för många säkerhetsregler, då du ska utföra vissa uppgifter.

- Ja
- Nej

Fråga3. Jag anser att min chef har påverkat mitt säkerhetsmedvetande i stor utsträckning.

- Instämmer helt
- Instämmer till stor del
- Instämmer till viss del
- Instämmer lite
- Instämmer inte alls

Fråga4. Har du mer än ett användarkonto? (Vid inloggning av olika system och applikationer på företaget)

- Ja
- Nej

Fråga5. Jag anser att det är tidskrävande att hantera olika användarkonton.

- Instämmer helt
- Instämmer till stor del
- Instämmer till viss del
- Instämmer lite
- Instämmer inte alls

Fråga6. Jag anser att det är tidskrävande att logga in i de olika systemen

- Instämmer helt
- Instämmer till stor del
- Instämmer till viss del
- Instämmer lite
- Instämmer inte alls

Fråga7. Jag anser att det är tidskrävande att byta lösenord.

- Instämmer helt
- Instämmer till stor del
- Instämmer till viss del
- Instämmer lite
- Instämmer inte alls

Fråga8. Jag anser att det är tidskrävande att hämta nytt lösenord då jag glömt mitt gamla.

- Instämmer helt
- Instämmer till stor del
- Instämmer till viss del
- Instämmer lite
- Instämmer inte alls

Fråga9. Jag anser att det är tidskrävande att följa säkerhetspolicy vid dokumenthantering.

- Instämmer helt
- Instämmer till stor del
- Instämmer till viss del
- Instämmer lite
- Instämmer inte alls

Fråga10. Jag anser att den utbildning jag fått gällande informationssäkerhet har gjort så att jag på ett effektivare sätt kan utföra mitt arbete.

- Instämmer helt
- Instämmer till stor del
- Instämmer till viss del
- Instämmer lite
- Instämmer inte alls

Fråga11. Har det hänt att du "hoppat över" regler från säkerhetspolicyn för att effektivisera din arbetsuppgift?

- Ja
- Nej

Fråga12. (Om svaret är Ja på fråga 11, besvara fråga 12) Jag går ofta runt säkerhetspolicyn för att effektivisera mina arbetsuppgifter.

- Instämmer helt
- Instämmer till stor del
- Instämmer till viss del
- Instämmer lite
- Instämmer inte alls

Fråga13. Har du någon gång fått påverka förändringar i informationssäkerhetspolicyn?

- Ja
- Nej

Fråga14. Anser du att ert arbete skulle effektiviseras om ni hade chans att påverka informationssäkerhetspolicyn?

- Ja
- Nej

Fråga15. Använder du internet sidor som inte är arbetsrelaterade mer än en timme om dagen?

- Ja
- Nej

Fråga16. Känner du till hur du bör hantera information med hög säkerhetsklassificering?

- Ja
- Nej

Fråga17. (Om svaret är Ja på fråga 16, besvara fråga 17) Jag anser att det är tidskrävande att hantera information med hög säkerhetsklassificering.

- Instämmer helt
- Instämmer till stor del
- Instämmer till viss del
- Instämmer lite
- Instämmer inte alls

Fråga18. Jag anser att jag har tillgång till information som har högre säkerhetsklassificering än vad jag använder.

- Instämmer helt
- Instämmer till stor del
- Instämmer till viss del
- Instämmer lite
- Instämmer inte alls

Fråga19. Jag anser att jag har access till irrelevant information när jag gör sökningar i olika databaser på företaget. (sökningar resulterar i för mycket information som måste granskas för att finna det jag söker)

- Instämmer helt
- Instämmer till stor del
- Instämmer till viss del
- Instämmer lite
- Instämmer inte alls

Fråga20. Sker det ofta automatiska uppdateringar på din arbetsstation under arbetstid (vilket medför att datorn måste startas om o.s.v.)?

- Ja
- Nej

Fråga21. Jag anser att automatiska säkerhetsuppdateringar ofta tar lång tid att genomföra.

- Instämmer helt
- Instämmer till stor del
- Instämmer till viss del
- Instämmer lite
- Instämmer inte alls

Fråga22. Använder du internet för att effektivisera ditt vardagliga arbete på företaget? (via ex wikis, forum m.m.)?

- Ja
- Nej

Fråga23. Jag upplever att säkerheten gennerellt bromsar mitt effektiva avändande av IT-system.

- Instämmer helt
- Instämmer till stor del
- Instämmer till viss del
- Instämmer lite
- Instämmer inte alls

Skicka

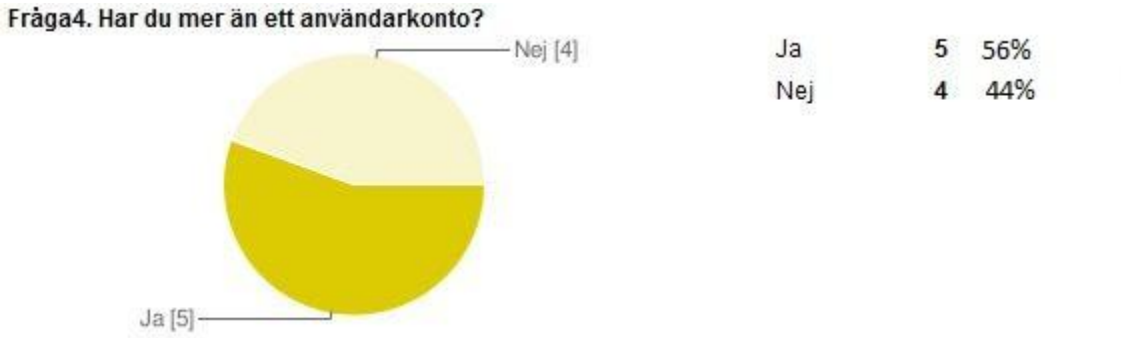
Bilaga 8 Resultat, Enkät, Företag B

Fråga 1

Fråga 2

Fråga 3

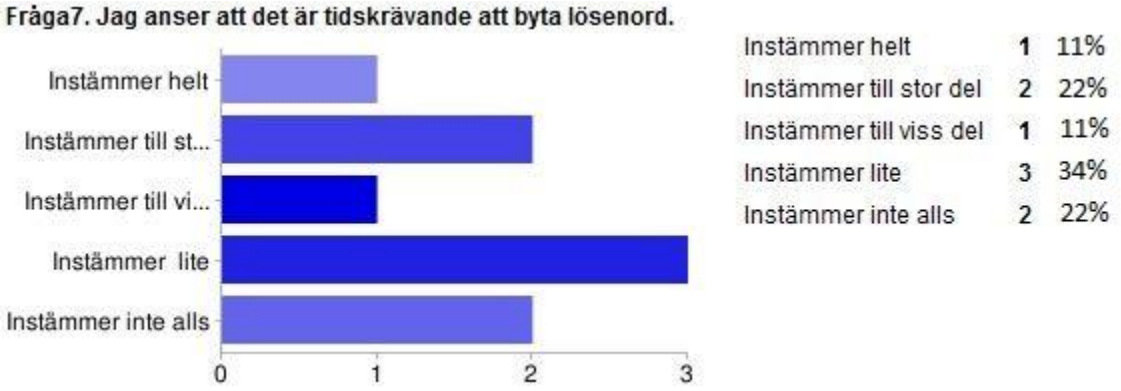
Fråga 4



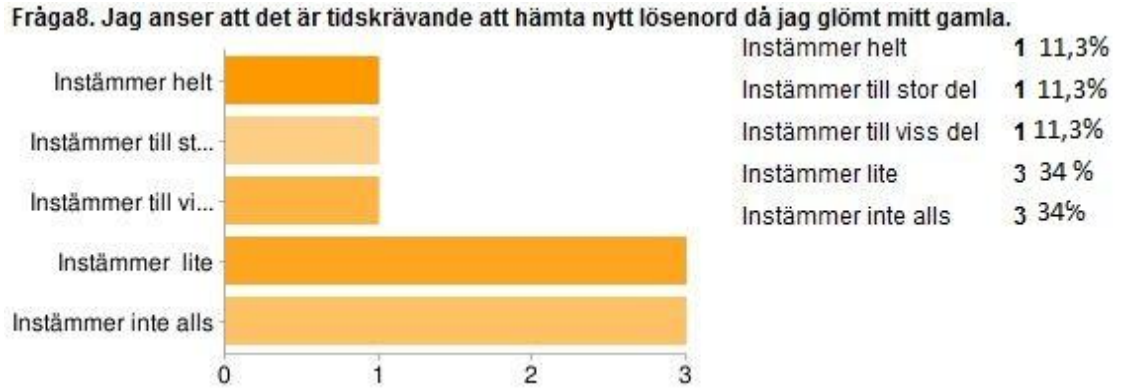
Fråga 5

Fråga 6

Fråga 7



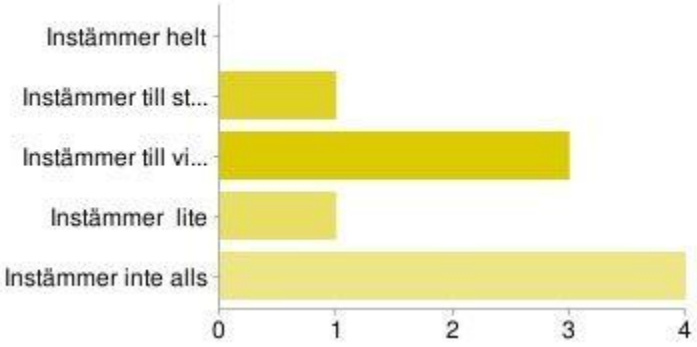
Fråga 8



Fråga 9

Fråga 10

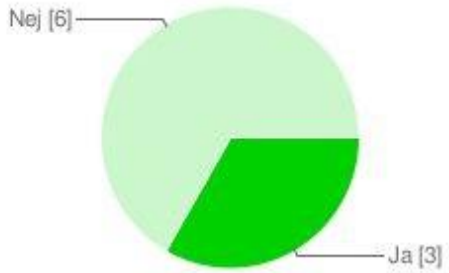
Fråga10. Jag anser att den utbildning jag fått gällande informationssäkerhet har gjort så att jag på ett effektivare sätt kan utföra mitt arbete.



Instämmer helt	0	
Instämmer till stor del	1	
Instämmer till viss del	3	34%
Instämmer lite	1	11%
Instämmer inte alls	4	45%

Fråga 11

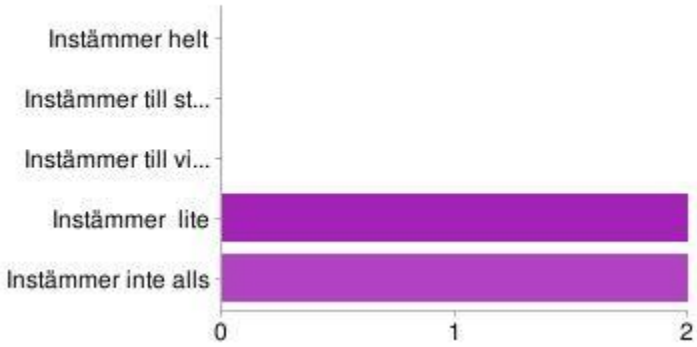
Fråga11. Har det hänt att du "hoppat över" regler från säkerhetspolicyn för att effektivisera din arbetsuppgift?



Ja	3	34%
Nej	6	66%

Fråga 12

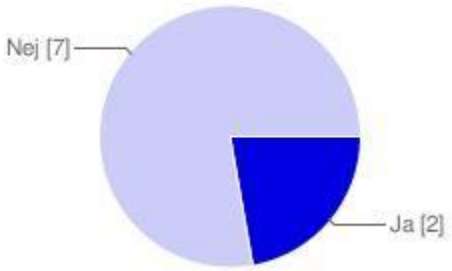
Fråga12. (Om svaret är Ja på fråga 11, besvara fråga 12) Jag går ofta runt säkerhetspolicyn för att effektivisera mina arbetsuppgifter.



Instämmer helt	0	
Instämmer till stor del	0	
Instämmer till viss del	0	
Instämmer lite	2	22%
Instämmer inte alls	2	22%

Fråga 13

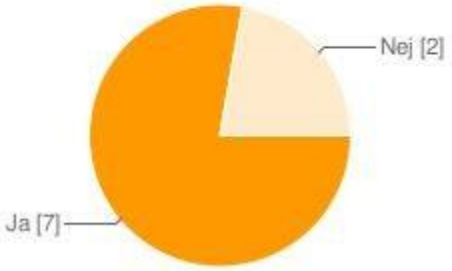
Fråga13. Har du någon gång fått påverka förändringar i informationssäkerhetspolicyn?



Ja	2	22%
Nej	7	78%

Fråga 14

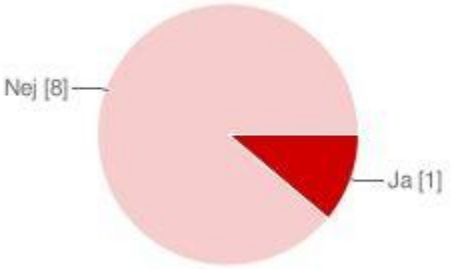
Fråga14. Anser du att ert arbete skulle effektiviseras om ni hade chans att påverka informationssäkerhetspolicyn?



Ja	7	78%
Nej	2	22%

Fråga 15

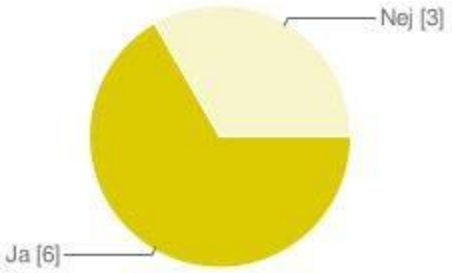
Fråga15. Använder du internet sidor som inte är arbetsrelaterade mer än en timme om dagen?



Ja	1	11%
Nej	8	89%

Fråga 16

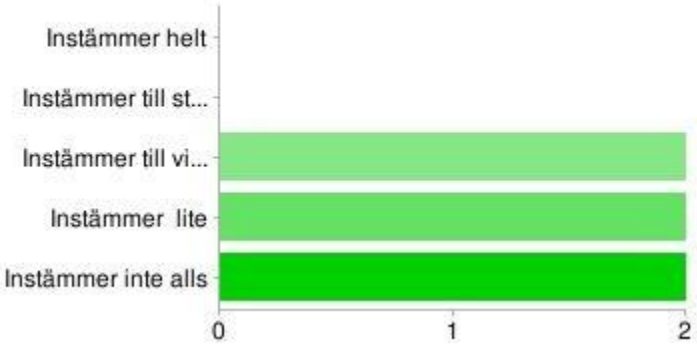
Fråga16. Känner du till hur du bör hantera information med hög säkerhetsklassificering?



Ja	6	66%
Nej	3	34%

Fråga 17

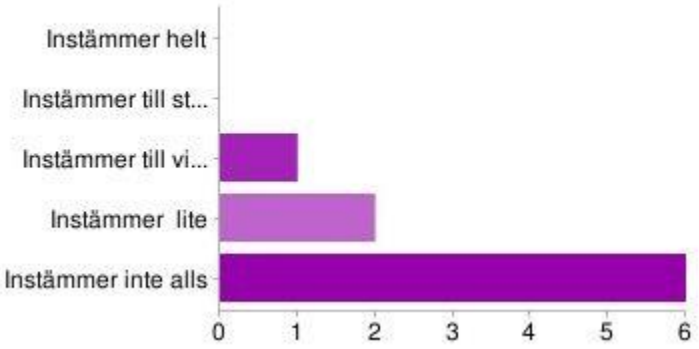
Fråga17. (Om svaret är Ja på fråga 16, besvara fråga 17) Jag anser att det är tidskrävande att hantera information med hög säkerhetsklassificering.



Instämmer helt	0	
Instämmer till stor del	0	
Instämmer till viss del	2	22%
Instämmer lite	2	22%
Instämmer inte alls	2	22%

Fråga 18

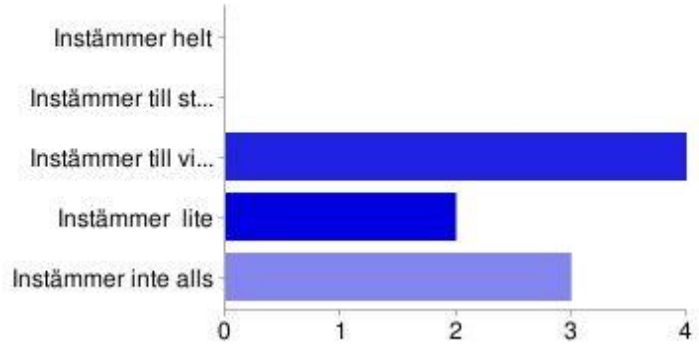
Fråga18. Jag anser att jag har tillgång till information som har högre säkerhetsklassificering än vad jag använder.



Instämmer helt	0	
Instämmer till stor del	0	
Instämmer till viss del	1	11%
Instämmer lite	2	22%
Instämmer inte alls	6	67%

Fråga 19

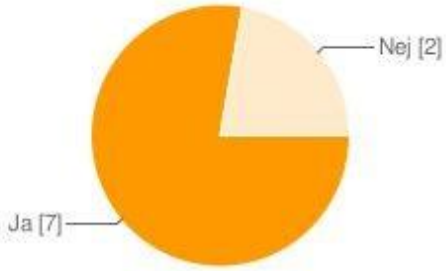
Fråga19. Jag anser att jag har access till irrelevant information när jag gör sökningar i olika databaser på företaget.



Instämmer helt	0	
Instämmer till stor del	0	
Instämmer till viss del	4	44%
Instämmer lite	2	22%
Instämmer inte alls	3	34%

Fråga 20

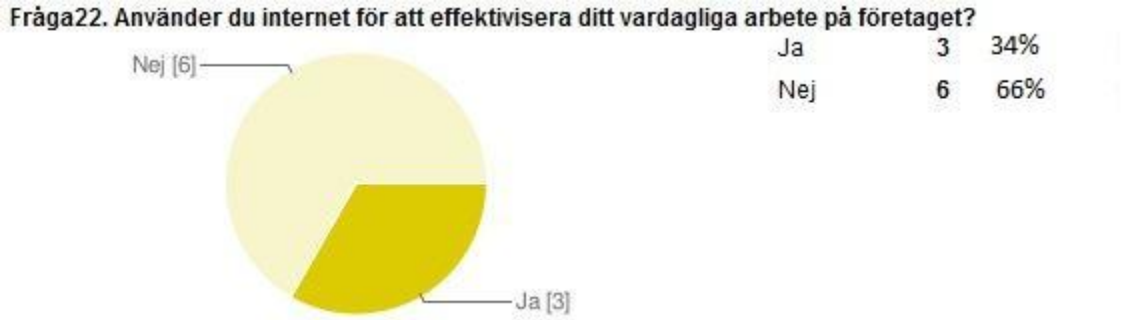
Fråga20. Sker det ofta automatiska uppdateringar på din arbetsstation under arbetstid (vilket medför att datorn måste startas om o.s.v.)?



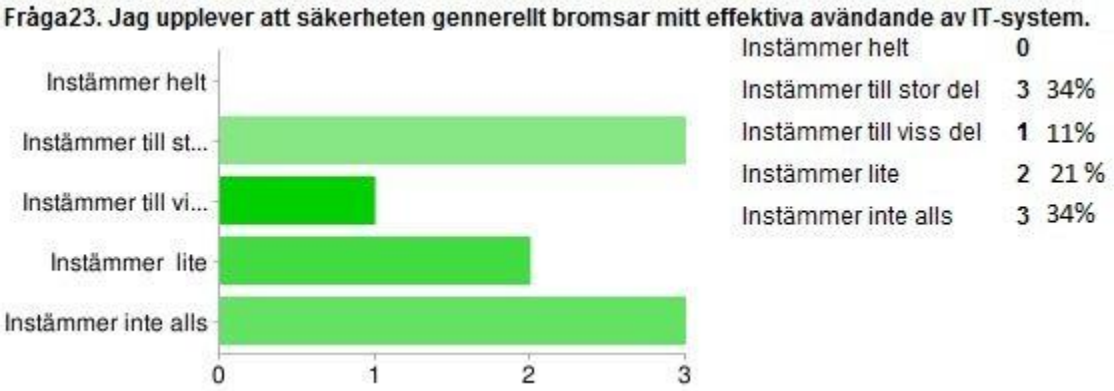
Ja	7	78%
Nej	2	22%

Fråga 21

Fråga 22



Fråga 23



Bilaga 9 Formelsamling & Uträckningar

medelvärde $\bar{x}$

$$\bar{x} = \frac{1}{n}\sum_{j=1}^{n} x_j = \frac{x_1 + x_2 + \cdots + x_n}{n}$$

där *n* är antalet observationer $x_1, x_2, \ldots, x_n$

standardavvikelse *s*

$$s = \sqrt{\frac{1}{n-1}\sum_{j=1}^{n}(x_j - \bar{x})^2}$$

där *n* är antalet observationer $x_1, x_2, \ldots, x_n$ och $\bar{x}$ medelvärdet

Uträkningar på flervalsfrågor med rangordnade svarsalternativ. Frågeföljd enligt Bilaga 7.

		antal svar för varje betyg							
	Företag	**5**	**4**	**3**	**2**	**1**	**antal svar**	**medelvärde**	**standardavvikelse**
fråga 1	**A**	9	36	7	1	0	53	4,00	0,62
	B	4	5	0	0	0	9	4,44	0,53
fråga 3	**A**	2	16	20	13	1	52	3,10	0,89
	B	0	2	3	2	2	9	2,56	1,13
fråga 5	**A**	1	8	14	7	0	30	3,10	0,80
	B	1	0	0	5	3	9	2,00	1,22
fråga 6	**A**	5	13	21	14	0	53	3,17	0,94
	B	2	0	2	3	2	9	2,67	1,50
fråga 7	**A**	5	14	14	16	4	53	3,00	1,13
	B	1	2	1	3	2	9	2,67	1,41
fråga 8	**A**	4	9	11	25	2	51	2,76	1,05
	B	1	1	1	3	3	9	2,33	1,41
fråga 9	**A**	0	7	17	25	4	53	2,51	0,82
	B	0	0	4	2	3	9	2,11	0,93
fråga 10	**A**	2	15	14	19	2	52	2,92	0,99
	B	0	1	3	1	4	9	2,11	1,17
fråga 12	**A**	0	0	6	17	3	26	2,12	0,59
	B	0	0	0	2	2	4	1,50	0,58

fråga 17	**A**	2	10	18	20	2	52	2,81	0,93
	B	0	0	2	2	2	6	2,00	0,89
fråga 18	**A**	1	4	6	34	8	53	2,17	0,85
	B	0	0	1	2	6	9	1,44	0,73
fråga 19	**A**	2	8	18	22	3	53	2,70	0,93
	B	0	0	4	2	3	9	2,11	0,93
fråga 21	**A**	5	15	8	21	4	53	2,92	1,17
	B	3	0	5	1	0	9	3,56	1,13
fråga 23	**A**	1	2	17	30	0	50	2,48	0,68
	B	0	3	1	2	3	9	2,44	1,33

REFERENSLISTA

Alter, S. (2006): *The work system method - Connecting people, Processes and IT for Business Results*. California, work system press.

Arnesen, D. W. & William, L. (2007): Developing an effective company policy for employee internet and email use, United Kingdom, In*: Journal of Organizational Culture*, Communications and Conflict, volym 11, nr. 2, sid. 53-65.

Applegate, S.D. (2009): Social Engineering: Hacking the Wetware! In: *Information Security Journal*: A Global Perspective , volym. 18, sid 40-47.

Bandura A. & Jourden F. J. (1991): *Self-regulatory mechanisms governing the impact of social comparison on complex decision making*, Journal of Personality and Social Psychology, Stanford University.

Blom, G., Enger, J., Englund, G. Grandell, J. och Holst, L. (2005): *Sannolikhetsteori och statistikteori med tillämpningar*, Lund, Studentlitteratur.

Brodkin J. (2008): Network World, Businesses Block Social Networks (Elektronisk). Tillgänglig på: www.pcworld.com/businesscenter/article/148663/businesses_block_social_networks.html, (Åtkomstdatum 4 maj 2010).

Daft, R. L. (2007): *Organization Theory and Design*. In: Canada, Gengage Learning 2007.

De la Hoz, E., García, A., Marsá-Maestre, I., Ángel López-Carmona, M. & Alarcos, B. (2009): *An Infocard-based proposal for unified single sign on*. In: Ninth Annual International Symposium on Applications and the Internet, Department of Automatica, University of Alcala.

Denemark, J., Matyska, L. & Ruda, M. (2005): *User Management for Virtual Organizations*: In: CoreGRID Technical Report, Institute of Computer Science, Masaryk University.

Dhillon G. & Backhouse J. (2000): Information system security management in the new millennium. In: *Technical Opinion*, volym. 43 nr. 7 sid. 126-128 .

Doherty N. F. & Fulford H. (2006): Aligning the information security policy with the strategic information systems plan. In: *Computers & Security*, volym 25, sid. 55-63.

Dutta, A. & Roy, R. (2008) : Dynamics of organizational information Security. In: *System Dynamics Review*, volym 24, nr. 3, sid. 349-375.

Gonzalez J. J. & Sawicka A (2002): *A Framework for Human Factors in Information Security*. In: 2002 WSEAS Int. Conf. on Information Security - Rio de Janeiro, Dept. of Information and Communication Technology, Agder University College.

Hyeun-Suk R, Kim, C. & Ryu, Y. U. (2009): Self-efficacy in information security: Its influence on end users' information security practice behavior, In: *Computer & Security,* volym 28, sid. 816-826.

Höne K & Eloff J. (2002): What makes an effective security policy? In: *Network Security*, volym 2002, nr. 6 sid 14-16.

ISO, (2009): International Standard Information technology - Security techniques - Information security management systems - Overview and vocabulary In: Switzerland.

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

Kamel, M., Benzekri, A., Barrere, F. & Laborde, R. (2007*): Evaluating the conformity of an access control architecture for Virtual Organizations with ISO/IEC 17799*. IRIT Toulouse, Universite Paul Sabatier

Karyda M, Kiountouzisa, E. & Kokolakis, S. (2005): *Information systems security policies: a contextual perspective*. In: *Computer & Security*, volym 24, sid. 146-160.

Layton, T P, (2007): *Information security: design, implementation, measurement, and compliance*. In: Florida, Auerbach Publications.

Lee Y, Kozar A. (2005): Investigating factors affecting adoption of anti-spyware systems. In: *Communications of the ACM,* volym 48, nr 8, sid. 72-77.

Oberlaender, M, (2010): *Comment: The magic triangle of information security* (Elektronisk). Tillgänglig på: http://www.infosecurity-us.com/view/6693/comment-the-magic-triangle-of-information-security/ (Åtkomstdatum19 maj 2010)

Potter, S. & Nieh, J. (2005): *Reducing Downtime Due to System Maintenance and Upgrades*. In: USENIX Association, December, sid. 47-62.

Rees, J., Bandyopadhay, S. & Spafford, E. H. (2003): PFIRES: A Policy Framework for Information Security. In: Communications of the ACM 2003, nr 7, volym 46, sid. 101-107.

Rescorla, E. (2003): *Proceedings of the 12th USENIX Security Symposium*. In: USENIX Association. sid. 75-90.

Saran M. & Zavarsky P. (2009): *A Study of the Methods for Improving Internet Usage Policy Compliance,* In: Information Systems Security Management, Concordia University College of Alberta.

Sfakiyanudis, E. (2008): Unclogging networks. In: *Government Technology*, Prism business media American City & County. sid. 24

Simms, D. (2009): *Information security optimization: from theory to practice*. In: 2009 International Conference on Availability, Reliability and Security. Faculty of Business and Economics. University of Lausanne.

Straub, D.W. & Welke, R.J. (1998): Coping with systems risk: security planning models for management decision making. In: *Management Information System Research Center*. Vol. 22 No. 4 sid. 441–469.

Torkzadeh, R., Pflughoeft, K. & Hall, L. (1999): Computer self-efficacy, training effectiveness and user attitudes: an empirical study. In: *Behavior and Information Technology, Information and Decisions Sciences Department*, volym 18, no. 4, sid. 299-309.

van Aken, J. E., Berends, H. & van der Bij, H.(2007): *Problem solving in organizations: A Methodological Handbook for Business Students*; Cambridge University Press, United States of America

Van Niekerk, J.F. & Von Solms, R. (2010): Information security culture: A management perspective. In: *Computers & Security*, volym 29, nr 4, sid 476-486.

Websense, Inc., (2006): Viewing Adult Content at Work, Infecting Company with Malicious Spyware Cited as Top Concerns for Putting Job on the Line, In: u o Internet: http://investor.websense.com/releasedetail.cfm?ReleaseID=285092 (28 april 2010)

Whitman, M E. & Mattord, H J. (2009): Principles of Information Security. In: Canada, Thomson Course Technology.