LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för Informatik

Säkerhetsmedvetande i en organisation som hanterar känslig information

Kandidatuppsats 15 hp, SYSK02 i informatik
Framlagd: maj 2016

Författare: Robert Andersson
Mathias Meltzer

Handledare: Anders Svensson

Examinatorer: Agneta Olerup
Mirella Muhic

Säkerhetsmedvetande i en organisation som hanterar känslig information

Författare: Robert Andersson och Mathias Meltzer

Utgivare: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

Dokumenttyp: Kandidatuppsats

Antal sidor: 71

Nyckelord: Säkerhetsmedvetenhet, IT-säkerhet, autentisering, lösenord, utbildning, säkerhetskopiering, datamissbruk, övervakning, konfidentialitet

Sammanfattning

Vår uppsats undersöker hur säkerhetsmedvetna försäkringsförmedlare i ett försäkringsbolag är. De samlar in och behandlar känslig information dagligen och det är då rimligt att anta att det ska finnas en hög säkerhetsmedvetenhet. Vi har tagit hjälp av motivationsteorin Temporal Motivation Theory (TMT) för att bygga vår undersökningsmodell. Efter att ha granskat litteratur har vi identifierat aktiviteter som vi anser kan användas regelbundet i ett försäkringsbolags verksamhet. Vi har sedan tagit en kvalitativ ansats i form av semistrukturerade intervjuer baserat på vårt litteraturkapitel och motivationsteorin TMT som har lett fram till insamlingen av vårt empiriska resultat.
Vi har genomfört fem intervjuer med försäkringsförmedlare på ett försäkringsbolag som finns lokaliserat i nordvästra Skåne.
Våra resultat visar bland annat på individuella skillnader i säkerhetsmedvetandet bland våra intervjupersoner gällande hur de hanterar lösenord men även ett gemensamt säkerhetsmedvetande när det kommer till att skydda konfidentiell information.

Innehållsförteckning

Figurer

Tabellförteckning

Ordlista

ISP - Information security policy.

TMT - Temporal Motivation Theory.

Aktivitet - En uppgift eller funktion som försäkringsförmedlarna utför, använder eller utsätts för regelbundet.

Mobil användning - Att använda mobila enheter så som laptops, surfplattor och mobiler när man arbetar i nätverk som inte är företagets.

1. Introduktion

Dagens teknik erbjuder alla typer av människor och företag nya sätt att interagera och arbeta på. Man behöver exempelvis inte längre vara uppkopplad via en dator och ett wifi för att chatta med sina vänner eller skicka arbetsrelaterade mejl. Idag räcker det med att användaren har en smartphone för att kunna utföra dessa aktiviteter. Det går att konstatera att dataintrången har ökat de senaste åren (Knapp et. al. 2009) samtidigt som ny teknik utvecklas och uppgraderas i dagens samhälle. Med detta sagt är det dock ett ständigt återkommande problem som verkar bestå eller åtminstone inte håller samma utvecklingskurva som produktionen av ny teknik, nämligen användarens säkerhetsmedvetenhet. En gemensam nämnare för många företag och deras respektive Information System Managers (ISM) är synen på den dagliga användaren, i vårt fall försäkringsförmedlaren, som den svagaste länken i ett informationssystem (IS) (Bulgurcu et. al. 2010; Warkentin & Willison, 2009). Med andra ord menar de att det inte spelar någon större roll vilka säkerhetsåtgärder företaget har tilltagit, såsom exempelvis virusskydd och Information Security Policies (ISP), ifall användaren inte klarar av att hantera, följa alternativt har motivationen att följa dessa.

IS-säkerhetsmedvetenhet hos användare prioriteras inte alltid tillräckligt vilket tänkta kunder kan se som en stor nackdel eftersom de då kan känna sig otrygga i att lämna över känslig information. Företaget och dess anställda bör ha en god kunskap i hur man hanterar och skyddar känslig information för att bli framgångsrika i sin verksamhet (Chen et. al. 2006).
Risken finns att många användare tar för givet att IS-säkerheten är något som IT-avdelningen ska ta ansvar för och lämnar därmed över hela ansvaret till dem (Workman et. al. 2008).

1.1 Problemområde

Ny teknik och nya funktioner medför inte enbart fördelar för företag och de anställda, utan även risker kan uppstå. Oavsett hur välbyggt ett företags IS är, så är det ändå i slutändan upp till de anställda att arbeta med det på rätt sätt. Det spelar ingen roll om ett företag sätter upp diverse policys om till exempel lösenordshantering om användaren inte följer dessa fullt ut (Bulgurcu et. al. 2010). Eftersom informationssäkerhetens fokus idag ligger på individen och det organisatoriska perspektivet har medarbetarnas uppföljningsförmåga framkommit som en viktig faktor, eftersom medarbetarna ofta ses som den svagaste länken i informationssäkerhet (Bulgurcu et. al. 2010). Uppskattningsvis är över hälften av alla informationsläckor inom ett IS direkt eller indirekt orsakat av användarens bristfälliga säkerhetsmedvetande (Siponen & Vance, 2010). Att konstatera så finns det stora risker för företag som behandlar känslig information även om företaget har ett bra informationssäkerhetssystem och konsekvenserna vid en informationsläcka kan bli stora. Enligt en amerikansk undersökning skulle 46% av de tillfrågade byta försäkringsbolag om känslig information skulle läcka ut och spridas (Alvarez, 2013).

1.2 Forskningsfråga

Hur ser de anställdas säkerhetsmedvetenhet ut inom ett försäkringsbolag som hanterar känslig information?

1.3 Syfte

Syftet med undersökningen är att ta reda på hur säkerhetsmedvetenheten ser ut hos de anställda inom ett försäkringsbolag och hur deras inställning till informationssäkerhet ser ut. Vidare vill vi också ta reda på deras motivation till utvalda aktiviteter.

1.4 Avgränsningar

Vi har valt att fokusera på säkerhetsmedvetande från det mänskliga perspektivet i vår uppsats och vi kommer därför bortse från virusprogram, brandväggar och liknande skydd.
Vi har valt att studera ett försäkringsbolag beläget i nordvästra Skåne.
Vi kommer inte att applicera någon formel på TMT i vårt resultat eftersom vi inte kommer kunna generalisera svaren, utan vi vill istället se sambanden och analysera en helhetsbild från intervjupersonerna.

2. Litteraturgenomgång

I detta kapitel börjar vi med att presentera Temporal Motivation Theory (TMT) som är en motivationsteori för att kunna undersöka hur motiverad en individ är till att genomföra en uppgift. Därefter presenterar vi de aktiviteter som vi applicerat TMT på och har hittat gemensamma för de artiklar som vi har funnit intressanta och relevanta gällande säkerhetsmedvetandet i ett företag och därmed också för vår uppsats. Aktiviteterna är sådana som vi har anledning till att tro att de utförs dagligen eller åtminstone bör utföras regelbundet efter att ha studerat litteraturen och att det krävs en god säkerhetsmedvetenhet när de utförs. Vi presenterar dessa för att kunna få en teoretisk grund som vi kan basera vår undersökning på för att till slut kunna uppnå vårt syfte med uppsatsen och kunna svara på vår forskningsfråga.

2.1 Temporal Motivation Theory

TMT är en motivationsteori där tid är en motiverande och avgörande faktor. Närmare bestämt hur användaren värdesätter och motiverar sina val och handlingar mot varandra i förhållande till tiden det tar att utföra dessa. Ett exempel kan vara när en användare ska logga in och väljer att antingen skriva in sitt användarnamn och lösenord vid varje inloggning jämfört med att spara uppgifterna för att kunna logga in med ett enda knapptryck. TMT tar i beräkning hur användaren tar ställning till sitt val i förhållandet till tiden det tar att utföra aktiviteten.

Generellt när man talar om teorier som beskriver mänskliga sätt och handlingar, så finns det olika sätt att applicera motivationsteorin TMT (Steel & König, 2006). TMT är en lämplig teori som kan användas för förklarande situationer där förväntad förmåga, värde, tid och belöning påverkar beslutsfattande samtidigt och där dessa aspekter influeras av individuella olikheter (Steel & König, 2006). Vidare så menar Steel & König (2006) att en genomförbar teori måste innehålla variabler som använder sig av förväntad förmåga, värde, tid och belöning både på individuella- och situationsbaserade nivåer. TMT:s aspekters samband kan enligt Steel (2007) beskrivas enligt följande formel:

$$\text{Utility} = \frac{\text{Expectancy X Value}}{\text{Impulsiveness X Delay}}$$

Figur 2.1 TMT:s samband enligt Steel (2007)

Utility visar hur önskvärd en uppgift är för en individ. Expectancy representerar den förväntade förmågan att utföra en aktivitet hos en individ och value står för värdet av aktiviteten. Impulsiveness representerar tiden, hur ofta aktiviteten utförs och vilken tid det tar att utföra den medan delay står för belöningen av att utföra aktiviteten.

Förväntad förmåga representerar den upplevda sannolikheten att resultatet man vill uppnå inträffar. Precis som aspekten värde, så påverkas den förväntade förmågan av både situations- och

individuella skillnader. Olika aktiviteter har högre och lägre sannolikheter att de kommer att inträffa, men där är också stabila trender angående hur människan i slutändan uppfattar dessa sannolikheter. Vi tenderar till att överskatta aktiviteter med låg sannolikhet, och underskatta aktiviteter med hög sannolikhet. Dessutom finns det generaliserade förväntningar som ökar och minskar, där specifika personlighetsdrag som påverkar förväntningen är utmärkande egenskaper, egen förmåga och optimism (Steel & König, 2006).

Värde representerar vilken tillfredsställelse eller hur stor reducering av driv resultatet eller utfallet tros uppnå. Attraktionskraften av en aktivitet beror även vid denna aspekt på både situations- och individuella skillnader, där resultaten av aktiviteterna kan tillfredsställa behoven på olika nivåer. Exempelvis när det gäller individuella skillnader, så skiljer sig människors vanor och behov. För att kunna förutse värdet av en aktivitet för en specifik person och personens val, måste man avgöra behovet av kraft som krävs och vilken tillfredsställelse som uppnåtts. Om individen ser ett högt behov av kraft och ingen belöning av en aktivitet så kommer också värdet att bli obetydligt (Steel & König, 2006).

Den tredje aspekten behandlar effekten av tid. Den beskrivs som människans känslighet för fördröjning (Steel & König, 2006). Monterosso & Ainslie (1999) menar att känslighet för fördröjning i stort sett motsvarar impulsivitet. Vidare menar Steel & König (2006) att impulsivitet bör alltid vara med i någon grad och är mestadels stabil, även om det kan finnas miljöfaktorer. Känsligheten för fördröjning kan också innebära bristande självkontroll och olika individers grad av distrahering. Något som också nämns under aspekten tid är själva fördröjningen i sig, vilket innebär själva tiden det tar att utföra aktiviteten.

Den sista aspekten, belöning, indikerar att varje komponent i TMT påverkas av individuella skillnader (förväntad förmåga, värde och tid). Det finns ytterligare skillnader beroende på om huruvida resultatet upplevs negativt eller positivt. Exempelvis kan människor önska fördröjningar om de får uppskattade belöningar och då kan samma resultat uppfattas som en förlust eller en vinst (Steel & König, 2006).

2.2 Aktiviteter berörande IS-säkerhet

Nedan presenterar vi de aktiviteter som vi fann relevanta att undersöka efter vår litteraturgranskning.

2.2.1 Autentisering

Den vanligaste formen av autentisering idag är lösenord, andra alternativ är biometriska som exempelvis scanning av fingeravtryck och smartcards (Stamp, 2006). En studie visar att en användare ofta inte byter sitt lösenord förrän kontot eller annan känslig information har blivit utsatt för någon form av hot. Då kan det redan vara för sent och skadan vara skedd (Adams & Sasse, 1999).

Kontroller för informationstillgång är otillräckliga för att ge ett fullständigt skydd av känslig information, även med kryptering så kan systemen för säkerhetskopiering nås via osäkra

administrativa gränssnitt. Busson (2008) nämner att det bedöms att över 70 % av överträdelserna i ett informationssystem (IS) ursprungligen är interna. De som gör sig skyldiga till dataintrången är ofta auktoriserade till nätverket, har kunskap om systemets åtkomstkoder och en noggrann uppfattning om värdefull information som man vill utnyttja. Med andra ord, en omfattande informationssäkerhetsstrategi kräver också starka användaråtkomstkontroller såväl som granskning. Administrativa åtkomstskontroller bör fastställas som integrerar med följande två aspekter: Stark autentisering/auktorisation och rollbaserad åtkomstbehörighet (Busson, 2008).

Stark autentisering - Kraven för autentisering, enligt Busson (2008), är det vanligaste skyddet för konfidentialitet, och autentisering bidrar till att säkerställa att en individ verkligen är den som han utger sig för att vara, genom att kräva att användaren identifierar sig. Enkel autentisering ger ett grundläggande skydd och kräver oftast ett användarnamn och lösenord. När information är särskilt känslig så rekommenderas två autentiseringsprocesser, där individen begärs att verifiera sig en andra gång i tillägg till användarnamn och lösenord, exempelvis via ett smartcard.

Rollbaserad åtkomstbehörighet - Företag bör implementera åtkomstbehörighet baserat på roller och ansvarsområden istället för full administrativ åtkomst. Att samla in och bearbeta information på ett tryggt och konfidentiellt tillvägagångssätt är enormt viktigt för alla typer av företag (Busson, 2008). Det kan till exempel bero på att en sekretesslag tvingar ett företag att skydda privatpersoners personuppgifter (Ni et. al. 2010). Vidare så föreslår Ni et. al. (2010) att ett företag som samlar in och bearbetar känslig information som exempelvis personuppgifter och kontouppgifter från kunder bör implementera någon form av rollbaserad åtkomstbehörighet (RBAC).
Byun & Li (2008) föreslår att syftet till varför man samlar in och bearbetar en viss typ av information ska vara tydligt formulerat och att det bör vara en avgörande faktor i ett företags rådande åtkomstbehörighetsmodell. En viss typ av information som ett företag har samlat in ska enbart kunna nås och bearbetas då syftet med att bearbeta information stämmer överens med dess ursprungliga syfte till varför det samlades in. Vidare menar Byun & Li (2008) att kunna marknadsföra sig som ett företag som behandlar sina kunders privata information på ett säkert tillvägagångssätt spelar även en avgörande roll i att både behålla sina nuvarande kunder och chansen till att attrahera nya.

Selvarani & Ravi (2013) påpekar vikten av att en person som saknar autentisering och tillgång till viss information inte ska kunna få tillgång till denna genom att till exempel använda en kollegas dator. Om detta händer så förlorar informationen sin konfidentialitet och integritet. Därför bör enheter skyddas med till exempel lösenord eller fingeravtrycksigenkänning.

2.2.2 Hantering av lösenord

Att få anställda att följa en ISP har visat sig vara ett problem eftersom det inte spelar någon roll hur man som företag skyddar sig om det inte kan efterföljas av användarna (Vance & Siponen, 2012). Det har skett en hel del forskning den senaste tiden om användarens oförmåga att följa en ISP.

Många användare måste komma ihåg flera lösenord då det ofta krävs vid användning av olika applikationer och program (Adams & Sasse, 1999). Att en användare har flera lösenord att komma ihåg tillsammans med det faktum att de ofta måste bytas regelbundet försvårar chansen för användaren att memorera dem (Warkentin & Willison, 2009). Användaren väljer då i många fall att anteckna sina lösenord vilket anses som en säkerhetsbrist (Stamp, 2006). Idag innehåller de flesta

företags information security policies (ISP) en funktion som inte tillåter en användare att välja enkla lösenord, exempelvis ”loggain”. För ett antal år sedan var bristfällig lösenordsdesign ett problem som kunde kopplas till när användaren skapade sina lösenord för att på ett enkelt sätt hålla reda på dem. En användare anses vara kapabel till att komma ihåg fyra till fem unika lösenord åt gången om de används regelbundet. Siffran är dock lägre ifall man tittar på lösenord som inte används regelbundet (Adams & Sasse, 1999). Enligt Gaw & Felten (2006) är problemet med lösenordshantering ofta relaterat till användare. Problemet är att användare inte kan eller försöker att memorera komplexa lösenord.

Adams & Sasse (1999) menar att det finns två huvudproblem med lösenordshantering. Systemfaktorer vilket användare upplever att de tvingas att kringgå och externa faktorer som uppfattas som svåra och inkompatibla med deras arbetsformer. Båda dessa problem beror på bristande kommunikation mellan säkerhetsavdelningen och användarna. Användarna förstår inte säkerhetsfrågor, medan säkerhetsavdelningen saknar förståelse för användarnas uppfattningar, uppgifter och behov. Användare uppfattar många säkerhetsmekanismer som mödosamma och onödiga som på så sätt blir ett hinder för deras verkliga arbete och därav uppstår låg säkerhetsmotivation hos dem. Om inte säkerhetsavdelningar förstår hur de mekanismer de utformar används i praktiken, kommer det vara en risk då de misslyckas i praktiken hos användarna. Användarens uppfattning om säkerhet innebär att säkerheten i systemen behöver att vara synliga, kunna eftersträvas och tas på allvar av företaget. Användare vill ha en förståelse för säkerheten i praktiken för att på så sätt öka deras medvetenhet om säkerheten i systemen och vikten av det (Adams & Sasse, 1999).

Yan, Blackwell, Anderson & Grant (2004) ger förslag på hur man bör resonera när man väljer ett lösenord. De föreslår att användaren helst ska blanda bokstäver (stora och små) med siffror för att generera ett tillräckligt säkert lösenord, men det ska även ha en rimlig längd. De poängterar att ett bra lösenord ser ut som en slumpmässig följd av bokstäver och siffror. Eftersom detta kan tänkas vara svårt för en användare att komma på och samtidigt memorera föreslår de i sin rapport att man använder sig av en så kallad lösenfras. Det vill säga att man använder de första bokstäverna i varje ord i en fras, ett känt talspråk eller något användaren själv har kommit på. Till exempel ”min syster Anna blir 32 år i maj”, vilket blir MsAB32åiM eller liknande beroende på hur användaren väljer att använda stora och små bokstäver. Detta är enligt Yan et. al. (2004) förmodligen den enklaste metoden för en användare att komma på en till synes slumpmässig följd av bokstäver och siffror som ger ett tillräckligt säkert lösenord som ändå är lätt för användaren att memorera.

Enligt Selvarani & Ravi (2013) är risken för att en mobil enhet, såsom laptop, surfplatta eller smartphone saknar lösenordsskydd eller att lösenordet inte är tillräckligt starkt är stor. Detta gör det lätt för en förbrytare att hacka sig in i en enhet som är stulen eller tappad och få tillgång till känslig information. Därför bör användaren använda sig av alla säkerhetsmekanismer som enheten har, exempelvis när en dator sätts i viloläge så krävs lösenord när den startar igen.

2.2.3 Utbildning

Det är av yttersta vikt att en användare följer företagets ISP på grund av som vi tidigare nämnt, de implementerade säkerhetslösningarna förlorar sin effekt om de inte efterföljs (Vance & Siponen, 2012; Puhakainen & Siponen, 2010). Puhakainen & Siponen (2010) menar att syftet med att inkludera och tillhandahålla utbildning inom IS-säkerhet är att ge användaren en förklaring till hur

systemet bör användas och varför det ska användas. Den mest vanligt förekommande formen av utbildning i IS-säkerhet har en pedagogisk form vilket innebär instruktioner steg för steg visualiserade i videor, skärmdumpar och webbaserade material.

Yngström & Björck (1999) menar att åtminstone grundläggande kunskap i informationssäkerhet i stort sett krävs i alla branscher och yrkesroller eftersom alla använder sig av någon form av IT. Yngström & Björck (1999) påpekar att tillsammans med utvecklandet av mer avancerad teknologi krävs det samtidigt utbildning till användarna i hur tekniken ska användas på rätt sätt för att minska risken för exempelvis informationsläckor. De poängterar vikten av att användaren förstår hur saker och ting fungerar rent tekniskt, exempelvis att utföra säkerhetskopior, för att det i slutändan ska fungera och påpekar att man ska undvika att förflytta ansvaret till någon annan, till exempel en IT-ansvarig.

Warkentin & Willison (2009) menar dock att det största hotet mot ett företag är den från insidan. Till skillnad från den eventuella hackaren som försöker få tillgång till viss information har den dagliga användaren på företaget tillgång genom ett giltigt användarnamn och lösenord. Användaren kan orsaka stor skada på två sätt: medvetet genom att sprida information till obehöriga eller omedvetet genom att inte följa företagets uppsatta ISP. Om en omedveten användare inte vet vad som ingår i företagets ISP, så kan exempelvis risken att glömma logga ut från sin arbetsstation förekomma. Det kan även förekomma att den omedvetna användaren saknar den rätta utbildningen för att kunna följa företagets ISP.

Vaughn, Dampier & Warkentin (2004) föreslår punkter som kan förbereda studenter innan de ger sig ut i arbetslivet angående informationssäkerhet som på så sätt kan utgöra en tillgång till företag. Eftersom Vaughn, Dampier & Warkentin (2004) främst riktar sig till studenter har vi valt att presentera de punkter som vi anser är lämpliga att implementera i ett försäkringsbolag.

- **Utbildning i operativsystem-** Först och främst kan man börja med att utbilda användarna i hur operativsystemet fungerar och ska användas.
- **Utbildning i datornätverk-** Internet skapades för att göra information delbar och nåbar till i princip vem som helst. Det skapades ur ett perspektiv med användarens tillit, inte användarens skydd. Här rekommenderas att gå igenom kända svagheter och luckor i internet.
- **Utbildning i informationssäkerhet-** Här ingår till exempel kryptering, ett sätt att skydda känslig information om det skulle hamna i fel händer. Här kan man också förklara enkelt hur ett antivirusprogram fungerar och kan upptäcka intrång.
- **Utbildning i på vilka tänkbara sätt nätverk kan bli hackat-** Inget nätverk är helt säkert. Det rekommenderas att ge användarna en insikt i hur ett IS kan bli attackerat, genom att studera hur liknande system har blivit attackerade tidigare och hur man kan förhindra att det händer igen. Selvarani & Ravi (2013) påpekar att det finns en mängd olika varianter av attacker som kan ske via en trådlös anslutning, till exempel phishing, spamming och spoofing. Hackaren kan spåra och profilera användaren av en enhet med hjälp av dessa metoderna.

Selvarani & Ravi (2013) presenterar och beskriver ytterligare säkerhetsaspekter som ett företag och användaren bör ha kunskap om och ta hänsyn till.

- **Virus-** Är ett program som replikerar sig själv och på de sättet infekterar en enhet utan att användaren nödvändigtvis märker det för att sedan fortsätta sprida sig till andra enheter. Ett exempel på ett virus är ett som riktar sig in på mobiler och låser dem och därmed gör dem helt

oanvändbara för användaren. Det vanligaste sättet att få en enhet smittat av ett virus är när användaren laddar ner ett mejl eller besöker en hemsida som utsätter användaren för phishing.

- **Trojan-** Det är ett program som bäddar in sig i en oftast annars pålitlig applikation som en användare laddar ner och därför kräver den mycket av offret för om det ska lyckas med sitt mål.
- **Maskar-** Den replikerar sig själv för att sedan spridas över ett nätverk och behöver inte vara en del i en annan applikation för att lyckas med detta.
- **Spionprogram-** Detta är ett program som installeras på en enhet i smyg för att anteckna och rapportera loggar och aktiviteter som användaren utför.
- **Insiderattack-** Den här typen, till skillnad från övriga nämnda attacker, är inte teknikbaserade attacker. Detta kan ske i den form att en anställd inte förstår eller känner till företagets rådande ISP gällande hur man operera i företagets IS. Detta är ett bevis på att ett företag bör implementera en kombination av både teknik och säkerhetsmedvetande i sin organisation.

2.2.4 Säkerhetskopiering

Säkerhetskopiering innebär helt enkelt att man sparar ner kopior på informationen man arbetar med. Säkerhetskopiering kan fungera på olika sätt, företag kan använda sig av både manuell och automatisk säkerhetskopiering. Informationen som säkerhetskopieras kan vara allt från mejl, operativsystem, användarfiler till databaser. En viktig aspekt som också företag bör tänka på är att regelbundet kontrollera att rutinen för säkerhetskopiering fungerar som den ska (if, u.å.).

Säkerhetskopiering är en av de vitala delarna som företag måste ta i beaktning i sitt IS, för att säkerställa att information behandlas på rätt sätt. Medan företag investerar i att skydda sitt nätverk från externa attacker så är det ett område som fram till nu varit relativt bortglömt, nämligen säkerheten i ett företags säkerhetskopiering, återskapning och arkiveringsprocess (Busson, 2008).

Säkerhetskopiering bör utföras med krypterad information, där lösningen bör utföras på så sätt att informationen krypteras innan det levereras och lagras. Kryptering av information säkerställer att obehöriga inte har möjlighet att få tillgång till informationen (if, u.å.). De flesta företag säkerhetskopierar sin information regelbundet och upprätthåller kopior på separata platser för datalagring i syfte för återställning av datakrascher. Trots att säkerhetskopior innehåller konfidentiell och regelbunden information så är det förhållandevis få företag som har tagit nödvändiga steg för att säkerställa den säkerhetskopierade informationen och informationen som transporteras till separata platser för lagring.
I praktiken, medan IT-avdelningar lägger stor vikt på säkerheten för attacker mot nätverket, så slarvar många företag i hur de skyddar sin infrastruktur för säkerhetskopior och själva säkerhetskopiorna (Busson, 2008).

Busson (2008) tar upp en studie av Enterprise Strategy Group som visar att 60 % av människor som arbetar med säkerhetskopior aldrig krypterar dem, medan endast 7 % gör det regelbundet. Resten menade att de gör det emellanåt eller inte var säkra på hur ofta de gjorde det. Busson (2008) menar att de flesta företag inser att säkerhetskopior kommer att vara det långsiktiga hjälpmedlet som används för arkivering och för återställning av information inom den närmaste framtiden, därför måste IT-managers prioritera frågan om säkerhetskopiering och ta den på allvar.
Vidare så menar Busson (2008) att för att nå robust backup-säkerhet så är det viktigt att tänka på säkerheten av information, applikationer och infrastrukturen (både internt och externt). Med ett heltäckande tillvägagångssätt av detta kan företag höja säkerheten mot ett brett antal hot.

Kryptering av information ger den högsta gradens skydd och är det säkraste sättet att skydda säkerhetskopior. Genom att klassificera information så är det inte nödvändigt att all information krypteras, utan IT-managers kan då tillämpa kryptering till särskilda klasser av information. Kryptering av information kan ske på olika sätt, till exempel databaskryptering, operativsystemskyptering, mjukvara för kryptering och olika krypteringsutrustningar (Busson, 2008).

Att skydda sekundära lagringsenheter som exempelvis minneskort innehållande känsliga uppgifter som lösenord, företagsinformation, kunduppgifter och referenser är också viktigt. Det bästa sättet för att skydda information på den här typen av enheter är kryptering (Selvarani & Ravi, 2013).

2.2.5 Datamissbruk och övervakning

En metod till att uppnå en lyckad implementering och användning av ett IS är computer monitoring (övervakning av användarens dataanvändning), alternativt uppföljning av hur användarna opererar i IS. Detta kan inkludera straff till användarna ifall de missköter sig eller bryter mot företagets ISP. Exempel på straff är böter, uppsägning och i värsta fall fängelse. Avskräckande åtgärder har visat sig effektiva mot att förhindra missbruk av information (Vance & Siponen, 2012).
Allvarligare straff medför generellt en lägre vilja från användaren att utföra den otillåtna handlingen. Om detta ska fungera i verkligheten måste dock användaren vara medveten om vad som inte är tillåtet. Det kräver att ledningen därmed är tydliga med deras ISP och att den når varje användare genom exempelvis föreläsningar eller mejl innehållande den gällande ISPen och konsekvenserna som följer om man bryter mot den (D'Arcy et. al. 2008; Herath & Rao, 2009).

Om ett företag ska kunna utdela straff när det är befogat måste de först kunna upptäcka användaren att missbruka IS, vilket inte är det lättaste alltid och det kan kräva resurser. Exempel på metoder för att övervaka användarna kan vara besök på arbetsplatsen, titta på individuella datorloggar och nätverksloggar. Den anställde visar sig mer inställsam till att följa företagets ISP ifall individen är medveten om att företaget utför regelbundna kontroller. Å andra sidan visar användaren större tendens att utföra en otillåten handling ifall risken att bli påkommen anses vara liten (Herath & Rao, 2009).

Anställda som missbrukar företagets IS kan till exempel leda till stora ekonomiska förluster och ge företaget ett dåligt rykte. Många tror att det största hotet för ett företag kommer från utsidan i form av hackare men det är användarnas missbruk som står för det största hotet. De motsvarar nämligen 60 % av datamissbruket (Lee & Lee, 2002).

Bulgurcu et. al. (2010) föreslår tre faktorer som påverkar en användares avsikt att följa en ISP, fördelen med att följa företagets ISP, den personliga kostnaden eller konsekvenserna av att följa företagets ISP och kostnaden eller konsekvenserna av att inte följa företagets ISP. Här spelar användarens tidigare erfarenhet och attityd ur ett säkerhetsperspektiv en avgörande roll för hur väl motiverad han är till att följa företagets ISP.
Faktorer som kan påverka användarens motivation kan exempelvis vara:

- att användaren upplever personlig tillfredsställelse genom att följa företagets ISP och därmed utför sitt arbete säkert.

- om företagets ISP kräver mer tid eller arbete för individen att genomföra en annars relativt lätt uppgift kan det leda till att individen bryter mot ISPen.
- vilka specifika straff eller konsekvenser han riskerar genom att inte följa företagets ISP.

Om ett företag vill uppnå ett större intresse hos de anställda att följa deras ISP kan de utdela en belöning i form av löneförhöjningar, bonusar eller personliga rekommendationer. Det är dock inte vanligt att företag idag belönar sina anställda för att de följer företagets ISP på detta sättet. Om en anställd ska följa en ISP kräver det oftast att han tvingas ta försiktighetsåtgärder som leder till besvär och längre tid att utföra en uppgift. Detta ser den anställde oftast som en nackdel och som ett hinder för produktiviteten. Bulgurcu et. al. (2010) föreslår också, precis som Vance & Siponen (2012), att man kan avskräcka användare från att bryta en ISP genom utdelning av diverse straff (externa straff). Bulgurcu et. al. (2010) nämner även att självpåtagna straff (interna straff), i form av skam, är ett effektivt medel för att hindra användare att bryta mot företagets ISP.

Busson (2008) nämner att företag bör införa loggövervakning på deras system för säkerhetskopiering för att spåra och rapportera aktiviteter av konfidentiell information. Att spåra inloggningar och utloggningar i kritiska system är viktigt, samt både lyckade och misslyckade försök till åtkomst. Granskningsloggning ger också en säker verifieringskedja.

2.2.6 Konfidentialitet

Klassificeringsmodellen enligt Oscarson et. al. (2009) omfattar de tre informationssäkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet. Klassificering av information är något elementärt för att information och resurser ska ges nödvändigt skydd. Modellen används på så sätt att informationen i organisationen klassificeras utifrån konsekvenser som oönskad påverkan av informationens kvalitet bedöms leda till. Exempelvis om en organisation får allvarliga problem och skador av att vital information för organisationen blir tillgänglig för obehöriga, så ska informationen betraktas med hög konsekvensnivå avseende konfidentialitet.

Vidare så nämner Oscarsson et. al. (2009) att andra aspekter också kan finnas när ett företag utför klassningsarbete, exempelvis spårbarhet och oavvislighet, men det är inte något som de tar upp i den generella modellen. De påpekar också att spårbarhet kan både användas som en aspekt vid klassificering av information, och även som en säkerhetsåtgärd för att möta kraven på informations konfidentialitet och riktighet.

Tabell 2.1: Klassificeringsmodellen enligt (Oscarson et. al. 2009).

Säkerhetsaspekt	**SIS Handbok 550**	**SS-ISO/IEC 27001**
Konfidentialitet	Skyddsmål att innehållet i informationsobjekt (eller ibland dess existens) inte får göras tillgängligt eller avslöjas för obehöriga	Egenskapen att information inte tillgängliggörs eller avslöjas till obehöriga individer, enheter, eller processer
Riktighet	Skyddsmål att information inte förändras, vare sig obehörigen, av misstag eller på grund av funktionsstörning	Egenskapen att skydda exaktheten och fullständigheten gällande tillgångar
Tillgänglighet	Skyddsmål där informationstillgångar skall kunna utnyttjas i förväntad utsträckning och inom önskad tid	Egenskapen att vara åtkomlig och användbar vid begäran av behörig enhet

Att säkerställa konfidentialitet, integritet och tillgänglighet av information, har enligt von Solms & van Niekerk (2013) blivit en standard inom informationssäkerhetsbranschen. En klar förståelse av innebörden av de ovan nämnda aspekterna är nödvändiga för förståelsen av information och IKT-säkerhet (informations- och kommunikationsteknik).

Enligt Diesburg & Wang (2010) finns det två huvudkomponenter för att skydda och säkerställa integriteten till uppgifter på elektroniska lagringsmedier. Först, så måste information lagras konfidentiellt för att förhindra obehörig tillgång, och att lösningen inte heller bör medföra väsentliga besvär vid normal användning. För det andra, i samband med borttagning, så måste konfidentiell information tas bort från lagringsmedierna såväl som i hela datormiljön på ett oåterkalleligt sätt.
Att använda kryptering för lagring av information eller autentisering av giltiga användare är exempel på hur konfidentialitet uppnås.

Puhakainen & Siponen (2010) menar att det är viktigt att konfidentialitet också används på rätt sätt i användandet av e-post. För det första så måste användarna vara medvetna om sin e-postpolicy och förstå dess innehåll, och framförallt bör användarna veta reglerna för kryptering av konfidentiell information. För det andra, utan tillräcklig kunskap av organisationens klassificeringsregler av information, skulle inte användarna känna igen konfidentiell information. För det tredje så bör användarna ha kunskap för användning av krypteringsprogram för e-post.

Användningen av mobila enheter (exempelvis laptops, mobiler och surfplattor) som har trådlösa accesstekniker som till exempel 4G och LTE tillåter användaren att få tillgång till ett nätverk ifrån längre avstånd och under större bandbredder. Detta kan resultera i en effektiv kommunikation mellan användaren och informationssystemet men det kräver fokus på riskbedömning med hänsyn till säkerhets- och kommunikationskrav eftersom att det kan äventyra informationens konfidentialitet (Huang, Zhang & Jim Luo, 2010).

Om känslig information såsom banknummer eller pinkoder till ditt bankkort finns lagrad på en enhet ska den inte finnas tillgänglig för andra. Om någon som saknar den rätta autentiseringen för att ta del av den här typen av information ändå får tillgång till den så sätts dess konfidentialitet och integritet på spel. Otillåten åtkomst och manipulering av sådan information ska förhindras. Detta

gäller även information om kunder som till exempel telefonnummer och adresser. En tänkbar lösning på detta problem kan vara kryptering och autentiseringsmekanismer (Selvarani & Ravi, 2013). Vidare menar Selvarani & Ravi (2013) att om en mobil enhet blir stulen eller förloras på något sätt av användaren så komprimeras konfidentialiteten på informationen som finns lagrad på enheten. Om man senare skulle hitta enheten eller få den inlämnad av någon utomstående så finns alltid risken att enheten har blivit smittad av något virus eller spionprogram som kan riskera företagets informationssystem. Därför bör man anse att så fort en enhet är förlorad så är informationen på den enheten likaså. En lösning på detta problem kan vara kryptering eller remote wiping. Antalet anställda som reser med känslig företagsinformation ökar konstant vilket medför fler hot mot informationens konfidentialitet.

2.3 Undersökningstabell

Vi valde att använda oss utav motivationsteorin TMT eftersom vi fann den lämplig eftersom den är en hopslagning av flera teorier. Vi ansåg därför att den skulle vara passande för att den tillåter oss att undersöka fler aspekter som kan påverka en individs säkerhetsmedvetande till skillnad från om vi till exempel bara skulle använda en av de teorier den är baserad på. Valet av de aktiviteter vi kommer att undersöka baseras på att de visade sig återkommande och gemensamma för de flesta av de vetenskapliga artiklar vi läste som handlade om säkerhetsmedvetenhet i en IS-miljö. Undersökningstabellen nedan ger en förklaring till hur vi kommer att applicera TMT på våra valda aktiviteter där vi kommer att undersöka varje aktivitet utifrån aspekterna förväntad förmåga, värde, tid och belöning. Tabellen visar även aktiviteternas koppling till vår litteraturgenomgång.

Tabell 2.2 Undersökningstabell.

	Aktiviteter	**Koppling till litteratur**
TMT (förväntad förmåga, värde, tid och belöning)	Autentisering	Stamp (2006), Adams & Sasse (1999), Busson (2008), Selvarani & Ravi (2013)
	Policy för hantering av lösenord	Vance & Siponen (2012), Warkentin & Willison (2009), Adams & Sasse (1999), Stamp (2006), Yan et. al. (2004), Selvarani & Ravi (2013)
	Utbildning	Vance & Siponen (2012), Puhakainen & Siponen (2010), Yngström & Björck (1999), Vaughn et. al. (2004), Selvarani & Ravi (2013)
	Säkerhetskopiering	if.se (u. å.), Busson (2008), Selvarani & Ravi (2013)
	Datamissbruk och övervakning	Vance & Siponen (2012), D'Arcy et. al. (2008), Herath & Rao (2009), Lee & Lee (2002), Bulgurcu et. al. (2010)
	Konfidentialitet	Oscarson et. al. (2009), Diesburg & Wang (2010), Puhakainen & Siponen (2010), Huang et al. (2010), von Solms & van Niekerk (2013), Selvarani & Ravi (2013)

3. Metod

När man talar om säkerhetsmedvetenhet, och rent allmänt om IT-säkerhet, så framkommer det att användaren ofta betraktas som den svagaste länken i ett IS (Bulgurcu, Cavusoglu & Benbasat, 2010; Warkentin & Willison, 2009). Som vår forskningsfråga visar har vi valt att utgå ifrån användarens perspektiv när vi studerar säkerhetsmedvetenhet inom ett försäkringsbolag. För att studera det har vi valt att använda oss av motivationsteorin Temporal Motivation Theory (TMT) för att komma fram till deras motivation och inställning att utföra olika aktiviteter, som är beskrivna i litteraturgenomgången, utifrån aspekterna förväntad förmåga, värde, tid och belöning (Steel & König, 2006). När vi undersökte aspekten värde ställde vi aktiviteterna mot varandra där varje intervjuperson värderade vilken av aktiviteterna som har störst värde. Vid aspekterna förväntad förmåga, tid och belöning använde vi oss av öppna frågor med tillåtelse för följdfrågor (Jacobsen, 2002). Med detta sagt använde vi oss av en deduktiv strategi när vi baserade våra intervjufrågor på vår teoridel för att sedan koppla det till vårt resultat (Jacobsen, 2002). Det vill säga att med hjälp av vår litteraturgenomgång har vi fått förståelse över hur säkerhetsaspekter kan tillämpas, som vi därefter vill jämföra med våra resultat från intervjupersonerna. Vi har utfört semistrukturerade kvalitativa intervjuer.

3.1 Tillvägagångssätt

Vi har valt att utföra en kvalitativ undersökning där vi utfört fem fysiska enskilda intervjuer hos ett försäkringsbolag. Anledningen till att vi har valt en kvalitativ undersökning är för att den medför djupare och mer ingående frågor och svar samtidigt som flexibilitet ges i form av att vi kan ställa följdfrågor till skillnad från en kvantitativ ansats (Jacobsen, 2002). Vi har valt att utföra våra kvalitativa intervjuer person för person för att vi anser att vi kommer att få mer utförlig information av våra intervjupersoner. Till skillnad från distansintervjuer som till exempel sker per telefon och som har visats öka risken för osanna utsagor (Jacobsen, 2002). Vi utförde semistrukturerade intervjuer med öppna svar men även frågor med fasta svarsalternativ förekom med tillåtelse för följdfrågor om tillfälle gavs (Jacobsen, 2002). Våra intervjuer var strukturerade i förväg, med vår intervjuguide, för att sträva efter att alla intervjuer skulle vara så likartade som möjligt. För att undvika att viktig information skulle förloras valde vi att spela in våra intervjuer (Jacobsen, 2002). Att spela in våra intervjuer tillät oss även att genomföra intervjuerna mer flytande då vi slapp ta pauser för att anteckna och det blev lättare att ha ögonkontakt med intervjupersonen (Jacobsen, 2002).

3.2 Metod för utformning av frågor

Alla våra intervjuer började med inledande frågor som var tänkta att introducera ämnet för intervjupersonen men också för att hjälpa oss att sätta oss in i intervjupersonens bakgrund. Jacobsen

(2002) föreslår att man börjar med icke-komplexa frågor för att på så sätt undvika att intervjun låser sig.

Vid utformandet av våra intervjufrågor utgick vi ifrån motivationsteorin TMT:s fyra aspekter: förväntad förmåga, värde, tid och belöning. Vi har sedan applicerat dessa på aktiviteterna som presenteras vårt litteraturkapitel.
När vi undersökte aspekterna förväntad förmåga, tid och belöning av att genomföra en aktivitet använde vi oss av öppna frågor (Jacobsen, 2002). Till exempel:

”***Hur hanterar du dina lösenord?***”

Frågorna som berör aspekten värdet av en aktivitet, ställdes mot varandra för att ta reda på hur intervjupersonerna värderar aktiviteterna gentemot varandra. Här ville vi att intervjupersonen tar ställning mellan två aktiviteter genom att svara utifrån fyra givna svarsalternativ, som kan ses som enkätfrågor, med tillåtelse för följdfrågor och djupare svar. Vi ville fortfarande tillämpa en kvalitativ ansats men vi ansåg det nödvändigt att inkludera en form av kvantitativ ansats när vi undersökte intervjupersonernas värderingar av aktiviteterna. Till exempel:

”***Är det viktigare att hantera lösenord än att ta backups?***”
Det är *absolut viktigare* att hantera lösenord än att ta backups
Det är *något viktigare* att hantera lösenord än att ta backups
Det är *något viktigare* att ta backups än att hantera lösenord
Det är *absolut viktigare* att ta backups än att hantera lösenord

Anledningen till att vi har valt fyra svarsalternativ och inte ett ojämnt antal, till exempel fem, är att vi vill att intervjupersonen ska ta ställning och inte ställa sig mitt emellan två aktiviteter.

I utformningen av vissa frågor kunde strukturen se något annorlunda ut då det gällde aktiviteter som den anställde inte utför personligen. Detta för att få fram deras inställning till aktiviteten som vi sedan kan analysera. Till exempel:

”Vad är belöningen med att övervakas?”

I vår avslutande del i våra intervjuer ställde vi ett antal avslutande frågor för att summera intervjun där det gavs tillfälle att utveckla eller komplettera intervjun. På detta sätt gav vi intervjupersonen chansen att dela ännu mer information som möjligtvis inte hade kommit fram tidigare under intervjun (Jacobsen, 2002).
Vid denna del valde vi även att ställa ett scenario angående hur intervjupersonerna väljer att arbeta mobilt med konfidentiell företagsinformation. Anledningen är att vi ville ha ytterligare förståelse för hur deras motivation och inställning är till att utföra olika handlingar.

Tabellen nedan visar sambandet mellan de framtagna aktiviteterna, vår insamlade litteratur och vår intervjuguide.

Tabell 3.1. Aktiviteternas koppling till intervjuguiden.

Aktiviteter	**Koppling till litteratur**	**Koppling till intervjuguiden**
Autentisering	Stamp (2006), Adams & Sasse (1999), Busson (2008), Selvarani & Ravi (2013)	5, 7, 11a-11e, 16a, 17a, 18a
Hantering av lösenord	Vance & Siponen (2012), Warkentin & Willison (2009), Adams & Sasse (1999), Stamp (2006), Yan, Blackwell, Anderson & Grant (2004), Selvarani & Ravi (2013), Gaw & Felten (2006)	4, 7, 11a, 12a-12d, 16b, 17b, 18b
Utbildning	Vance & Siponen (2012), Puhakainen & Siponen (2010), Yngström & Björck (1999), Vaughn, Dampier & Warkentin (2004), Selvarani & Ravi (2013)	6, 7, 11b, 12a, 13a-13c, 16c, 17c, 18c
Säkerhetskopiering	if.se (u.å.), Busson (2008), Selvarani & Ravi (2013)	7, 8, 11c, 12b, 13a, 14a-14b, 16d, 17d, 18d, 22
Datamissbruk och övervakning	Vance & Siponen (2012), D'Arcy, Hovav & Galetta (2008), Herath & Rao (2009), Lee & Lee (2002), Bulgurcu, Cavusoglu & Benbasat (2010)	7, 9, 11d, 12c, 13b, 14a, 15a, 17e, 18e, 19
Konfidentialitet	Oscarson, Öberg & Rystedt (2009), Diesburg & Wang (2010), Puhakainen & Siponen (2010), Huang et. al. (2010), von Solms & van Niekerk (2013), Selvarani & Ravi (2013)	7, 10, 11e, 12d, 13c, 14b, 15a, 16e, 17f, 18f, 20, 21, 23, 24, 25

3.3 Urval

Jacobsen (2002) presenterar ett en antal olika faser som rekommenderas att följa vid urvalsprocessen, och som vi tog i beaktning när vi utförde vår urvalsprocess.
För att hitta ett relevant företag som passade in till vår undersökning gick vi igenom vilka försäkringsbolag som hade kontor och var belägna i nordvästra Skåne. Därefter tog vi telefonkontakt med en kontaktperson hos försäkringsbolaget där vi beskrev vilka vi var och vad vi hade tänkt att undersöka. Vi angav att vi ville ha fem uppgiftslämnare som använder datorer dagligen och därmed kan ge oss riktig och relevant information om det vi ville undersöka. Individens tidigare erfarenhet är något vi inte direkt aktivt djupare inkluderat i vår undersökning. Vi påpekade att både företaget och uppgiftslämnarna kommer att hållas anonyma. Vår kontaktperson gav oss fem personer som baserat på vår beskrivning och vad vi ville undersöka ansågs vara lämpliga. Försäkringsbolaget är internationellt och har ungefär 4000 anställda.

Tabell 3.2 Intervjupersoner.

Intervjuperson 1 (I1)	**Roll inom företaget:** Skadereglerare motor privat **Datorvana (skala 1-4):** 3 **Säkerhetsmedveten (skala 1-4):** 2
Intervjuperson 2 (I2)	**Roll inom företaget:** Skadereglerare motor privat **Datorvana (skala 1-4):** 3 **Säkerhetsmedveten (skala 1-4):** 4
Intervjuperson 3 (I3)	**Roll inom företaget:** Skadereglerare motor privat **Datorvana (skala 1-4):** 3 **Säkerhetsmedveten (skala 1-4):** 4
Intervjuperson 4 (I4)	**Roll inom företaget:** Skadereglerare motor privat **Datorvana (skala 1-4):** 3 **Säkerhetsmedveten (skala 1-4):** 3
Intervjuperson 5 (I5)	**Roll inom företaget:** Skadereglerare motor privat **Datorvana (skala 1-4):** 4 **Säkerhetsmedveten (skala 1-4):** 3,5

Förklaring till tabell: Datorvana och säkerhetsmedvetenhet är bedömt enligt intervjupersonerna själva i inledningen av intervjuerna och som finns bifogat i bilagorna 2-6.

3.4 Bearbetning av data

Efter att våra intervjuer genomförts började arbetet med transkribering, där vi lyssnade igenom allt vårt inspelade material och skrev ned det i textform. Vi valde att transkribera hela intervjuerna för att inte missa något vitalt. Eftersom både företaget och intervjupersonerna hålls anonyma så har vi valt att kryptera intervjupersonerna till I1, I2, I3, I4 och I5. När vi transkriberade intervjuerna så valde vi att använda oss utav ett transkriberingsprogram, vilket underlättade arbetet avsevärt. Det gjorde det möjligt för oss att enkelt lägga till noteringar och kommentarer under tiden vi transkriberade, vilket Jacobsen (2002) menar är en stor fördel. Under intervjuerna så gjordes anteckningar, som sedan var till hjälp när vi bearbetade informationen och sammanställde det. Eftersom vi utförde semistrukturerade intervjuer så innebar det att alla svaren inte alltid kunde hittas på samma ställe. Vi utgick från tabell 3.1 som visar aktiviteternas koppling till intervjufrågorna och började sortera svaren utifrån den, vilket vi ansåg var en lämplig metod och där vi kunde identifiera relevanta svar till våra olika delar. Vid bearbetningen av frågorna om värdet av en aktivitet gentemot en annan, valde vi att använda oss utav kodning som rekommenderas av Jacobsen (2002). Vi ville få en uppfattning om hur aktiviteterna prioriteras gentemot varandra och vår kodning såg ut som följande: ju mer positivt laddat en aktivitets värde ansågs vara tilldelades desto högre poäng eftersom det bör stämma överens med aktivitetens stigande eller fallande ordningsföljd vilket Jacobsen (2002) rekommenderar. Om en intervjuperson sade att ”det är absolut viktigare att ta backups än att hantera lösenord” gavs det 4 poäng till aktiviteten säkerhetskopiering medan aktiviteten hantera lösenord tilldelades 1 poäng. Om intervjupersonen istället svarade ”det är något viktigare att hantera lösenord än att ta backups” tilldelades aktiviteten hantera lösenord 3 poäng medan aktiviteten säkerhetskopiering gavs 2 poäng.

Den totala poängfördelningen i den här typen av frågor blev därmed alltid 5 poäng.
Det minsta antalet totala poäng en aktivitet kunde få är 5 poäng medan den totala maxpoängen var 20 poäng. Anledningen till att vi valt detta system beror på att om en intervjuperson värderar aktivitet 1 som ”något viktigare” så behöver det inte betyda att aktivitet ”2” är oviktig, och därmed har vi givit poäng i båda fallen. För att säkerställa att all nödvändig och relevant information tolkats på rätt sätt så gick vi igenom transkripten flertalet gånger.

3.5 Validitet och Reliabilitet

Jacobsen (2002) menar att intern och extern validitet är viktigt att ta hänsyn till när man gör en undersökning. Intern validitet syftar på resultatens giltighet, det vill säga att vi faktiskt mäter det som vi vill mäta. Vi uppnår intern validitet genom att vi har baserat våra intervjuer på akademiska källor. Alla våra källor har vi granskat kritiskt, särskilt de som är äldre. Extern validitet handlar i sin tur om ett resultat från en viss tidpunkt och område är giltigt också i andra sammanhang och på så sätt kan generaliseras. Från vårt perspektiv kan det vara svårt att generalisera våra resultat eftersom vi enbart genomförde kvalitativa intervjuer med fem personer på ett försäkringsbolag. Till skillnad från om vi hade genomfört en kvantitativ undersökning där vi hade fått insyn från fler personer på olika företag. Vi utförde fysiska intervjuer med alla intervjupersonerna och därmed intervjuades alla under samma förutsättningar, vilket medför att alla intervjuer utförts på samma tillvägagångssätt där inga avvikelser skett. På så sätt bidrog det till att öka kvalitén på intervjuerna (Jacobsen, 2002). Tillförlitligheten i studien stärktes av att vi tydligt förankrade våra intervjufrågor i vår litteraturstudie, och därefter analyserade intervjupersonernas svar med litteraturstudien. Vi har haft intervjuareffekten (Jacobsen, 2002) i åtanke när vi har genomfört våra intervjuer genom att försöka undvika att ställa ledande frågor för att på så sätt undvika att påverka våra intervjupersoners svar. För att öka tillförlitligheten i vår undersökning lät vi våra intervjupersoner läsa igenom och godkänna de transkriberade intervjuerna.

3.6 Etik

Jacobsen (2002) menar att en undersökning generellt sätt bryter sig in i en enskild individs privatsfär. Han menar även att en person ofta tenderar att agera annorlunda när han vet om att han observeras. Vi försökte minimera den här risken genom att hålla intervjupersonerna, och företaget, anonyma i vår studie. När våra intervjuer var genomförda fick respektive intervjuperson möjlighet till att godkänna de transkriberade intervjuerna. Vid analysering av svaren från intervjupersonerna var det viktigt att vi använde dem i sitt rätta och hela sammanhang. Det vill säga att vi använde eventuella citat i dess rätta kontext för att undvika feltolkningar och inte manipulera information för att få fram bättre resultat (Jacobsen, 2002). Ytterligare en anledning till varför vi höll intervjupersonerna och företaget anonyma i vår undersökning var för att det kan tyckas behandla känslig information ur ett företagsperspektiv. Jacobsen (2002) nämner att frivilligt deltagande är en punkt som måste uppfyllas, och det uppfyller vi i vår undersökning eftersom uppgiftslämnarna inte har påtvingats att delta och är medvetna om vad vi ville undersöka.

3.7 Kritik mot metodval

Vi är medvetna om att det inte går att generalisera våra resultat eftersom vi endast har undersökt ett företag och fem personer på det företaget. Dock gav det oss en möjlighet till att studera hur säkerhetsmedvetenheten kan tänkas se ut bland de anställda på vårt företag. Vi valde att intervjua fem försäkringsförmedlare med samma arbetsroll på företaget för att undvika ett snett urval (Jacobsen, 2002) eftersom de är ca 70 anställda på det kontoret.

4. Resultat av undersökningen

I detta kapitel presenterar vi resultatet av vår empiriska undersökning som utförts i form av semistrukturerade intervjuer. Vi intervjuade fem personer på ett försäkringsbolag och alla var försäkringsförmedlare. Både försäkringsbolaget och våra intervjupersoner är informerade och medvetna om att all information presenteras anonymt. Våra genomförda intervjuer är transkriberade och finns bifogat som bilaga 2-6. Vi presenterar det empiriska resultatet utifrån aktiviteterna som är presenterade i tabell 2.2.

4.1 Autentisering

Alla våra intervjupersoner autentiserar sig med hjälp av användarnamn och lösenord för att logga in och få tillgång på sina enheter. Även när det gäller inlogg till diverse program och applikationer så använder alla intervjupersoner sig av användarnamn och lösenord. Merparten av intervjupersonerna är överens om och menar att autentisera sig är en lätt process och ser värdet av det gentemot de andra aktiviteterna. I4 ansåg att eftersom de använder sig av flera olika system och därmed autentiserar sig ofta för att få tillgång, är det omständigt med flera unika användarnamn och lösenord i de olika systemen. Däremot ansåg I4 att det tar rimligt med tid att autentisera sig mot en tjänst och värdet av att autentisera sig när vi ställde aktiviteten mot de andra aktiviteterna gav 14 poäng av 20 möjliga, vilket innebar att han värderade aktiviteten två gånger som ”absolut viktigare” och en gång som ”något viktigare” gentemot de andra aktiviteterna. Vid de två andra tillfällena valde han därmed bort aktiviteten gentemot de andra aktiviteterna. I4 såg också en klar belöning med att kunna autentisera sig, där han menade på att det är en trygghet att veta att ingen annan kan logga in och utföra uppgifter i hans namn och utge sig för att vara honom.

På frågan om värdet av aktiviteten, att autentisera sig mot en tjänst, gentemot de andra aktiviteterna var det endast I2 som valde bort autentisering och menade att de andra aktiviteterna var “absolut viktigare”, därav endast 5 poäng. Han satte det minsta möjliga värdet på aktiviteten autentisering gentemot de andra aktiviteterna, men menade att det tar rimligt med tid att autentisera sig mot en tjänst. Han såg däremot en stor belöning med det, nämligen tryggheten att veta att ingen får tillgång till hans dator och att han inte kan få skuld för någon annans handlingar.

”Då kan man veta att det bara är jag som har varit där, ingen kan göra något på min dator. Jag kan inte få skuld för någon annans misstag.” (Bilaga 3, 18a)

Tre av intervjupersonerna, ansåg att det tar rimligt med tid att autentisera sig gällande en tjänst med användarnamn och lösenord, men I1 och I2 ansåg att det tar för lång tid och är omständigt, när de ser till helheten, att autentisera sig i alla diverse system på en arbetsdag. Det vill säga att det görs för ofta. När det gäller vad intervjupersonerna får ut av att kunna autentisera sig, menade alla intervjupersonerna att de såg en klar belöning. Fyra intervjupersoner menade att de kan bevisa att det är dem som är inloggade och att ingen annan kan utge sig för att vara dem. I3 nämnde att

belöningen av att autentisera sig är vikten av rollbaserad åtkomstbehörighet. Det vill säga att din arbetsroll avgör vilka funktioner och vilken information som du har tillgång till.

I I3 och I5:s svar var båda eniga om att aktiviteten att autentisera sig på sin arbetsplats inte är något bekymmer. De ansåg att det är en lätt process och har vid denna aktivitet givit poängen, 18 respektive 15 poäng gentemot de andra aktiviteterna när de ställdes mot varandra. De menade att det tar rimligt med tid att autentisera sig mot en tjänst samt att det finns en klar belöning med att kunna autentisera sig.

Tabell 4.1 Sammanfattning autentisering.

	I1	I2	I3	I4	I5
Förväntad förmåga: Anser det är lätt att autentisera sig mot en tjänst	Ja.	Ja.	Ja.	Nej, omständigt med flera unika användar-namn och lösenord.	Ja.
Värde: Poäng på aktiviteten gentemot de andra aktiviteterna	14/20	5/20	18/20	16/20	15/20
Tid: Hur ofta autentiserar du dig? Anser det tar rimligt lång tid	Många ggr/ dag. Ja, men omständigt.	20 ggr/dag. Ja, men för lång tid att autentisera sig mot alla system.	10 ggr/dag. Ja.	10-15 ggr/ dag. Ja.	10 ggr/dag. Ja.
Belöning: Ser belöning i att kunna autentisera sig	Ja, ingen kan göra något i mitt namn.	Ja, ingen annan kan göra något på min dator.	Ja, ha tillgång till viss information som andra kollegor inte har.	Ja, ingen annan gör något i mitt namn.	Ja, att jag är jag och man kan ta ut statistik.

4.2 Hantering av lösenord

I frågan på hur intervjupersonerna i försäkringsbolaget hanterar sina lösenord var svaren väldigt varierande. I1 och I2 medgav att de upplever det som svårt att memorera sina lösenord i huvudet. De behöver antingen skriva ned dem i datorn, mobilen eller fysiskt på papper. I1 medgav även att han förstod att det förmodligen inte var säkert att spara sina lösenord i mobilen men att han kände

sig tvungen att göra det med tanke på hur systemen är uppbyggda. Vidare ansåg I3 och I4 att de var motiverade till att memorera sina lösenord men när det blev för många var även de tvungna att skriva ned dem. I5 var den enda av våra intervjupersoner som memorerade sina lösenord samtidigt som han tyckte att hanteringen var en lätt process och att han såg en klar belöning. Belöningen enligt I5 var att ingen kan ta del av hans lösenord om han memorerar dem.

Gällande värdet av att hantera lösenord gentemot de andra aktiviteterna gavs väldigt varierande svar från våra intervjupersoner. I3 ansåg att hantering av lösenord är en ”absolut viktigare” aktivitet, då han valde att hantering av lösenord är viktigare vid alla fem tillfällena, och där han valde ”absolut viktigare” vid fyra av dem. I2 påstod också att hantering av lösenord är en viktigt aktivitet, då han valde aktiviteten som viktigare gentemot de andra aktiviteterna fyra gånger, två gånger som ”absolut viktigare” och två gånger som ”något viktigare”. Detta resulterade i 16 poäng.

Vidare ansåg I1 att han inte ser någon belöning med att hantera sina lösenord, och där han värderade aktiviteten gentemot de andra aktiviteterna som ”något viktigare” vid två tillfälle och vid de andra tre tillfällena valde han bort aktiviteten. Detta resulterade i den näst lägsta poängen av intervjupersonerna, 10 poäng. I4 värderade hantering av lösenord lägst av alla intervjupersoner när vi ställde aktiviteterna mot varandra, 7 poäng, där han enbart valde aktiviteten som viktigare en gång vid de fem tillfällena. I4 menade att samtidigt som han tycker att det är irriterande att behöva ändra sina lösenord regelbundet, såg han en klar belöning med att memorera dem till skillnad från att skriva ned dem, eftersom ingen annan därmed kan ta del av dem.

Tidsmässigt var merparten av intervjupersonerna eniga om att det tar rimligt med tid att utföra hantering av lösenord. Uppskattningsvis tvingas de av systemen att ändra lösenord en gång i månaden eller en gång varannan månad beroende på vilket system. I1 menade att ändra sina lösenord inte tar lång tid utan problemet är att lösenord byts ut för ofta och vid olika tidpunkter, och därmed blir svårt att memorera dem. Han tvingas att skriva ned dem för att han inte ska glömma dem. I1 menade att han skulle vilja ha en förändring i det här fallet eftersom han tycker att det är orimligt att ha så pass många lösenord som krävs att ändras ofta.

På frågan om hur många unika lösenord våra intervjupersoner hanterar fick vi relativt lika resultat där endast I2 utmärkte sig och svarade att han har 10-13 unika lösenord att hantera. De andra intervjupersonerna svarade att de har mellan fyra-sju unika lösenord.

Tabell 4.2 Sammanfattning hantering av lösenord.

	I1	I2	I3	I4	I5
Förväntad förmåga: Hur hanterar du dina lösenord? Anser det är lätt att hantera lösenord	Nedskrivna i mobilen. Nej det är omöjligt.	Nedskrivna i mobilen, datorn eller på papper. Nej.	Försöker memorera, antecknar ibland. Ja.	Försöker memorera, antecknar ibland. Ja.	Memorerar alla lösenord. Ja.
Värde: Poäng på aktiviteten gentemot de andra aktiviteterna	10/20	16/20	19/20	7/20	11/20
Tid: Hur ofta hanterar du dina lösenord? Anser det tar rimligt lång tid	1 gång varannan månad. Nej, måste bytas för ofta.	1 gång/månad. Ja.	1 gång varannan månad. Ja.	1 gång/ månad. Ja.	1 gång/ månad. Ja.
Belöning: Ser belöning i att hantera lösenord	Nej.	Ja, att säkert förvara sina lösenord.	Nej, det är istället ett krav.	Ja, det är säkrare att memorera dem.	Ja, Ingen kan ta del av dem

4.3 Utbildning

Eftersom vi fick reda på att det inte tillhandahålls utbildningar inom IT-säkerhet kommer vi inte presentera, och inte heller senare analysera, aspekterna förväntad förmåga och tid när det gäller utbildning i IT-säkerhet. Det är därför vi endast väljer att sammanställa svaren på frågorna kring aspekterna värde och belöning i tabell 4.3.

Alla våra intervjupersoner påvisade en gemensam åsikt om att utbildning inom IT-säkerhet inte är något de känner att de har något behov av eftersom de anser att deras befintliga kunskap är tillräcklig. I4 påpekade tydligt att han överhuvudtaget inte hade någon motivation till att vilja utbildas och lära sig mer inom IT-säkerhet. Resterande intervjuperson svarade att de hade varit intresserade av att lära sig mer inom IT-säkerhet om företaget hade erbjudit utbildning. I4 nämnde att han förväntade sig att systemen de arbetar i ska vara tillräckligt säkra, och att ansvaret ligger på IT-avdelningen. Enbart I1 och I2 såg ett litet värde i att lära sig mer om IT-säkerhet.

När det gäller våra intervjupersoners uppfattningar om vilken typ av belöning som de hade fått ifall företaget hade tillhandahållit utbildningar var i princip helt olika. I1 och I2 såg ingen belöning, medan I3 svarade att han hade fått en större förståelse för hur saker och ting fungerar. I4 menade att belöningen hade varit att han hade kunnat skydda sina kunder och deras känsliga information mer

säkert. I5 menar att belöningen hade varit möjligheten att applicera kunskapen generellt och blivit mer säkerhetsmedveten i sitt privata liv, till exempel när han ska slå in sin kod.

Tabell 4.3 Sammanfattning utbildning.

	I1	I2	I3	I4	I5
Värde: Poäng på aktiviteten gentemot de andra aktiviteterna	10/20	12/20	5/20	6/20	8/20
Belöning: Finns det någon belöning om det hade tillhandahållits utbildningar	Ingen.	Ingen.	Större förståelse och uppfattning.	Skydda sina kunder och deras konfidentiella information.	Att bli mer säkerhets-medveten privat.

4.4 Säkerhetskopiering

Angående aktiviteten säkerhetskopiering såg svaren lika ut vid vissa punkter och vi såg tydliga mönster från intervjupersonerna. Angående vem det är som utför säkerhetskopiering av information på arbetsplatsen fick vi oklara resultat på. Det var endast I3 som med säkerhet kunde säga att han var medveten om att företaget ansvarar för säkerhetskopieringen och att det sköts per automatik i systemen. Resterande intervjupersoner antingen tror att ansvaret ligger hos företaget och att det sköts per automatik, eller så vet de inte. Samtidigt som de inte vet hos vem ansvaret ligger, har de heller ingen uppfattning om hur ofta det utförs. Det är enbart I1 som tror sig ha en uppfattning om hur ofta det utförs. Noterbart är att endast I5 är medveten om att ifall information lagras på en USB-sticka krävs det kryptering.

Angående värdet av säkerhetskopiering gentemot de andra aktiviteterna var intervjupersonerna av olika mening. I1, I4 och I5 såg ett högre värde med säkerhetskopiering då det valdes som majoritet av aktiviteterna, i jämförelse med I2 och I3 som värderade säkerhetskopiering något lägre.

Samtliga intervjupersoner, förutom I5, såg en klar belöning med säkerhetskopiering och menade att både dem själva samt företaget kan känna trygghet om det skulle hända något med deras information. I4 menade att konsekvenserna skulle vara enorma ifall det inte skulle utföras säkerhetskopiering.

En gemensam nämnare hos samtliga intervjupersoner var att de ansåg att ansvaret med säkerhetskopiering bör ligga hos företaget, där I3 menar att det är en omöjlighet ifall ansvaret hade legat på individen då det är väldigt mycket information som behandlas. I2 poängterar att om ansvaret ska ligga på individen så finns den mänskliga faktorn, vilket gör att något alltid kommer att missas.

”Den mänskliga faktorn finns alltid, vilket gör att det alltid någon gång kommer att missas. Så jag tycker att det ska ligga på högre ort.” (Bilaga 3, fråga 22).

Tabell 4.4 Sammanfattning säkerhetskopiering.

	I1	I2	I3	I4	I5
Förväntad förmåga: Har full förståelse om vems ansvar det är att utföra säkerhetskopiering	Nej.	Nej.	Ja, det sker automatiskt.	Nej.	Nej.
Värde: Poäng på aktiviteten gentemot de andra aktiviteterna	17/20	12/20	11/20	16/20	14/20
Tid: Vet hur ofta det utförs	Tror det sker 1 gång per dag.	Nej.	Nej.	Nej.	Nej.
Belöning: Ser belöning i att säkerhetskopiering utförs	Ja, trygghet.	Ja, säkerhet och trygghet.	Ja, säkerhet och trygghet.	Ja, om något händer är det bra med en kopia.	Nej, vet inte.

4.5 Datamissbruk och övervakning

Samtliga intervjupersoner medgav att de inte har full vetskap angående företagets ISP, och menade att de känner till att det existerar en ISP och de är medvetna om de viktigaste punkterna i den.

Det var delade åsikter mellan våra intervjupersoner avseende deras uppfattning om det upplevs lätt eller svårt att bryta mot företagets ISP. I4 menade att han upplevde det som svårt eftersom han följer de direktiv som finns medan, I1 och I2 påpekade hur lätt det kan vara att bryta mot den genom att till exempel glömma eller strunta i att låsa sin dator när man lämnar sin arbetsstation. I3 och I5 svarade att de anser det är svårt att bryta mot företagets policy, dock medger alla utom I1 att de har gjort små överträdelser enstaka gånger.

Samtliga intervjupersoner verkade vara överens om att de inte lägger någon större vikt i att företaget kan tänkas utföra övervakning av sina anställda för att upprätthålla säkerheten. Även om I5 inte tyckte övervakning var direkt nödvändigt så förstod han ändå varför företaget skulle vilja övervaka sina anställda.

Det var inte förvånande att ingen av våra intervjupersoner med säkerhet kunde svara på frågan om hur ofta företaget utför någon typ av övervakning av dem. I1 menar på att han tror att företaget har möjlighet att kunna övervaka och granska sina anställda när som helst, dock tror han att det måste finnas en tydlig anledning eller misstanke till varför de skulle göra det.

”...möjligheten finns ju att övervakas hela tiden tror jag…Utan där måste finnas någon anledning till att man ska titta på det.” (Bilaga 2, fråga 17e).

Även I2 hade en uppfattning om hur ofta företaget kan tänkas utföra övervakning och granskning av sina anställda. Han säger sig tro att det utförs dagligen genom ett system som flaggar aktiviteter som inte är tillåtna.

Alla våra intervjupersoner gav olika svar på vad en möjlig belöning kan vara om företaget utför övervakning av dem. I1 var den enda respondenten som inte såg någon belöning alls ur ett personligt perspektiv. Enligt honom skulle det inte göra någon skillnad om han skulle vara medveten om att företaget utförde övervakningar av honom eller inte. Han nämnde även att vissa anställda kan uppleva det som något negativt med att bli övervakad. I2 ansåg att övervakning och granskning av anställda kan resultera i en trygghet bland de anställda till följd av en känsla att arbetet utförs korrekt och säkert. I3 ansåg att belöningen är att han kan rättfärdiga sina handlingar ifall det av någon anledning skulle behövas, och att de som bryter mot företagets policy i någon form kan bli upptäckta. I4 var inne på samma spår att övervakning och granskning är nödvändigt och ett effektivt sätt att upptäcka och hindra oärliga handläggare. I4 såg inget problem personligen med att företaget övervakar sina anställda, utan det är något han förväntar sig att de gör. I5 menade i sin tur att det kan vara en metod för att bli varse sina egna brister i sitt arbete och på så sätt kunna lära sig av sina misstag och bli bättre.

Tabell 4.5 Sammanfattning datamissbruk och övervakning.

	I1	I2	I3	I4	I5
Förväntad förmåga: Är det lätt eller svårt att bryta mot företagets ISP?	Lätt hänt.	Det är nog väldigt lätt.	Svårt, med risk för små övertramp.	Svårt, följer de direktiv som finns.	Svårt, med risk för små övertramp.
Värde: Poäng på aktiviteten gentemot de andra aktiviteterna	7/20	12/20	8/20	12/20	9/20
Tid: Vet hur ofta det utförs övervakning	Nej.	Tror det utförs dagligen.	Nej.	Nej.	Nej.
Belöning: Ser belöning i att övervakas	Ingen.	Trygghet.	Rättfärdiga sina handlingar.	Hindra oärliga handläggare.	Förbättras om man gör misstag.

4.6 Konfidentialitet

För aktiviteten att skydda konfidentiell information såg vi ett tydligt och gemensamt resultat. När det gäller förväntade förmågan att skydda den konfidentiella informationen, så menade samtliga intervjupersoner att de gör det, men inte aktivt. Det var ingenting som intervjupersonerna

gjorde på daglig basis, i form av funktioner eller att lagra information på specifika ställen på sin enhet.
Vissa intervjupersonerna nämnde att de var medvetna om att informationen de arbetar med är skyddad på ett säkert sätt i systemen, medan de andra intervjupersoner antog att systemen var tillräckligt säkra och att det inte krävdes extra handlingar från dem. I1, I2 och I4 nämnde att de var särskilt säkerhetsmedvetna när det gäller att lämna ut konfidentiell information via mejl och telefon, där det handlade om försiktighetsåtgärder så att viktig information inte kommer till fel personer. I3 menade på att där fanns en problematik om det skulle ligga på individens ansvar och de skulle utföra det personligen. Han menade att de behandlar väldigt mycket information dagligen så det hade varit en omöjlighet, eftersom det hade tagit för mycket tid.

När vi ställde aktiviteten att skydda konfidentiell information mot de andra aktiviteterna så ansåg samtliga intervjupersoner att det var viktigare att skydda konfidentiell information gentemot alla de andra aktiviteterna. Noterbart var att merparten av intervjupersonerna värderade att skydda konfidentiell information som ”absolut viktigare”, förutom I3 som ansåg den var viktig men inte i samma grad som de övriga fyra intervjupersonerna.

Att alla ansåg att skydda konfidentiell information som viktig, speglades även i deras svar på belöningen med det. Samtliga intervjupersoner var övertygade och eniga om att det är något som måste göras. I1, I2, I3 och I4 menade att det är ett krav, och I1 menade att det är något som ska tas för givet då det är otroligt viktigt att hantera konfidentiell information med tanke på deras arbete. I4 påpekade att det inte är något som de själva har hittat på, utan att det enligt svensk lag krävs att säkert skydda sina kunders konfidentiella information. I4 och I5 nämnde också att det är en skyldighet mot våra kunder och för att få dem nöjda. Samtliga intervjupersoner medgav att de inte utförde kryptering eller andra metoder för att skydda konfidentiell information. Därför väljer vi att inte presentera resultaten angående hur ofta de skyddar konfidentiell information eftersom de menar att de gör det varje dag på diverse vis som att exempelvis låsa sina datorer. Angående om hur lång tid det tar att skydda konfidentiell information menade samtliga att det tar rimligt med tid att utföra åtgärderna.

När vi ställde vårt scenario till intervjupersonerna, angående hur de hade agerat och motiverat sina val vid mobil användning (se bilaga 1, fråga 25), så fanns det inget klart mönster över hur de hade reagerat. Antingen får det ta lite längre tid och är säkrare, än att det ska gå snabbt och effektivt men är mindre säkert. Två av intervjupersonerna, I1 och I2, menade att de hade skickat mejlet direkt utan att tänka på säkerheten, där även I1 påpekade att han inte tror att det är någon skillnad avseende säkerheten i publika nätverk jämfört med privata. De tre andra intervjupersonerna menade att de hade skickat vidare mejlet beroende på hur känslig informationen mejlet innehöll. Det var enbart I3 som svarade att han inte sätter sig på en offentlig yta och arbetar därifrån. Han menade att han hade väntat med att skicka mejlet tills han är tillbaka på arbetsplatsen, eller möjligtvis väntat tills han hade befunnit sig i en offentlig miljö där han inte har folk runt omkring sig.

Tabell 4.6 Sammanfattning konfidentialitet.

	I1	I2	I3	I4	I5
Förväntad förmåga: Skyddar information på något sätt	Försiktig-hetsåtgärder.	Försiktig-hetsåtgärder.	Försiktig-hetsåtgärder.	Försiktig-hetsåtgärder.	Försiktig-hetsåtgärder.
Värde: Poäng på aktiviteten gentemot de andra aktiviteterna	17/20	18/20	14/20	18/20	18/20
Tid: Anser det tar rimligt lång tid	Ja.	Ja.	Ja.	Ja.	Ja.
Belöning: Ser belöning i att skydda konfidentiell information	Nej, främst en nödvändig-het som ska tas för givet.	Nej, skyldighet mot våra kunder.	Nej, ett krav från vår sida mot våra kunder.	Ja, främst enligt lag men det leder till nöjda kunder.	Ja, nöjda kunder.
Scenario mobil användning: Anser att vara effektiv är viktigare än säkerhetsaspekten	Ja.	Ja.	Nej.	Beroende på hur känslig information-en är.	Beroende på hur känslig information-en är.

5. Analys och diskussion

Här analyserar vi empirin genom att koppla resultaten från våra intervjuer med vår teoretiska bakgrund från litteraturgenomgången (kapitel 2). Vi analyserar utifrån varje aktivitet samtidigt som vi analyserar likheter och skillnader bland våra intervjupersoner.

5.1 Autentisering

Vår undersökning visar att samtliga intervjupersoner enbart använde användarnamn och lösenord för att autentisera sig mot systemen. Det är idag den vanligaste formen av autentisering som framkommer enligt Stamp (2006). Detta kan stödja våra intervjupersoners svar angående förmåga av att autentisera sig, då merparten ansåg att det är en lätt process. I4 menade att det är en svår process med tanke på att det är omständigt att ha fem unika användarnamn och lösenord, vilket stämmer överens med Adams & Sasse (1999) påstående om att en individ max kan memorera 4-5 unika lösenord samtidigt. Vi menar att det kan ses som en säkerhetsbrist då han behöver skriva ner sina lösenord när de blir för många att memorera, vilket strider mot Stamp (2006) rekommendationer för säker hantering av lösenord. Stamp (2006) nämner även smartcards och biometriska autentiseringar som alternativ eller komplement men det kan uppfattas som överflödigt i det här fallet eftersom att användarnamn och lösenord bör vara tillräckligt ifall de hanteras på rätt sätt.

Vid frågan om värdet av aktiviteten när vi ställde aktiviteterna mot varandra, såg vi ett tydligt mönster där merparten av intervjupersonerna var överens om att aktiviteten autentisering var en av de aktiviteter som värderades högst. Anmärkningsvärt var att I2 värderade aktiviteten som lägst möjliga, vilket kan bero på att han är den som loggar in flest gånger per dag och att han anser att det tar för lång tid att autentisera sig mot alla diverse system. Det märkliga är att samtidigt som han värderar aktiviteten lågt, ser han en klar belöning med att kunna autentisera sig då ingen annan kan utföra något på hans dator och i hans namn. Vilket som överensstämmer med Steel & König (2006) påstående om att attraktionskraften av en aktivitet beror på både situations- och individuella skillnader där man avgör behovet av kraft som krävs för en viss aktivitet och kan på så sätt utgöra en risk då han inte inser värdet av aktiviteten.

Busson (2008) och Ni et. al. (2010) understryker att ett företag som samlar in och bearbetar känslig information som personuppgifter och kontouppgifter bör använda någon form av rollbaserad åtkomstbehörighet. Detta samstämmer med I3:s beskrivning av vilken belöning han får ut av autentisera sig. Han understryker vikten av att han får tillgång till viss information som andra kollegor inte har tillgång till. Medan våra övriga intervjupersoner menade på att belöningen med att autentisera sig är att ingen annan kan göra något i hans namn och på så sätt har ryggen fri ifall något skulle hända. I1 och I4 nämnde att de andra medarbetarna inom avdelningen också har tillgång till samma information som de andra, vilket visar att de är medvetna om att företaget använder sig av rollbaserad åtkomstbehörighet, men de såg inte detta som en belöning med autentisering. Alla intervjupersoner påvisar en god säkerhetsmedvetenhet eftersom de ser en klar orsak till varför man

behöver autentisera sig. Vi tolkar detta som att I3 är mer införstådd och medveten om att rollbaserad åtkomstbehörighet är något som är vitalt och som ska tas på allvar, jämfört med de andra intervjupersonernas åsikter.

5.2 Hantering av lösenord

Avseende hur hantering av lösenord sker, råder det stora skiljaktigheter mellan intervjupersonerna. Anmärkningsvärt är att det endast är en av våra fem intervjupersoner, I5 som alltid memorerar sina lösenord och aldrig skriver ned dem. Därmed är I5 väl medveten om riskerna som uppstår vid nedskrivande av sina lösenord då han menar att belöningen är att ingen kan ta del av dem, vilket även stöds av Stamp (2006) som poängterar att nedskrivande av lösenord kan anses som en säkerhetsbrist. I3 och I4 visade motivation till att försöka memorera sina lösenord men när de blev för många eller när de skulle vara lediga en längre tid var de tvungna att skriva ned dem. I1 och I2 ansåg att det var en omöjlig uppgift att memorera alla sina lösenord och menade att det krävs att skriva ned sina lösenord för att kunna komma ihåg dem, där I2 poängterade att han kunde ha upp till 10-13 unika lösenord samtidigt. I1 poängterade trots allt att han är medveten om att det inte är en säker hantering av sina lösenord. Anledningen till att intervjupersonerna tvingas att skriva ned sin lösenord kan grunda sig i det som Adams & Sasse (1999) och Gaw & Felten (2006) påpekar att en användare endast kan memorera fyra till fem unika lösenord samtidigt samt att ju mer komplexa lösenord en användare har desto svårare blir det att memorera dem. Warkentin & Willison (2009) understryker också att en användare som har flera lösenord att komma ihåg i kombination till att de måste bytas regelbundet försvårar chansen för användaren att kunna memorera dem. Detta tolkar vi som starka bidragande orsaker till att de flesta av våra intervjupersoner tvingas att skriva ner dem vilket utgör en säkerhetsrisk. I3 påstod att han hanterar sina lösenord säkert när han antecknar dem i mobilen när han åker på semester. Vi tolkar detta som att han har ett lågt säkerhetsmedvetande i den här aspekten eftersom det mostrider vad Stamp (2006) och Selvarani & Ravi (2013) påpekar angående nedskrivande av lösenord och resande med företagsinformation.

Vi ser ett tydligt mönster av att beroende på hur intervjupersonerna hanterar sina lösenord så anser de att hanteringen av dem är av olika svårighetsgrad. De intervjupersonerna som behöver skriva ned sina lösenord anser att hanteringen är en svår process, medan de intervjupersoner som memorerar eller åtminstone försöker memorera anser att det är en lätt process.

Den bild vi har fått förmedlat av I1 är att han anser att hantering av lösenord är en svår process och som han inte ser någon belöning av, och därmed inte ser något större värde överrensstämmer med Steel & König (2006) som påstår att om en individ ser ett högt behov av kraft och ingen belöning av en aktivitet så kommer också värdet att bli obetydligt. Vi menar att hantering av lösenord är en viktig process som man bör ha bra kunskap i och sätta stort värde på och som användare bör ta på allvar vilket understryks av Chen, Shaw & Yang (2006).

Att endast två intervjupersoner, I2 och I3 värderade aktiviteten hantering av lösenord högt gentemot de andra intervjupersonerna, 16 respektive 19 poäng, är något som är anmärkningsvärt och där vi tydligt ser att det råder skiljaktigheter mellan intervjupersonerna. Att tre av intervjupersonerna såg ett lägre värde med att hantera lösenord kan bero på att det kan förekomma bristande kommunikation mellan säkerhetsavdelningen och användarna som Adams & Sasse (1999) påpekar.

Adams & Sasse (1999) understryker att användarna vill ha en förståelse för säkerheten i praktiken och på så sätt öka deras säkerhetsmedvetande i systemen och vikten av det.

5.3 Utbildning

Med hjälp av våra intervjuer fick vi reda på att försäkringsbolaget inte gav sina anställda möjligheten till att utbilda sig inom IT-säkerhet. Därför kan vi inte analysera deras svar angående förväntad förmåga och tid eftersom deras svar på dem frågorna saknar validitet i detta sammanhang (Jacobsen, 2002).

Aktiviteten utbildning visade sig inte ha något större värde hos våra intervjupersoner, gentemot de andra aktiviteterna. Det var I1 och I2 som värderade utbildning i IT-säkerhet högst av våra intervjupersoner men samtidigt var de ensamma om att inte se någon belöning med ifall företaget hade gett dem den möjligheten. Detta kan anses bero på att de tycker sig besitta tillräcklig kunskap i IT-säkerhet. Yngström & Björck (1999) påpekar att det krävs att utbildning ges till de anställda i takt med utvecklandet av ny teknik och i vårt företags situation skickas det enbart ut information till de anställda när det cirkulerar spammejl och liknande.

I4 visade ingen motivation överhuvudtaget till att lära sig om IT-säkerhet vilket enligt Steel & König (2006) kan bero på personliga skillnader i hans behov och vanor jämfört med de andra intervjupersonerna. Vi tolkar honom som en eventuell säkerhetsrisk eftersom han påvisar en tendens att vilja lägga över hela ansvaret för IT-säkerheten på IT-avdelningen vilket överensstämmer med Workman, Bommer & Straub (2008). Yngström & Björck (1999) påpekar vikten av att ha åtminstone grundläggande kunskap om informationssäkerhet oavsett vilken bransch en person arbetar i. Vi tycker att det är värt att vårt försäkringsbolag ställer sig frågan om den grundläggande kunskapen som deras anställda för med sig in i deras informationssystem och arbetsmiljö är tillräcklig. Det kan vara värt att de erbjuder någon form av utbildning i IT-säkerhet, utöver den information som de skickar ut i mejl, eftersom enligt Alvarez (2013) kan konsekvenserna av en informationsläcka leda till förlorade kunder.

5.4 Säkerhetskopiering

I3 var den enda av våra intervjupersoner som med säkerhet kunde svara att säkerhetskopiering utförs automatiskt och därmed inte ligger på den enskilda individens ansvar. Detta tolkar vi som att I3 påvisar en högre säkerhetsmedvetenhet i förhållande till resterande intervjupersoner eftersom han bevisar en viss förståelse för hur den interna infrastrukturen för säkerhetskopiering ser ut som enligt Busson (2008) leder till att man blir mer säkerhetsmedveten och kan behandla och lagra informationen mer säkert. Att ingen av våra intervjupersoner kunde svara på hur ofta det utförs säkerhetskopiering tillsammans med att det endast var en intervjuperson som visste var ansvaret låg påvisar att förståelsen för den interna infrastrukturen för säkerhetskopiering, som enligt Busson (2008) är viktig att förstå, överlag är bristande bland våra intervjupersoner.

Värdet av att säkerhetskopiera information var alla våra intervjupersoner någorlunda överens om. Alla utom en intervjuperson påpekade att de på ett eller annat sätt förstod att anledningen till varför

man bör utföra säkerhetskopiering är för att, precis som Busson (2008) påpekar, det är en vital aspekt för ett företags informationssäkerhetssystem och för att säkerställa den information som de behandlar och lagrar. De fyra intervjupersonerna uppgav i sina svar att belöningen av att säkerhetskopiera information är att det skapar en trygghet och säkerhet vilket vi tolkar som att de förstår vikten av att säkerställa den behandlade och lagrade informationen.

Enligt Workman, Bommer & Straub (2008) innebär det ofta att när en användare lägger över ansvaret för IT-säkerheten på någon annan leder det till en säkerhetsrisk. Vi fann ett exempel som säger emot detta påstående när vi intervjuade I2. Han ansåg att det skulle vara fullt orimligt ifall företaget skulle låta varje anställd ansvara för sina respektive säkerhetskopior på grund av att den mänskliga faktorn alltid kommer finnas och att en anställd därmed någon gång kommer att glömma att säkerhetskopiera. I2s argument kan kopplas till att den anställde ofta ses som den svagaste länken i ett informationssystem, enligt Bulgurcu, Cavusoglu & Benbasat, 2010 och Warkentin & Willison, 2009, och därför bör ansvaret för vissa arbetsuppgifter läggas på någon annan än användaren av systemet som i vårt fall är respektive försäkringsförmedlare.

5.5 Datamissbruk och övervakning

Samtliga av intervjupersonerna menade att de är medvetna om att det finns en uttalad och tillgänglig ISP på deras intranät, och som de skrev på när det anställdes av företaget men att de inte fullt ut kommer ihåg vad den innehåller.
Merparten av intervjupersonerna menade på att det kan vara enkelt att göra små överträdelser av företagets ISP i form av att glömma att låsa datorn när man exemplevis ska gå iväg på toaletten en kortare stund. Om användaren lämnar sin arbetsstation tillgänglig för personer som saknar åtkomstbehörighet kan detta enligt Alvarez (2013) och Lee & Lee (2002) ses som en säkerhetsbrist och lågt säkerhetsmedvetande vilket kan leda till stora konsekvenser för företaget i form av ekonomiska förluster och dåligt rykte. Detta styrker Lee & Lee's (2002), Bulgurcu, Cavusoglu & Benbasat (2010) och Warkentin & Willison (2009) vidare påstående att det största hotet kommer från insidan och att användaren i det här fallet kan ses som en svag länk.

Busson (2008) rekommenderar att företag bör införa loggövervakning på deras system för att spåra och rapportera aktiviteter av konfidentiell information och Herath & Rao (2009) påpekar att en anställd är mer inställsam till att följa företagets ISP om han är medveten om att det utförs regelbundna kontroller. Våra intervjupersoners svar angående belöning av att deras arbetsgivare kan tänkas utföra övervakning av dem stämmer överens med detta. De uppger att det kan vara ett effektivt tillvägagångssätt att rättfärdiga sina handlingar och för att hindra oärliga försäkringsförmedlare, vilket vi anser ses som positivt ur säkerhetssynpunkt.

Bulgurcu, Cavusoglu & Benbasat (2010) nämner att om en anställd ska följa en ISP kräver det oftast att han tvingas ta försiktighetsåtgärder som leder till besvär och längre tid att utföra en uppgift, och att den anställde oftast ser det som en nackdel och ett hinder för produktiviteten, men detta anser vi inte överrensstämmer med den bild som vi skapat oss utifrån intervjupersonernas beskrivningar angående försikthetsåtgärder med avseende på konfidentiell information. Samtliga intervjupersoner menade på att när det skyddar konfidentiell information i den grad de kan, så tar de till försiktighetsåtgärder för att upprätthålla störst möjliga säkerhet kring att vital information inte ska läcka ut till fel personer. Alla anser att det har ett stort värde och att det tar rimligt med tid att

utföra, därav anser vi att det inte ses som en nackdel eller hinder för produktiviteten, och därmed visar de ett säkerhetsmedvetande vid denna punkt.

Vidare har vi förståelse för att intervjupersonernas uppskattade värde på aktiviteten gentemot de andra aktiviteterna fick ett av de lägsta poängen, kan bero på att det inte är en aktivitet som utförs personligen och tanken var att vi ville undersöka hur väl medvetna de är samt deras inställning till företagets ISP och övervakning av de anställda från företagets sida.

5.6 Konfidentialitet

Att skydda konfidentiell information var den aktivitet som totalt sett värderades högst av våra intervjupersoner. Alla våra fem intervjupersoner visade sig förstå och arbeta efter vad Oscarsson, Öberg & Rystedt (2009) säger om informations konfidentialitet, nämligen att känslig information inte ska göras tillgänglig för obehöriga. I1, I2 och I4 efterföljer detta genom att tänka på hur och vilken information de lämnar ut via mejl och telefon. Det var dock det enda aktiva samtliga intervjupersoner utförde för att skydda konfidentiell information. Både I3 och I5 nämnde att den enda gången det krävs att kryptera konfidentiell information är när de ska lagra information på usb-minne. Detta stämmer väl överens med vad Selvarani & Ravi (2013) och Diesburg & Wang (2010) förespråkar att användaren skall utföra när han sparar information på sekundära lagringsenheter.

Byun & Li (2008) som menar att syftet till varför ett företag samlar in och bearbetar en viss typ av information ska vara tydligt formulerad och fungera i företagets åtkomstbehörighetsmodell. På frågan om hur de hade reagerat ifall en kollega hade tagit del av deras konfidentiella information utan deras tillstånd (Bilaga 1, fråga 21) svarade I1, I2, I3 och I5 identiskt. De hade inte tyckt att det varit okej om det hade skett, där de bland annat hade undrat vad anledningen kunde tänkas vara. Därmed visar dessa fyra intervjupersoner att de förstår tanken som Byun & Li (2008) lyfter fram angående att en viss typ av information endast ska kunna nås och bearbetas när syftet med att bearbeta informationen stämmer överens med dess syfte när det samlades in.

Enligt alla våra intervjupersoner gör de inget rent tekniskt för att skydda konfidentiell information eftersom de förväntar sig att systemen de sitter och arbetar i ska vara tillräckligt säkra. Vi vet inte med säkerhet vilka instruktioner de anställda har fått angående hur de ska genomföra sitt arbete avseende konfidentiell information. Vi tolkar det ödmjukt genom att påpeka att vi ser en potentiell risk av den anledning att vi får en tydlig uppfattning om att de tenderar att vilja lägga över ansvaret för att säkra den konfidentiella informationen på de som ansvarar för IT-säkerheten, vilket Workman, Bommer & Straub (2008) lyfter fram som en eventuell säkerhetsrisk. Det dem gör för att skydda konfidentiell information går i större omfattning ut på försiktighetsåtgärder. Utöver att samtliga intervjupersoner är uppmärksamma och försiktiga när det gäller utlämning av information över mejl och telefon beskrev I3 att de har särskilda bestämmelser när det gäller hantering och oåterkallig kassering av utskrivna dokument. Detta faller i linje med vad Diesburg & Wang (2010) rekommenderar att ett företag ska implementera angående borttagning av dokument som kommer ifrån datormiljö.

Angående belöningen med att skydda konfidentiell information säkert menade intervjupersonerna att det inte fanns en direkt belöning utan att de hävdade att det handlade om krav enligt svensk lag, exempelvis personuppgiftslagen. Detta var den gemensamma synen hos I1, I2, I3 och I4. I5 gick

istället in på vad kravet kan leda till, nämligen nöjda kunder. Med detta sagt förstod alla våra intervjupersoner vikten av att skydda konfidentiell information i den branschen de arbetar i och konsekvenserna som kan följa av att inte säkerställa den konfidentiella informationen vilka lyfts fram av Alvarez (2013).

Huang, Zhang & Jim Luo (2010) påpekar att det krävs riskbedömning av användaren med hänsyn till säkerhets- och kommunikationskrav när han ska arbeta mobilt i ett trådlöst nätverk. I3, I4 och I5 påvisade att de skulle gjort en riskbedömning när det handlade om att arbeta mobilt i ett trådlöst nätverk som inte är företagets. De tre intervjupersonerna nämnde att informationens känslighet spelar en avgörande roll för om de hade valt att arbeta offentligt eller inte. I5 menade att krypteringen på deras telefoner förmodligen inte är den bästa och att han då hade tänkt sig för om han skulle öppna ett mejl innehållande känslig information. Både I3 och I5 visade att de även bedömer den sociala aspekten och inte enbart den tekniska. De hade sett sig omkring för att säkerställa att ingen kan ta del av deras konfidentiella information genom att ”tjuvkika”. Med detta sagt tolkar vi det som att I3, I4 och I5 påvisar en riskbedömning enligt Huang, Zhang & Jim Luo (2010) när det gäller hantering och bearbetning av känslig information när de arbetar mobilt i publika nätverk och i offentliga miljöer. I1och I2 påvisade inte någon riskbedömning som sina kollegor gjorde. I1 sa sig tro att säkerheten är den samma i privata som i publika nätverk, och som vi ser som en säkerhetsrisk. Som Vaughn, Dampier & Warkentin (2004) påpekar så skapades internet för att göra information delbar och nåbar för alla. Deras privata nätverk är mer skyddat än de flesta publika nätverken som oftast inte ens kräver ett lösenord eller enbart skyddas med ett lösenord som är direkt tillgängligt för alla.

6. Slutsatser

I uppsatsens inledning formulerade vi forskningsfrågan:

> *Hur ser de anställdas säkerhetsmedvetenhet ut inom ett försäkringsbolag som hanterar känslig information?*

Efter att studerat våra intervjupersoners syn och förmåga gällande aktiviteten *autentisering* visade vår undersökning inget utmärkande mer än att I4 tyckte att det upplevdes som omständigt eftersom informanten ansåg att de hade för många system som de behövde autentisera sig emot på en arbetsdag. Samtliga av våra intervjupersoner påvisade en god säkerhetsmedvetenhet genom deras syn på belöningen av funktionen att autentisering i form av att ingen kan utge sig för att vara någon annan. Alla var överens och ansåg det vitalt att företaget genom autentisering kan spåra vem som har utfört en viss handling vilket kan förhindra anställda att utföra datamissbruk.

När vi undersökte våra fem intervjupersoners förmåga att *hantera sina lösenord* fann vi en säkerhetsrisk då fyra av fem åtminstone någon gång antecknade sina lösenord i datorn, mobilen eller på anteckningsblock. I3 påvisade ett lågt säkerhetsmedvetande i den här aspekten när han menade att det var säkert att spara sina lösenord i mobilen. Till skillnad från I3 så var däremot I1 medveten om säkerhetsrisken i att anteckna sina lösenord i mobilen men medgav att han gjorde det ändå. I5 var den enda som både memorerar alla sina lösenord och samtidigt ser anledningen till varför man ska försöka memorera dem istället för att anteckna dem vilket gör honom till den enda med högt säkerhetsmedvetande av våra intervjupersoner när det gäller säker hantering av lösenord.

Aktiviteten *utbildning i IT-säkerhet* blev lägst värderad av våra intervjupersoner. Även om merparten av våra intervjupersoner inte ansåg att de behövde utbildas ställde de sig ändå positiva till låta företaget erbjuda utbildning. De ansåg att det inte skulle skada att lära sig nytt och hålla sig uppdaterade med ny teknik. I4 var den som utmärkte sig från de andra genom att påvisa en låg säkerhetsmedvetenhet när han förklarade att han varken hade viljan eller motivationen till att lära sig något nytt. I4 lade inget intresse på att försöka förstå hur IT-säkerheten är uppbyggd utan visade en stark tendens till att vilja lägga över hela ansvaret på IT-avdelningen.

Samtliga av våra intervjupersoner påvisade en brist i förståelsen kring hur infrastrukturen för *säkerhetskopiering* ser ut på företaget. I3 var den enda som var medveten om var ansvaret för att genomföra säkerhetskopieringar låg men han kunde dock inte svara på hur ofta det genomförs. Med tanke på att de flesta såg en klar belöning och värde i säkerhetskopiering brister ändå deras säkerhetsmedvetande genom att de inte kan svara på om det är individen eller företagets ansvar att genomföra säkerhetskopiering och hur ofta det utförs eller ska utföras.

Avseende *datamissbruk och övervakning* var ingen av våra intervjupersoner medvetna om allt vad företagets ISP innehåller. Eftersom att den här punkten kan anses vara den mest känsliga för våra intervjupersoner att uttrycka sig fullt sanningsenligt tolkade vi deras svar ödmjukt.
Samtliga utom I1 medgav att de någon gång har brutit mot företagets ISP genom att, medvetet eller omedvetet, inte låst sin dator när de av en enkel anledning lämnat sin arbetsstation för en kort stund.

Detta anser vi är en säkerhetsbrist då de bryter mot företagets ISP, även om de befinner sig i en sluten miljö tillsammans med sina kollegor. Det är en handling som de är medvetna om inte är tillåten men det sker ändå. Majoriteten såg trots det en klar belöning i och orsak till varför företaget kan tänkas behöva övervaka sina anställda, det kan hindra oärliga handläggare och det skapar en slags trygghet, och påvisar därmed en klar säkerhetsmedvetenhet.

Det är inte förvånande att våra intervjupersoner sammanlagt värderade *skydd av konfidentiell information* högst gentemot de andra aktiviteterna. Vi anser därmed att det råder en hög säkerhetsmedvetenhet bland samtliga intervjupersoner. Att skydda konfidentiell information prioriteras högt i försäkringsbranschen och även så i vårt försäkringsbolag. Det finns dock en potentiell risk för lågt säkerhetsmedvetande eftersom de tenderar att lägga över en del av ansvaret för säkringen av konfidentiell information på IT-avdelningen.

Vi har kunnat svara på hur säkerhetsmedvetenheten kan se ut bland de anställda på vårt försäkringsbolag. Att aktiviteterna utbildning i IT-säkerhet och säkerhetskopiering inte utfördes alls eller på det sättet vi förväntade oss efter vår granskning av litteratur, medförde att vårt syfte fick nya infallsvinklar på dessa aktiviteter. Vi vill poängtera att när vi har låtit våra intervjupersoner värdera aktiviteterna har vi ställt dem mot varandra. Det behöver inte betyda att de anser att en aktivitet som de har värderat lågt anses helt oviktig. Vår studie visade sig även ha bidragit till att upplysa de anställda om att de bör ta en djupare titt på företagets ISP och kring infrastrukturen för säkerhetskopiering, vilket en av våra intervjupersoner påpekade. För att kunna generalisera säkerhetsmedvetenheten i ett enstaka försäkringsbolag eller i branschen rekommenderar vi att i framtida forskning utföra kvantitativa studier med ett större urval. Vi valde en kvalitativ ansats för att vi var mer intresserade av att ta reda på hur en individ uppfattar och resonerar kring en situation. Vi rekommenderar även att i framtida forskningar om säkerhetsmedvetande hos anställda att utföra en förintervju med en expertanvändare och därmed få en verklighetsbild över hur företagets ISP ser ut och för att på så sätt ta reda hur de förväntas arbeta och vilka krav som ställs på dem.

Bilaga 1 - Intervjuguide

Inledande frågor:

1. Vilken roll har du inom företaget?
2. Hur god datorvana har du enligt dig själv?
3. Hur säkerhetsmedveten är du enligt dig själv? 1-4?

Förväntad förmåga att slutföra en aktivitet med avseende på säkerhet:
4. Hur hanterar du dina lösenord och hur lätt/svårt anser du att det är?
-Får ni era lösenord genererade till er eller får ni välja dom själva?
-Hur lätt är det att memorera dina lösenord?
-Brukar du skriva ner dina lösenord? Hur?
5. Hur loggar du in på en tjänst och hur lätt/svårt anser du att det är?
-något utöver användarnamn och lösenord?
-hur många användarnamn/lösenord har du?
6. Lär du dig mer om IT-säkerhet (utbildning) och anser du att det är lätt/svårt?
7. Har företaget en tydligt uttalad ISP?/ Kan du den?
8. Hur säkerhetskopierar du information? Är det lätt/svårt?
-gör ni det själv eller sköts det automatiskt?
9. Anser du att det är lätt eller svårt att bryta mot er bestämda policy?
-på vilket sätt?
10. Hur skyddar du viktig information (konfidentiell information) anser du att det är lätt/svårt?
-t.ex. kryptering?

Värde att slutföra en aktivitet med avseende på säkerhet:
Här kommer frågor där vi ställer två aktiviteter mot varandra. Vi vill att ni ska välja ett av alternativen med hjälp av svarsalternativen (1-4). Samt en kort kommentar om varför.
1. det är absolut viktigare att hantera lösenord än att ta backups
2. det är något viktigare att hantera lösenord än att ta backups
3. det är något viktigare att ta backups än att hantera lösenord
4. det är absolut viktigare att ta backups än att hantera lösenord

Autentisering:
11. Är det viktigare att kunna autentisera (logga in) dig mot en tjänst än att
a) du hanterar dina lösenord?
b) lära dig mer inom It-säkerhet?
c) ta backups?
d) företaget utför övervakning av er?
e) skydda viktig information (konfidentiell information)?

Hantering av lösenord:
12. Är det viktigare att hantera lösenord än att
a) lära dig mer inom IT-säkerhet?
b) ta backups?
c) företaget utför övervakning av er?
d) skydda viktig information (konfidentiell information)?

Utbildning:
13. Är det viktigare att lära sig mer inom IT-säkerhet än att
a) ta backups?
b) företaget utför övervakning av er?
c) skydda viktig information (konfidentiell information)?

Säkerhetskopiering:
14. Är det viktigare att ta backups än att
a) företaget utför övervakning av er?
b) skydda viktig information (konfidentiell information)?

Datamissbruk/övervakning:
15. Är det viktigare att företaget utför övervakning av er än att
a) skydda viktig information (konfidentiell information)?

(Tid) Hur lång tid tar det att utföra en aktivitet med avseende på säkerhet:
16. Hur lång tid tar det och anser du det tar rimligt lång tid att

a) autentisera dig mot en tjänst?
b) hantera lösenord (i form av ändra, memorera mm)?
c) lära sig mer inom informationssäkerhet?
d) ta backups?
e) skydda viktig information (konfidentiell information)?

(Tid) Hur ofta utförs en aktivitet med avseende på säkerhet:
17. Hur ofta

a) autentiserar du dig mot en tjänst?
b) hanterar du lösenord (i form av ändra, memorera mm)?
c) utbildas du och lär dig mer inom informationssäkerhet?
d) tar du backups?
e) utför företaget övervakning av er?
f) skyddar du viktig information (konfidentiell information)?

Belöningen med att slutföra en aktivitet med avseende på säkerhet:
18. Vad är belöningen med att

a) autentisera sig mot en tjänst?
b) hantera dina lösenord?
c) lära dig mer inom IT-säkerhet?
d) ta backups?
e) övervakas?
f) skydda viktig information (konfidentiell information)?

Avslutande frågor:
19. Fråga om motivationen till att följa en ISP, är du villig att bryta mot den?
20. Om någon skulle hacka din konfidentiella information, hur skulle du reagera (kritiskt/harmlöst)?
21. Om en kollega skulle ta del av din konfidentiella information utan ditt godkännande, hur skulle du reagera (kritiskt/harmlöst)?
22. Hos vem ligger ansvaret att ta backups?
-Hos vem bör ansvaret ligga?
23. Har ni mobila företagsenheter?
24. Hur gör du för att skydda eventuellt känslig information på dem?
25. Scenario (medvetet svagt formulerad för att hålla frågan någorlunda öppen och för att försöka få dem att svara sanningsenligt); Du får ett mejl innehållande kundinformation när du är ute på lunch som du måste vidarebefordra till en kollega. Vad gör du och varför? a) du väntar till du är tillbaka på jobb efter lunchen. b) du använder din smartphone direkt för att vidarebefordra mejlet.
26. Har du några övriga åsikter/funderingar kring IT-säkerhet? Något ni är speciellt bra på eller som du ser skulle behöva förbättras?

Bilaga 2 - Intervjuperson 1 (I1)

När; Utfört 22/4 - 2016
Var; På plats hos företaget

1. M: Vilken roll har du i företaget?
I1: Skadereglerare motor privat.
2. M: Enligt dig själv, hur god datorvana har du?
I1: God
R: Skala 1-4?
I1: När du säger 1-4, alltså är det basic?
R: Bakgrundsmässigt med hur du klarar av arbetet?
I1: Alltså, just arbetet och sådär är ju väldigt, det är inga konstigheter men bakgrunden hur program är uppbyggda eller sådana saker, det har jag ingen aning om. 3.
3. M: Hur säkerhetsmedveten är du enligt dig själv, enligt skalan 1-4?
R: Inom IT?
I1: 2.
4. M: Då är vi med, hur hanterar du dina lösenord och hur lätt/svårt anser du att det är?
I1: De byts, fyra olika system, plus windows, och de byts med jämna mellanrum. Lösenord uppdateras genom att korrigera två siffror i slutet.
M: Så då blir det autogenererat då?
I1: Nej, måste manuellt göra det. En var 45 dag eller en gång varannan månad eller liknande och ändra det.
M: Så då måste du hela tiden memorera vad ditt nya lösenord är?
I1: Ja
M: Anser du att det är lätt/svårt? Eller skriver du ner dem till exempel eller har du dem i huvudet?
I1: Jag har dem nedskrivna på min telefon, det har jag. Säkerhetsmässigt är det kanske inte det bästa egentligen, om folk vet vad det ska vara. Men såsom det är uppbyggt så är det helt omöjligt egentligen och ha allting i huvudet. Framförallt när du är tillbaka från semestern, en lite längre ledighet eller något sådant där, så nej de skrivs ned på ett säkert ställe.
M: Hur autentiserar du dig mot en tjänst och hur lätt/svårt anser du att det är?
I1: Logga in i system?
5. R: Är det användarnamn och lösenord eller är det något mer utöver det?
I1: Det är användarnamn och lösenord.
R: Det är på alla inloggningar du har?
I1: Ja, och det är inte mejladress utan där har vi en speciell identitet också ju, i form av, tror det är två bokstäver och sex siffror.
6. M: Lär du dig mer inom IT-säkerhet, då i form av utbildning? Och anser du att det är lätt eller svårt?
R: Tillhandahåller företaget några utbildningar inom IT-säkerhet eller IT överhuvudtaget?
I1: Nej.
M: Om ni måste lära er mer så får ni göra det på egen hand?
I1: Så är det på egen hand ja, allt som är i fråga ja, det finns inget så vitt jag kan komma på att vi har om säkerhet, det har vi inte.
M: Är den egna viljan att lära dig mer om IT-säkerhet i och med att företaget inte gör det?
I1: Den är nog inte speciellt stor, det skulle jag inte vilja påstå. Där är en ganska stor tillit att det är säkert.
R: Ni tar det för givet eller?
I1: Ja precis, så skulle jag vilja uttrycka mig att det är.
7. M: Och om man ser då till företaget, har företaget en tydlig IS-policy? Och isåfall, kan du den?
I1: Jag kan inte den utantill, det kan jag inte. Där finns ramar, riktlinjer och regelverk. Det finns det, nedskrivna.
M: Som ni får när ni startar här?
I1: Ja, som du får skriva under, ett avtal eller vad man ska säga, fråga inte vad det står i det bara. Det kommer jag inte ihåg. Riktlinjer som vi ska följa, vad som är tillåtet, exempelvis du får inte lämna platsen utan att låsa datorn, lite sådana sker. Och vad datorn ska användas till och sådär.
M: Så i form av ett kontrakt?
I1: Ja.
8. M: När det gäller säkerhetskopiering, hur säkerhetskopierar du?

R: Eller om du gör det överhuvudtaget?
I1: Nej.
R: Ni säkerhetskopierar inte?
I1: Nej, inte manuellt iallafall, säkerhetskopierar tror jag att, nu är jag ute på djupt vatten, men det tror jag sker på automatik.
R: Okej, vet du hur ofta det utförs isåfall?
I1: Det är, alltså om jag hade blivit av med något idag, alltså jag tror nästan, skulle chansa på en gång i dygnet. För då skulle vi kunna hämta det som var, gårdagen om det finns där, och säkerhetskopia därifrån tror jag, det tror jag nog.
9. M: okejokej, anser du att det är lätt eller svårt att den policyn som ni då skriver under, att det då är lätt att bryta mot den? I form av, som du nämnde att man ska inte lämna datorn öppen när man går ifrån? Är det lätt att glömma och bara gå därifrån?
I1: Ja det är det ju, det är ju väldigt, jag menar detta är en liten arbetsplats också, alla har stor tillit till varandra, så visst händer det att man glömmer och låsa datorn, absolut. Sen likadant när det gäller mejl och sådär också, där är också en policy på hur mycket du får använda den, alltså privat egentligen också, men det är ju ganska lätt att bryta mot det också. Men sen, det går inte att ladda ner program och liknande exempelvis på datorn, för då måste du ha lösenord och inlogg som inte vi har tillgång till, så där är det ju ganska säkert alltså så isåfall.
10. M: När det gäller just konfidentiell information? Hur skyddar du din konfidentiella information som du har på datorn och så? I form av till exempel kryptering, är det något som du gör?
I1: Nej.
M: Just den informationen om en kund, personnummer.
I1: Ja, allt det skyddas, alltså det är inget som vi, vi lämnar ju inte ut det via telefon om man säger så, till de kunderna vi pratar med eller om vi pratar med andra bolag givetvis. Alltså rent skyddsmässigt vad som finns i systemen , och vad som rensas bort, alltså personuppgiftslag och liknande, det sköts per automatik, det gör det.
M: Jag tänkte på en sak just nu, finns det möjlighet att jobba med konfidentiell information på din dator och om du exempelvis går väck från den och du glömmer låsa den? Alltså kan sådana tillfälle ske?
I1: Ja, men det är ju inte för, om vi säger specifikt information i ärendet som är hemlig, det är ju inte hemligt för mina kolleger, egentligen, för de sitter och kan läsa samma information som jag, bara de loggar in med sina i systemen.
R: Kan alla som jobbar här på kontoret, har alla tillgång till samma information som du har?
I1: Både ja och nej, det har dem, men alltså skadeavdelningen har ju tillgång till, vi jobbar i samma system, men exempelvis kundtjänst är låsta för att komma ini skadorna, det kan inte dem se, så jo, rent teoretiskt skulle de kunna se om det är känslig information om ett ärende med, exempelvis poliser inblandade, droger eller rattfylla eller liknande, personnummer och sådär, skulle de kunna se det, genom att titta på min dator, om jag glömmer att låsa den, det skulle dem göra. Samtidigt som mina kolleger på skadeavdelningen kan se det oavsett om jag låser datorn eller inte, det är bara att gå in i mitt ärende så kan de se det. Och de är öppna för alla på den avdelningen.
R: Nu kommer vi ställa två aktiviteter mot varandra, och vi vill att du ska välja vilket av dem som du tycker är viktigast när de ställs mot varandra, och du har fyra svarsalternativ, antingen så är det första absolut viktigare än det andra, eller så är det första något viktigare än det andra, och så tvärtom om du förstår det?

11a. R: Är det viktigare att kunna autentisera dig mot en tjänst än att du hanterar dina lösenord på ett rätt sätt eller korrekt sätt?
I1: Då skulle jag vilja säga att det är viktigare att hantera lösenord på korrekt sätt.
R: Kan det vara för att alla ändå kan se, alla som jobbar på kontoret kan mer eller mindre se samma information?
I1: Det kan dem göra ja.
R: Är det lite därför?
I1: Den första, när du säger då alltså att jag är jag, hur menar du där?
R: I och med du sa innan att, alla här på kontoret kan se i princip, mer eller mindre samma information, om jag förstod det rätt, är det så att du anser att det inte är lika viktigt på den här arbetsplatsen att ni just har alltså logga-in funktionen än vad det kan vara på andra arbetsplatsen ifall du hade haft tillgång till extremt känslig information, medan andra inte hade någon som helst tillgång till det?
I1: Då är det absolut viktigare att man loggar in med lösenord.
R: Ja, men här, skulle du välja då att hantera lösenord är viktigare?
I1: Ja.
R: Absolut viktigare eller något viktigare?
I1: något viktigare.
11b. R: Är det viktigare att kunna autentisera dig mot en tjänst än att lära dig mer inom IT-säkerhet? Absolut viktigare eller något viktigare?

I1: Något viktigare att kunna logga in och lära sig mer, för det är så mycket, säkerheten, så det tas för givet.
11c. R: Är det viktigare att kunna autentisera dig mot en tjänst än att ta backups?
I1: För mig är det viktigare att kunna logga in.
M: I form utav att det sköts automatiskt?
I1: Ja.
R: Absolut viktigare eller något viktigare?
I1: Absolut viktigare.
11d. R: Är det viktigare att kunna autentisera dig mot en tjänst än att företaget utför övervakning av er (i form utav de loggar, alltså kollar i loggar eller till och med utför någon annan övervakning)?
I1: Ja alltså, för min del är det viktigare att kunna logga in, det är det. Däremot så vet jag att företaget kan se allt vi gör, så ur säkerhetssynpunkt så är det ju för deras så skulle jag påstå att det är viktigare för dem, om man ser det så.
M: Men för dig?
I1: Min dagliga… så är det viktigare att jag kan logga in än att företaget kan övervaka mig.
R: Är det absolut viktigare eller något viktigare?
I1: Absolut.
11e. R: Är det viktigare att kunna autentisera dig mot en tjänst än att skydda viktig information?
I1: Kan jag inte logga in kan jag inte skydda den. Den är klurig den. För min del är det viktigare annars så kan jag inte jobba.
R: Men vi tänker scenariot att ni inte hade behövt autentisera er mot en tjänst eller alla hade haft datorer med samma åtkomst? Bara skippar tanken att ni behöver logga in, den funktionen finns inte. Är det viktigare att kunna logga in som ni gör nu eller är det mer viktigt att kunna skydda viktigt information (konfidentiell information)?
I1: Då är det absolut mer viktigt att skydda konfidentiell information.
12a. R: Är det viktigare att hantera lösenord än att lära sig mer inom IT-säkerhet?
M: Alltså att hantera lösenord på rätt sätt i form av alltså om du skriver ner dem, byter lösenord med byte av de två sista siffrorna eller då att man utbildas och lär sig mer inom IT-säkerhet?
I1: Isåfall det sistnämnda, skulle jag säga är något viktigare. För kan man det så behöver du ju inte behöva byta så mycket lösenord.
R: Är det absolut viktigare eller något viktigare?
I1: Något viktigare.
12b. R: Är det viktigare att hantera lösenord än att ta backups?
I1: Viktigare att ta backups.
R: Något viktigare eller absolut viktigare?
I1: Absolut viktigare.
12c. R: Är det viktigare att hantera lösenord än att företaget utför övervakning av er?
I1: Då är det viktigare att hantera lösenord, något viktigare.
12d. R: Är det viktigare att hantera lösenord än att skydda viktig information?
I1: Absolut viktigare att skydda konfidentiell information.
13a. R: Är det viktigare att lära sig mer inom IT-säkerhet än att ta backups?
I1: Absolut viktigare att ha backups.
13b. R: Är det viktigare att lära sig mer inom IT-säkerhet än att företaget utför övervakning av er?
I1: Då är det något viktigare att lära sig mer.
13c. R: Är det viktigare att lära sig mer inom IT-säkerhet än att skydda viktig information?
I1: Absolut viktigare att skydda viktig information.
14a. R: Är det viktigare att ta backups än att företaget utför övervakning av er?
I1: Absolut viktigare att ta backups.
14b. R: Är det viktigare att ta backups än att skydda viktig information?
I1: Absolut viktigare att ha backups.
15a. R: Är det viktigare att företaget utför övervakning av er än att skydda viktig information?
I1: Absolut viktigare att skydda viktig information.

16a. M: Hur lång tid tar det och anser du att det tar rimligt lång tid att autentisera dig mot en tjänst?
I1: Ja, det skulle jag nog vilja påstå. Sen har vi många olika system, så du måste logga in i varje… men själva inloggningen på varje system är ju inte speciellt lång egentligen. Vi måste skriva det en del två gånger och en del system en gång, alltså lösenord och användarnamn. Så den är väl rimlig.
16b. M: Hur lång tid tar det och anser du det tar rimligt lång tid att hantera lösenord (i form av ändra, memorera och i ditt fall skriva ner och så)?

I1: Ja, ändra lösenord tar ju inte mer än 20 sekunder kanske, det gör det. Hantera dem och komma ihåg dem är den svåra biten med tanke på att det är så många och att de byts vid olika tidpunkt, så där skulle jag vilja ha en ändring för jag tycker inte det är rimligt att ha behöva ha så mycket.
M: Så många lösenord eller ha lite färre?
I1: Eller så pass mycket korrigeringar eller ändringar hela tiden.
M: Just för att skriva ner och memorera dem och så?
I1: Ja.
16c M: Hur lång tid tar det och anser du det tar rimligt lång tid att lära sig mer inom informationssäkerhet?
I1: Vi lär oss inte så mycket om den så den kan jag nog inte svara på.
16d. M: Hur lång tid tar det och anser du det tar rimligt lång tid att ta backups?
I1: Det har jag ingen information alls om.
R: Det är inget som kan tänkas slöa ner era datorer ifall det skulle tas en backup kl 9 på en fredagsmorgon liksom och ni sitter framför datorn? Det är inget ni isåfall märker av?
I1: Det är ingenting som märks av, visst kan jag uppleva att systemen är lite sega emellanåt, men jag har ingen aning om vad det handlar om. Det skulle vara om man kör en backup då, så det vet jag tyvärr inget om.
16e. M: Hur lång tid tar det och anser du det tar rimligt lång tid att skydda viktig information?
I1: Beroende på vilket system det handlar om, så kan det ta lång tid och vara komplicerat. Jag har inget att jämföra med heller… jo rimligt. Om du ska skydda det, allting dokumenteras ju, så det som ska skyddas, det är egentligen att du får informera att det ska skydda och inte tillgång utåt.
M: Så det tar rimligt lång tid?
I1: Ja det gör det.

17a. R: Hur ofta loggar du in (autentisering) på en tjänst?
I1: Flertalet gånger om dagen.
R: På ett ungefär?
I1: I varje system, ett par tre gånger om dagen kanske.
R: Ni hade fyra eller fem sa du?
I1: Ja. Är du inaktiv för länge eller iväg på lunch så måste du logga in igen.
17b. R: Hur ofta hanterar du lösenord? Du sa det kanske innan om hur ofta ni behöver byta.
I1: Hur ofta det behöver bytas eller dagligen?
R: Ja, både i form av hur ofta du behöver byta och då hur ofta du måste memorera eller skriva ner nytt lösenord?
I1: Ja, det är en gång varannan månad i stort sett.
17c. R: Hur ofta utbildas du inom informationssäkerhet, men det är kanske inte så ofta då?
I1: Precis.
M: Hur länge har du jobbat här?
I1: I Februari är det två år.
M: Det har aldrig pratats om att ni ska skickas iväg på en säkerhetskurs?
I1: Nej.
17d. R: Hur ofta det tas backups? Det sa du innan, det tas en gång om dagen?
I1: Jag skulle gissa det, vi kan ju, skulle jag råkat ta bort någonting igår som jag inte vet vart det finns eller behöver tillgång till, så tror jag nog att jag skulle kunna ta, backupa, det från i förrigår exempelvis. För att kunna hitta det där. Så jag skulle nog tippa på att det är någonting sådant där ja. Det tror jag nog.
17e. R: Vet du hur ofta företaget kan tänkas övervaka er? Om de gör det regelbundet eller det är bara om något skulle dyka upp?
I1: Alltså möjligheten finns ju att övervakas hela tiden tror jag. Det måste finnas en anledning till det, så det är inte det att någon chef kan titta vad han gör för någonting. Utan där måste finnas någon anledning till att man ska titta på det.
M: De gör inte stickprov utan det ska ha hänt någonting för att de ska gå in och checka?
I1: Ja, under mina år har det aldrig skett.
17f. R: Hur ofta skyddar du viktig information?
I1: Dagligen, i form utav kontouppgifter och liknande.
R: Krypterar du själv?
I1: Skyddar ska jag inte säga, men om jag får så att jag kommer i kontakt med det, men sedan skyddar, vi lägger in det i systemen, sparar ner det i ett elektroniskt arkiv som är inbyggt i systemet om man säger så.
R: Så det gör ni själva? Att ni sparar vissa dokument då?
I1: Precis, ja, sen hur säkerheten är i systemen, det är jättesvårt att svara på.

R: Gör du det dagligen då?
I1: Ja.

18a. M: Om vi kollar lite på belöningen, eller vad ni får ut av att göra dessa tjänsterna, så är frågan vad är belöningen med att du loggar in på en tjänst och autentiserar dig att du är du så att säga?
R: Vad du anser är anledningen, varför du alltså antingen vill autentisera dig att du är du eller vad du ser i helhet varför man har funktionen att kunna logga in och logga ut?
I1: Att vi får lön för det vi gör eller för att vi ska kunna hjälpa kunderna?
R: Vad ser du är fördelen med att kunna logga in och kunna logga ut, här på arbetsplatsen?
I1: Just funktionen logga in och logga ut att det jag gör, eller just på min dator kan ingen annan nyttja. Sen kan ju folk se i systemen också men det jag får ut av det är ju att ingen annan kan ju göra något i mitt namn om jag säger så.
18b. M: Vad är belöningen med att hantera sina lösenord, såsom du gör att skriva ner så att ingen får åtkomst till det, mer än du?
I1: Jag ska inte påstå att det finns någon belöning.
18c. M: Vad är belöningen med att lära dig mer inom IT-säkerhet, är kanske en irrelevant fråga?
I1: Där finns ingen.
18d. M: Vad är belöningen med att ta backups finns ju inte heller på samma sätt, sett ur ditt perspektiv.
I1: Trygghet rent spontant.
18e. M: Vad är belöningen eller vad får man ut av företaget övervakar en, eller har möjlighet att övervaka en?
I1: Personligen tycker jag inte jag, alltså, du får givetvis ut det alla gör. Men en del tycker kanske att det är negativt att man inte vill vara övervakad, men jag får varken ut mer eller mindre av mitt dagliga arbete om jag skulle vara det eller inte vara det.
M: Så ur din synpunkt spelar det mindre roll men ur företagets så är det kanske...
I1: Ja.
18f. M: Vad är belöningen med att skydda viktig information?
I1: Där är ingen belöning i den bemärkelsen heller, men det är ju givetvis nödvändigt. Oerhört nödvändigt. Det är något som ska tas för givet.

19. R: Skulle du kunna tänka dig och isåfall har det hänt att du har brutit mot företaget informationssäkerhetspolicy?
I1: Nej det har aldrig inträffat som jag kan komma på.
M: Det står till exempel inte någonting i er policy att ni måste memorera och du väljer att skriva in det i telefonen, det står inget sådant i en policy?
I1: Nej.
20. R: Om du skulle få reda på att någon hade hackat och tagit del av din konfidentiella information, hur skulle du reagera (kritiskt/harmlöst)?
I1: Det hade jag tyckt vara obehagligt.
21. R: Om en kollega skulle ta del av din konfidentiella information utan ditt godkännande, hur skulle du reagera då (kritiskt/harmlöst)?
I1: Samma sak där, det hade jag inte tyckt varit okej.
22. R: Vi har tagit lite om det innan, att det tas backups automatiskt? Hos vem tycker du ansvaret bör ligga, på er personligen eller som det gör nu, att det tas automatiskt?
I1: Jag tycker per automatik, vi skulle inte ha en möjlighet att kunna hinna med att göra det, så jag skulle inte vilja påstå, hur lång tid det tar att göra en det vet jag inte. Men nej, det bör ligga på företaget automatiskt.
23. R: Har ni mobila företagsenheter eller jobbar ni bara härifrån?
I1: Nej, vi har bärbara datorer och har möjlighet att jobba, i stort sett varifrån som helst.
R: Bara datorer eller telefoner också?
I1: En del har telefoner också.
M: Så du har möjlighet att ta med en bärbar dator hem och göra företagssaker?
I1: Jag kan sitta hemma, hela tiden om jag vill egentligen och jobba där.
24. R: Gör du något speciellt för att skydda känslig information på den eller det är också bara där, lösenord och användarnamn?
I1: Det är samma sak där, vi har inga… man får logga in genom, jag vet inte vad det heter. Men alltså verifiera sig med lösenord och grejer.
M: Autentisera sig?
I1: Ja precis, så där i allt, vi har inga känsliga dokument eller något sådär hemma heller om vi skulle jobba med det utan allt sker via datorn.

R: Har du också en företagstelefon?
I1: Nej.
25. R: Om vi tänker oss att du hade haft det, och du var på lunch och du får ett mejl innehållande kundinformation som du måste vidarebefordra till en kollega. Vad gör du och varför? a) du väntar till du är tillbaka på jobb efter lunchen och tagit hand om det då. b) eller hade du använt din smartphone direkt på lunchen för att vidarebefordra det.
I1: Alltså, ur min kunskap, hade jag nog trott att det var samma säkerhet att skicka det direkt och vidarebefordra det som att komma till kontoret och vara på nätverket här. Det tror jag nog, så jag hade vidarebefordrat det direkt om det hade varit nödvändigt. Eller jag hade inte ens tänkt tanken, att nej jag måste göra det på kontoret för att jag är tillbaka då. Rätt eller fel, vet ej men det tror jag nog.
26. R: Har du några övriga åsikter/funderingar kring IT-säkerhet? Här på företaget, om det är någonting som du känner att ni är speciellt bra på eller som ni skulle kanske behöva förbättras på?
I1: Alltså jag är dålig inom området, så vad som skulle behöva förbättras, det är inget generellt.
R: Inget som du har upptäckt att när du gör en viss uppgift, här kanske vi skulle behöva göra såhär istället eller bli bättre på eller bli säkrare?
I1: Inget konkret jag kan komma på.
M: Just det med utbildning till exempel, att företaget inte utför några utbildningar och så? Är det någonting som du anser hade varit bra och intressant och lära sig mer om och utvecklas inom det, eller den IT-säkerheten du har nu, det är den som krävs?
I1: Det är den som krävs, men jag hade absolut lärt mig att kunna mer om det. Det hade inte skadat.
M: En sak också som jag har tänkt på innan vi avslutar, just det med policy när vi sa är det viktigare att hantera lösenord än att göra det andra så ansåg du till exempel att det var viktigare att lära sig mer inom IT-säkerhet eller något viktigare att det tas backups och så, är det just för att det med hantering av lösenord, att du vet redan att du har ett säkert lösenord och du ändrar bara de två sista. Anser du alltså att det va något viktigare eller absolut viktigare att skydda viktig information än att hantera lösenord i form utav att du redan vet att du har ett säkert lösenord?
I1: Ja då är det absolut viktigare att skydda information, viktig information. För att jag har ett lösenord som jag kommer ihåg och är enkelt, men som arbetsplatsen är så är det ingen som vet det ändå ju, så det är absolut viktigare att skydda viktig information ut gentemot kunderna för företaget.

Bilaga 3 - Intervjuperson 2 (I2)

När: Utfört 22/4 - 2016
Var: På plats hos företaget.

1. M: Vilken roll har du inom företaget?
I2: Skadereglerare motor privat.
2. M: Hur god datorvana har du enligt dig själv? 1-4?
I2: 3.
3. M: Hur säkerhetsmedveten är du enligt dig själv?
I2: Väldigt skulle jag vilja säga.
M: 1-4?
I2: På jobb tänker du, 4.
4. M: Hur hanterar du dina lösenord och hur lätt/svårt anser du att det är?
I2: Man har ju dem ofta för sig själv gömt någonstans, ibland på datorn. Men också i egna anteckningsblock som man har med sig. Eller i telefonen kan man också ha dem, de byts ju ut ganska ofta.
M: Då är det att de genereras eller att du själv byter ut dem?
I2: Jag byter själv ut dem.
M: Anser du att det är lätt att memorera, eller då i form av att du noterar de i anteckningsblock eller i datorn?
R: Skriver du ned dem oftare än att du memorerar dem?
I2: Jag skriver alltid ner dem, det gör jag. Sen kommer man ihåg dem precis innan man ska byta dem.
5. M: Hur loggar du in på en tjänst och hur lätt/svårt anser du att det är?
I2: Alltså man loggar ju alltid… allting som vi jobbar med loggar man in med lösenord. Om det är det ni tänker?
R: Användarnamn och lösenord?
I2: Ja precis
R: Där är ingenting annat?
I2: Nej, de tjänsterna som vi använder i arbetet är det bara lösenord och användarnamn.
M: Anser du att det är lätt eller svårt att autentisera dig mot en tjänst?
I2: Det är lätt.
M: Anser du det var lätt eller svårt med hantering av lösenord, då i form utav skriva, komma ihåg dem?
I2: Alltså att komma ihåg är omöjligt, det är med alla. Iallafall för mig. Jag får skriva ner dem.
M: Hur många användarnamn/lösenord har du för att komma in på diverse system här?
I2: Om man bara tittar på olika system, skulle jag gissa på fyra eller fem, men sen har vi andra tjänster runt detta som krävs i arbetet, så jag skulle kanske gissa på en 10,12,13.
R: Unika användarnamn och lösenord?
I2: Ja.
M: Det blir kanske lite knivigt att komma ihåg alla då?
I2: Det blir det.
6. M: Lär du dig mer om IT-säkerhet (utbildning)?
I2: Nej, väldigt lite utbildningar, dock så påminns det ibland från företaget att man inte ska göra si och inte göra så, tänka på detta och detta. Utbildningar, inte jättemycket men heads up iallafall.
M: Lär du dig något själv utanför företaget, för att just förbättra din IT-säkerhet?
I2: Inte aktivt.
7. M: Har företaget en tydligt uttalad ISP? Kan du den?
I2: Nej det kan jag inte, Det finns säkert en väldigt bra där man kan grunderna till de. Men tyvärr är man nog ganska dålig på att uppdatera sig själv. Jag vet att det finns nedskrivet iallafall.
8. M: När det gäller säkerhetskopiering, hur sköts det?
I2: Just på mina egna saker?
M: På det du arbetar med på dina personliga dator ja, på jobbet?
I2: Det är inget som sker aktivt.
M: Är det du som ska göra det eller står det på företaget?
I2: Vet faktiskt inte.
9. M: Anser du att det är lätt eller svårt att bryta mot denna bestämda policy?

I2: Alltså det är säkert lätt att göra det, det kan ju vara allt från att inte öppna specifika mejl när man måste vara väldigt noggrann, till exempel. Det är nog väldigt lätt. Ja.
10. M: Hur skyddar du konfidentiell information (då den viktiga informationen)?
I2: Alltså just det där vi själv kan göra skillnad, det att just se upp vart vi skickar informationen, just med mejl. Vi försöker också ta reda på vem det (alltid) är vi pratar med, innan vi skickar någonting och överlag, det är en viss sekretess i försäkringsbranschen. Så att man tar reda på vem det är man pratar med, skickar kanske till mejl som innehar den försäkringstagarens namn i sig, inte till konstiga mejladresser osv. Man får känna igen den man pratar med, eller mejlar till, till exempel.
M: Om det gäller konfidentiell information på din dator, krypterar du denna information?
I2: Nej.
M: Just det som du sade, att du skickar iväg konfidentiell information, att du kollar vem du skickar till, anser du att det är lätt eller svårt?
I2: Det är väl ganska lätt, sedan är det ju kanske, man är kanske lite för nitisk ibland. Det är väl kanske bättre på det hållet.

11a. R: Är det viktigare att kunna logga in överhuvudtaget alltså här på arbetsplatsen, att du ska kunna säga att du är du, att respektive anställd är dem, eller att du hanterar dina lösenord i form av att du måste ändra det en gång i månaden eller komma ihåg dem, vilket är viktigast?
I2: Ursäkta, men jag tror inte riktigt att jag förstår skillnaden. Att jag är jag? Alltså menar du mot mina kolleger då eller?
R: Nej alltså när du ska logga in, ifall du tänker dig att ni inte hade haft funktionen att logga in. Vad är viktigast, att kunna logga in eller att hantera lösenord?
I2: Hantera lösenord.
R: Absolut eller något viktigare?
I2: Absolut.
11b. R: Är det viktigare att kunna autentisera dig mot en tjänst än att lära sig mer om IT-säkerhet?
I2: Lära sig mer om IT-säkerhet är viktigare.
R: Något viktigare eller absolut viktigare?
I2: Det är absolut viktigare.
11c. R: Är det viktigare att kunna autentisera dig än att ta backups?
I2: Ta backups är viktigare.
R: Något viktigare eller absolut viktigare?
I2: Absolut viktigare.
11d. R: Är det viktigare att kunna autentisera dig än att företaget utför övervakning av er?
I2: Bättre att företaget övervakar.
R: Något eller absolut?
I2: Absolut.
11e. R: Är det viktigare att kunna autentisera dig än att skydda viktig information?
I2: Mycket viktigare att skydda viktig information.
12a. R: Är det viktigare att hantera lösenord än att lära sig mer om IT-säkerhet?
I2: Hantera lösenord skulle jag vilja säga löser mycket, så absolut.
R: Absolut viktigare?
I2: Ja.
12b. R: Är det viktigare att hantera lösenord än att ta backups?
I2: Jag tycker inte egentligen att dem går att jämföra riktigt. Jag tycker det är viktigare med lösenord.
12c. R: Är det viktigare att hantera lösenord än att företaget utför övervakning av er?
I2: Det är nästan likställt, allting handlar ju om att det ska gå rätt till, att man inte ska kunna. Jag säger lösenord, för då är det bara jag som kan komma in.
R: Något viktigare?
I2: Det är något viktigare.
12d. R: Är det viktigare att hantera lösenord än att skydda viktig information?
I2: Där skulle jag säga något viktigare att skydda viktig information.
13a. R: Är det viktigare för dig att lära dig mer inom IT-säkerhet än att ta backups?
I2: Det är något viktigare för mig att lära mig mer om IT-säkerhet.
13b. R: Är det viktigare att lära dig mer inom IT-säkerhet än att företaget utför övervakning av er?
I2: Något viktigare att jag lär mig mer, faktiskt, om IT-säkerhet.

13c. R: Är det viktigare att lära sig mer inom IT-säkerhet än att skydda viktig information.
I2: Det är viktigare att skydda viktig information.
R: Absolut viktigare?
I2: Absolut.
14a. R: Är det viktigare att ta backups än att företaget utför övervakning av er?
I2: Det är något viktigare att företaget övervakar.
14b. R: Är det viktigare att ta backups än att skydda viktig information?
I2: Egentligen samma sak, på ett vis. Men något viktigare att skydda viktig information.
M: När du sa, att det är något viktigare att företaget utför övervakning av er än att ta backups, är det just för att backups görs automatiskt, att det inte ligger hos dig så att säga?
I2: Det är lite min tanke där, att jag tycker om när förtaget sköter sådana delar automatiskt, om man säger så. Men sen samtidigt så vet man också det viktiga med det, men ja, jag gillar när företaget har koll på vad som händer, så man själv kan liksom lite släppa det.
M: Det finns någon trygghet hos dig också i det?
I1: Ja precis.
15a. R: Är det viktigare att företaget utför övervakning av er än att skydda viktig information?
I2: Det är viktigare att skydda viktig information?
R. Absolut eller något?
I2: Absolut.

16a. M: Hur lång tid tar det och anser du det tar rimligt lång tid att autentisera dig mot en tjänst?
I2: Om man ser till en tjänst, så är det rimligt. Men när vi tänker på att vi har kanske 10 olika, så är det lång tid om man räknar ihop dem.
M: Så det blir lite för mycket inlogg?
I2: Ja, men sedan samtidigt så förstår man nyttan med det. Men självklart, det tar en hel del tid.
16b. M: Hur lång tid tar det och anser du det tar rimligt lång tid att hantera lösenord (i form av allting med att ändra, memorera, skriva ner)?
R: Du nämnde det kanske lite tidigare också att du lär dig dem precis innan du ska byta?
I2: Det är rimligt i den mån att man förstår allvaret med det och nytta, dock så kan det alltid göras bättre.
16c. M: Hur lång tid tar det och anser du det tar rimligt lång tid att lära sig mer om informationssäkerhet?
I2: Det är som sagt ingenting som görs aktivt, ingenting som finns på ens schema. Och då det är ett ganska hektiskt jobb så har man väldigt lite tid till att göra det själv. Så att det tar säkert inte så lång tid men det läggs inte tid på det.
16d. M: Hur lång tid tar det och anser du det tar rimligt lång tid att ta backups (nu gör du det inte själv så att säga).
R: Du vet inte heller hur ofta det görs?
I2: Har inte en aning.
R: Och du har inte märkt av att det skulle slöa ner datorerna?
I2: Jag kan inte sätta det i samband med det. Tyvärr.
16e. M: Hur lång tid tar det och anser du det tar rimligt lång tid att skydda viktig information?
I2: Det är väl rimligt, som sagt så märker vi inte så supermycket av det heller, vi gör vad vi kan för att inte skicka ut fel information och känslig information. Men sedan hur det skyddas, det är ju säkert tusen brandväggar och sådant där som intrång till exempel. Jag kan gissa att företaget lägger väldigt mycket tid på det, men det är bara en gissning.

17a. R: Hur ofta loggar du in på en tjänst under en dag, alltså på ett program eller applikation. Hur ofta skulle du säga att du behöver autentisera dig mot en tjänst under en dag?
I2: Vissa system loggas man ut automatiskt, vilket innebär att på ett system kan det vara att man loggar in tio gånger om dagen. Så att jag skulle gissa på i olika system, sammanlagt tjugo gånger per dag.
17b. R: Hur ofta hanterar du lösenord?
I2: Dagligen.
R: Hur ofta behöver du ändra lösenord?
I2: Också lite olika, men det kan vara allt från, Säg tio system och kanske fem av dem måste ändras en gång i månaden. Någonting sådant.
17c. R: Utbildning har ni inte så mycket om heller om, eller ingenting.
I2: Gällande säkerhet, nej tyvärr.
R: Du kan inte svara på den direkt?
I2: Nej.
17d. R: Inte heller på backups?

I2: Nej, tyvärr.
17e. R: Du vet inte hur ofta företaget utför övervakning av er?
I2: Jag tror det är dagligen. Och likadant, det finns säkert ett system som gör att, aktiverar någon tjänst när man går in på något speciellt, skriver något speciellt som flaggas skulle jag gissa på, så det är säkert stenhårt.
17f. R: Hur ofta skyddar du viktig information?
I2: Dagligen.
R: Är det på något speciellt sätt, att du lägger vissa filer i speciella mappar, eller du krypterar själv?
I2: Vi har ju speciella personer som sysslar just till exempel med skyddad identitet. De får all den bördan.
R: Så det sköts mer eller mindre automatiskt då? Beroende på vilket fall det är eller så?
I2: Det kan man säga. Sen gör vi allt för att, ja samma där, inte skicka känslig information. Skicka så lite som möjligt, när vi gör det så är det till rätt person.
M: Vara skeptiskt då?
I2: Ja, uppmärksam.

18a. M: vad är belöningen med att kunna autentisera dig mot en tjänst?
I2: Då kan man veta att det bara är jag som har varit där, ingen kan göra något på min dator. Jag kan inte få skuld för någon annans misstag.
18b. M: Vad är belöningen med att hantera dina lösenord?
I2: Egentligen samma där, det är bara jag som ska ha tillgång till dem. Jag vet att det som står är gjort är det jag som gjort det.
18c. M: Vad är belöningen med att lära dig mer inom IT-säkerhet (blir tuff kanske)?
18d. M: Vad är belöningen med att ta backups, finns kanske inte heller så mycket att säga?
R: Vi säger att det tas backups automatiskt en gång om dagen, vad ser du belöningen med det?
I2: Det är en viss säkerhet och trygghet för företaget, även för mig och för mina saker som jag sparat isåfall. Skulle allting krascha så kan vi ändå återgå till förra dagens uppgifter. Det säger sig själv.
18e. M: Vad är belöningen med att företaget utför övervakning av er?
I2: Det är också en säkert… det största hotet idag är väl just med IT-övertramp om man säger så. Det är ju våra jobb det handlar om, kanske personer som har en viss sekretess som vars personuppgifter inte ska exponeras och dylikt, och det är jätteviktigt. Belöningen är att det kan vara tryggt att jobba.
18f. M: Vad är belöningen med att skydda viktig information?
I2: Det är samma där, man har en viss skyldighet mot sin kunder, och de uppgifter man hanterar och företaget i sig. Övervakas det så är det bra och tryggt.

19. R: Du sa innan att du inte kunde företaget IS-policy helt och hållet, men hade du kunnat tänka dig att bryta mot den (behöver vi inte prata om rejäla övertramp utan sådana saker som kanske glömma logga ut eller strunta i att logga ut och sådana grejor)? har det hänt?
I2: Det har säker hänt, det kan ha varit att man har lämnat sin dator utan att stänga ner den, till exempel, vilket inte är så bra. Men absolut, det har hänt, men inte medvetet.
20. R: Om någon utomstående hade hackat din konfidentiella information, hur skulle du reagera (kritiskt/harmlöst)? Hur skulle du känna?
I2: Känslan hade nog mest varit om man själv hade gjort någonting som underlättade, så att man själv har någon del i det, men sedan självklart bara tagit kontakt med någon som är ansvarig så snabbt som möjligt. Ibland kan man inte skydda sig mot sådant, ibland kan de göra det ändå.
21. R: Om en kollega skulle ta del av din konfidentiella information, hur skulle du reagera (kritiskt/harmlöst)?
I2: Beror på om det fanns någon relevans i det, men att bara ta reda på det av någon anledning som han inte kan förklara, då är det något suspekt skulle jag vilja säga.
22. R: Vi antar att backups tas automatiskt, och tycker du att det ska vara så eller tycker du att det ska ligga på den enskildes ansvar att ta backups när man känner att det behövs eller ska det vara såsom det är att företaget utför?
I2: Den mänskliga faktorn finns alltid, vilket gör att det alltid någon gång kommer att missas. Så jag tycker att det ska ligga på högre ort. Det ska finnas ett ansvar högre upp.
23. R: Har ni mobila företagsenheter? laptops, telefoner?
I2: Ja vi kan ju ta och jobba hemma om vi vill, absolut.
R: Du har det också?
I2: Ja.
24. R: Gör du något speciellt för att skydda känslig information på dem eller det är användarnamn och lösenord?

I2: Det är så att vi kan ju jobba hemma om vi vill, men jag gör inte det. På grund av att jag troligtvis kan lite för lite om det, när man kopplar upp sig på sitt wifi med den här datorn då. Jag jobbar bara på jobb.
25. R: Kanske lite svar på förra frågan, men vi kör den ändå: Vi tänker att du är ute på lunch och du har en företagsmobil som är kopplar till din jobbmejl, du får ett mejl innehållande kundinformation och du måste vidarebefordra det till en kollega. Vad gör du och varför? du väntar till du är tillbaka på jobb efter lunchen eller vidarebefordrar du det direkt via telefonen?
I2: Det är svårt att säga, vi jobbar ju inte direkt på det viset.
R: Mer bara ett scenario, ifall det skulle vara så?
I2: Alltså, hade man inte tänkt sig för hade jag säkert vidarebefordrat det, det hade jag säkert gjort. Man vill ju göra saker snabbt. Så troligtvis om jag inte hade tänkt mig för.
26. R: Har du några övriga åsikter/funderingar kring IT-säkerhet? Här på företaget, om det är något som du känner att ni är bra på eller någonting som ni kanske skulle behöva förbättras på?
I2: Inte på rak arm, det är som sagt lite mer information som ni nu har belyst att vi faktiskt inte har eller jag personligen inte har så stor koll på. Policy till exempel. Och likadant, vilket innebär att man kanske förmodar då att företaget gör backuper automatiskt eftersom vi inte har hört någonting om det, får man ju hoppas att de gör det. Men det är kanske också något som man borde ta reda på.
M: Utbildning och så, anser du att företaget skulle vara lite mer och kunna hjälpa er i form av utbildning här på jobb och så. För att lära sig mer inom det och kunna utvecklas?
I2: Ja, absolut. Det finns vissa riktlinjer som man ska följa när man sköter sitt jobb. Dock så är de väldigt grundläggande, och som sagt, finns det någon ytterligare säkerhetspolicy så är den inte lätt att få tag i eller lätt att hitta. Så absolut, en utbildning kanske en gång i månaden eller en gång varje halvår med nya saker som man hade kommit på.
M: Ja precis, och att fräscha upp och fortsätta hålla säkerheten vid god?
I2: Ja.

Bilaga 4 - Intervjuperson 3 (I3)

När; Utfört 22/4 - 2016
Var; På plats hos företaget

1. M: Vilken roll har du inom företaget?
I3: Skadereglerare motor privat.
2. M: Hur god datorvana har du mellan 1-4?
I3: 3.
3. M: Hur säkerhetsmedveten är du enligt dig själv mellan 1-4?
I3: 4.
4. M: Hur hanterar du dina lösenord och hur lätt eller svårt är det?
I3: Jag hanterar dem i huvudet. Men när jag vet att jag ska vara ledig länge så brukar jag skriva ner dem i telefonen. Så jag har dem i säkert förvar. Den är ju lösenordsskyddad också.
M: Väljer ni dem (lösenorden) själv eller blir dem genererade till er?
I3: Dem väljer vi själva. Med kriterier på hur långa de ska vara och hur många siffror och asterix osv. Beroende på vilket system det är.
M: Anser du att det är lätt att memorera dem (lösenorden)?
I3: Ja det tycker jag. Jag tycker nog att jag har ett system som jag hänger upp mina lösenord på.
5. M: Hur autentiserar du dig mot du en tjänst?
I3: Med lösenord och användarnamn.
R: Inget utöver lösenord och användarnamn?
I3: Nej. Både användarnamn och lösenord på allt.
M: Hur många olika användarnamn och lösenord har du till de olika systemen?
I3: Jag har nog, huvudsystemet är ett. Tre huvudsystem och sen har vi bisystem som kanske är tre till fyra stycken. Några av dem är lösenord för företaget alltså licenser så det är ju inget säkerhets???. Man måste gå in i datorn för att kunna spara så det är sparat i datorn.
M: Är det lätt eller svårt att autentisera sig mot en tjänst(applikation)?
I3: Ja det tycker jag absolut (lätt).
6. M: Lär du dig mer om IT-säkerhet?
I3: Ingen aktiv utbildning så. Vi får lite information när det har varit hackerangrepp med spammejl och sådana saker hur vi ska hantera det. Men ingen aktiv utbildning.
M: Lär du dig själv på fritiden, är du intresserad av det?
I3: På IT-nivå just nu är jag nog inte jätteintresserad. Det går lite i vågor. Det är väl personliga saker som gör att man lägger tid på annat istället.
7. M: Har företaget en tydligt uttalad ISP? Och kan du den i så fall?
I3: Dem har en tydlig som finns på intranätet. Jag ska inte säga att jag kan den utantill. Jag har läst igenom den och skummat igenom den. Framförallt när man börjar anställningen så får man ju bibbar med information. Den känns ju som att den är, när man har jobbat på något mer försäkringsbolag så är den likgiltig och då skummar man tyvärr igenom den.
8. M: Hur sköts säkerhetskopiering?
I3: Vad tänker ni med kopiering?
R: Backups. Gör ni det själva eller sköts det automatiskt?
I3: Det ligger på en server. Så fort man är inne i ett skadesystem så sparas ju det automatiskt. När det gäller brev och information till kunden så blir det låst som en pdf när du har gjort det färdigt. Så det blir ju en form av backup på det. Annars gör jag väl inga aktiva backups på något annat sätt. Vi litar nog mest på systemen, eller allt ska ju ligga i ett skadesystem och det ska ju vara slutet egentligen. Trots att vi har det uppdelat i olika kringsystem så ska det ligga säkert där.
M: Anser du att det är lätt eller svårt att göra det?
I3. Att spara är lätt men det är kanske inte det mest användarvänliga systemet annars. Men själva sparningen är inga problem.
9. M: Anser du att det är lätt eller svårt att bryta mot denna bestämda policy (ISP)? T.ex. om du ska byta lösenord en gång om dagen men du gör det istället en gång i månaden.
I3: Nej sådana saker går inte att bryta emot för det kommer påminnelser.

R: Och det måste du göra då (direkt)?
I3: Ja, det kommer påminnelser en vecka innan "nu går det ut om sju dagar". Så då måste man ändra. Några av systemen är så att du inte kan ha samma lösenord som innan eller du kan inte bara byta ut en siffra t.ex. utan du måste byta ut hela ord osv.
10. M: Hur skyddar du viktig (konfidentiell) information?
I3: Den ligger ju i systemen och det är ju bara vi på skadeavdelningen som behörighet till våra dokument. Dem som sitter på kundtjänst kan inte gå in på våra dokument. Gäller det utskrifter och sånt så är det ju säker hantering när man ska slänga konfidentiell information.
M: Men du krypterar inte viss information?
I3: Nej. Jag vet att om man vill ha usb-minnen så måste man kryptera dem för att kunna komma in i våra datorer. Men det är inget som jag krypterar aktivt. Jag vet inte om våra mejl är krypterade.
M: Är det lätt eller svårt att skydda konfidentiell information?
I3: Jag gör ju inget aktivt mer än att låsa min dator när jag går ifrån den. Det är det jag gör. Jag gör inget aktivt för att kryptera eller så.

11a. R: Är det viktigare att kunna autentisera sig (logga in och visa att du är du) eller är det viktigare att du hanterar dina lösenord?
I3: Användarnamnet kan man ju oftast spara men lösenordet är bättre att ha själv så att ingen annan går in i min dator.
R: Är det viktigare att hantera lösenord då?
I3: Det är något viktigare att hantera lösenord.
11b. R: Är det viktigare att kunna autentisera sig eller är det viktigare att du lär dig mer om IT-säkerhet?
I3: Det är viktigare att logga in för att det ska kunna fungera för alla. Dock personligen skulle jag vilja ha mer kunskap och vidga vyerna på det. Det är absolut viktigare att kunna logga in. Jag tänker rent generellt för hur en verksamhet ska kunna fungera.
11c. R: Är det viktigare att kunna autentisera sig eller är det viktigare att ta backups?
I3: Eftersom vi inte jobbar med backups aktivt så säger jag att det är viktigare att kunna logga in.
R: Vad hade du helst valt, antingen att kunna autentisera sig eller att kunna ta backups?
I3: Att kunna logga in är absolut viktigare.
11d. R: Är det viktigare att kunna autentisera sig eller är det viktigare att företaget utför övervakning av er? Att dem granskar loggar eller att de kanske till och med besöker arbetsplatsen.
I3: Alltså det är väl ett storebrorsamhälle på något sätt så jag förutsätter att om dem skulle behöva gå tillbaka och kolla loggar så gör dem det. Så då är det viktigare att man kan logga in och utföra sitt arbete. Det är absolut viktigare att kunna logga in.
11e. R: Är det viktigare att kunna autentisera sig eller är det viktigare att kunna skydda viktig (konfidentiell) information?
I3: Det är absolut viktigare att kunna logga in med tanke på att det är företagets information jag sparar.
M: Om vi går tillbaka för ett litet förtydligande, är det viktigare att kunna autentisera sig eller att ta backups?
I3: Jag tycker det är viktigare med att kunna logga in i så fall än att det blir backups på det. För det är inte privat egendom som vi har. Den ska kunna spåras om det blir någon utredning från finansinspektionen eller något liknande så är det ju företagets grejor.
12a. R: Är det viktigare att hantera lösenord eller är det viktigare att du lär dig mer inom IT-säkerhet?
I3: Jag tror inte man kommer ifrån lösenord, så det är nog det som är viktigare. Det är absolut viktigare med att hantera lösenord.
12b. R: Är det viktigare att hantera lösenord eller är det viktigare att ta backups?
I3: Det är viktigare att hantera lösenord. Absolut viktigare.
12c. R: Är det viktigare att hantera lösenord eller är det viktigare att företaget utför övervakning av er?
I3: Att hantera lösenord är absolut viktigare.
12d. R: Är det viktigare att hantera lösenord eller är det viktigare att skydda viktig information?
I3: Det är absolut viktigare att hantera lösenord.
13a. R: Är det viktigare för dig att lära dig mer inom IT-säkerhet eller är det viktigare att ta backups?
I3: Nej det är absolut viktigare att ta backups.
13b. R: Är det viktigare att lära dig mer inom IT-säkerhet eller är det viktigare att företaget utför övervakning av er?
I3: Det är absolut viktigare att företaget utför övervakning av oss i slutändan.
13c. R: Är det viktigare att du lär dig mer inom IT-säkerhet eller är det viktigare att kunna skydda viktig information?
I3: Det är absolut viktigare att kunna skydda viktig (konfidentiell) information.
14a. R: Är det viktigare att kunna ta backups eller är det viktigare att företaget utför övervakning av er?

I3: Det är absolut viktigare att kunna ta backups.
14b. R: Är det viktigare att kunna ta backups eller är det viktigare att kunna skydda viktig (konfidentiell) information?
I3: Det är viktigare att skydda den viktiga (konfidentiella) informationen. För det kan komma till fel händer. Det är absolut viktigare att skydda den viktiga (konfidentiella) informationen.
15a. R: Är det viktigare att företaget utför övervakning av er eller är det viktigare att kunna skydda viktig (konfidentiell) information?
I3: Absolut viktigare att kunna skydda viktig (konfidentiell) information.

16a. M: Hur lång tid tar det och anser du att det tar rimligt lång tid att autentisera dig mot en tjänst (applikation)?
I3: Det tar rimligt lång tid. Man lär sig sina lösenord rätt snabbt och det blir som ett muskelminne nästan. Det tar 5-10 sekunder.
16b. M: Hur lång tid tar det och anser du att det tar rimligt lång tid att hantera dina lösenord?
I3: Jag skulle nog säga att det tar rimligt lång tid. Alla system har olika intervaller, vissa ska man byta oftare (lösenord) och vissa är det längre tidspann på. Det är okej.
16c. M: Hur lång tid tar det och anser du att det tar rimligt lång tid att lära dig mer inom informationssäkerhet? Nu är det inget som sker aktivt (på företaget).
I3: Nej det tar väl lång tid eftersom man inte gör det i vardagen och man inte hinner prioritera det. Företaget lägger inte den fokusen eller utbildning (till oss).
16d. M: Hur lång tid tar det och anser du att det tar rimligt lång tid att ta backups? Nu sköts det också automatiskt.
I3: Nej men det är rimligt tycker jag. Det fungerar ju.
R: Ni märker inte av att det slöar ner (påverkar) era datorer?
I3: Nej inte just med sparningen eller backups.
16e M: Hur lång tid tar det och anser du att det tar rimligt lång tid att skydda viktig (konfidentiell) information?
I3: Svårt att svara på den. Men det är väl rimligt (lång tid). Det är ju egentligen bara att låsa datorn så ingen annan kan gå in o se det (den konfidentiella informationen). Som jag sa innan så har vi ett visst skydd på det sättet att det bara är en viss avdelning eller vissa personer som har behörighet till vissa saker. Så även om det är hundra personer här så skulle inte de kunna gå in i våra dokument. Då måste dem gå in från min dator eller en kollegas dator. Så det är såna som ni som kommer och kan sätta fingret på det om jag inte har låst min dator.

17a. R: Hur ofta skulle du säga att du autentiserar dig mot ett program/applikation under en dag totalt sett?
I3: Alltså vi har fyra huvudsystem som man måste logga in i varje dag varav ett loggas ut om du är inaktiv. Med tanke på varje inloggning så kanske man ligger på ca tio inloggningar totalt (per dag).
17b. R: Hur ofta hanterar du dina lösenord? Hur ofta behöver du byta dem och i så fall memorera nya?
I3: Jag tror det är ett system som kräver byte av lösenord var sjätte månad. Nästa är var tredje månad och inloggningen på server är nog en gång i månaden eller varannan månad.
17c. R: Ni hade inte några utbildningar i informationssäkerhet?
I3: Nej inte mer än information.
R: Information som ni får på mejl då eller?
I3: På intranätet.
R: Hur ofta på ett ungefär skulle du säga att ni får ett sånt?
I3: Det är nog mest när det är aktuellt, när det dyker upp spammejl. Det är väl ett par gånger om året.
17d. R: Har du någon aning om hur ofta det tas backups (automatiskt)?
I3: Nej.
17e. R: Har du någon aning om hur ofta företaget kan tänkas utföra övervakning av er?
I3: När det gäller besök av arbetsplatsen vet jag om att de inte har gjort. Att de gör stickprov eller kollar på oss (loggar) är jag övertygad om att de gör. Men jag har ingen aning om hur ofta.
M: Men du tror att de gör stickprov (i förebyggande syften) istället för att de granskar när det väl har hänt något?
I3: Det kan nog vara både och. Jag kan tänka mej att en varningssignal från en chef eller stickprov bara för att kolla verksamheten eller om man kollar detaljerat mot en viss målgrupp kan jag tänka mig att de gör. Jag har dock ingen aning om det och ingen kontakt med dem.
17f. R: Hur ofta skulle du säga att du skyddar viktig konfidentiell information?
I3: Om jag ska relatera det till kryptering så har jag inte gjort det.
R: Har ni specifika mappar som vissa filer ska ligga i om det är mer känslig information?
I3: Nej det sparas automatiskt på den skadan det gäller till den kunden det gäller.

R: Ni har inte specifika mappar som ska vara säkrare än andra?
I3: Jo det finns ju t.ex. personer med skyddad identitet. Då är det bara vissa som har behörighet. Så det finns ju begränsningar men det är inte så att man lägger dem aktivt. Är du behörig på den avdelningen så kommer du in de dokumenten.
R: Med andra ord så skyddar du inte direkt aktivt (vissa filer)?
I3: Nej eftersom det inte är min information så kan jag ju inte göra det. Utan det är företagets information. Skulle jag sluta så är kunden fortfarande kund hos oss.

18a. M: Vad är belöningen med att kunna autentisera sig mot en tjänst? Vad ser du är belöningen med att du kan autentisera dig?
I3: Alltså jag kommer in på vissa saker som vissa kollegor inte gör kanske. Det är väl den belöningen jag kan se i så fall.
18b. M: Vad är belöningen med att hantera lösenord?
I3: Ingen. Det är ett krav skulle jag vilja säga.
18c. M: Vad är belöningen med att lära dig mer inom IT-säkerhet?
I3: Belöningen hade jag sett hade varit att man får en större förståelse och bakgrundsinformation. Det är alltid roligt att veta hur saker och ting fungerar.
18d. M: Vad är belöningen med att ta backups?
I3: Säkerhet eller trygghet för mig som anställd att jag vet att jag kan komma åt det.
18e. M: Vad är belöningen med att övervakas?
I3: Belöningen kan vara att rättfärdiga att jag gör rätt. Har jag inte rent mjöl i påsen så blir jag ju upptäckt förhoppningsvis. Ett svar på att man gör rätt.
18f. M: Vad är belöningen med att skydda viktig (konfidentiell) information?
I3: Belöningen, är ju att det är ett krav för företagets säkerhet. Mot kunder och osv.

19. R: Skulle du kunna tänka dig eller vara villig att bryta mot den? Behöver inte vara rejäla övertramp utan det kan handla om att göra något för att tjäna tid. T.ex. att inte logga ut när du ska hämta en kopp kaffe.
I3: Det händer ju absolut. Det gör man ju varje dag tyvärr. Men man försöker att inte göra det. Framförallt om man ska till skrivaren som ligger tio meter bort så är det ju inte alltid jag loggar ut och kanske inte heller alltid när jag ska hämta en kopp kaffe. Man vill ju ändå lita på sina kollegor som sitter precis jämte. Men jag är nog en av dem, jag tycker jag försöker göra mer (vara mer säkerhetsmedveten) än genomsnittet skulle jag säga.
20. R: Om du hade fått reda på att någon utomstående hade hackat din konfidentiella information. Hur hade du reagerat?
I3: Jag har knappt någon personlig information på min dator. Jag skulle inte känna det så personligt.
R: Det skulle inte vara alltför kritiskt med andra ord?
I3: Nej. Jo jag skulle tycka att det skulle vara kritiskt för företaget. Men det är ingen personlig information som jag skulle känna mig kränkt över. Däremot är det en säkerhetsrisk för företaget och för våra kunder.
21. R: Om en kollega skulle ta del av din konfidentiella information utan din vetskap och du sedan hade fått reda på det. Hur hade du reagerat då?
I3: Det beror lite på vilken kollega det är. Vilken relation man har till kollegan.
R: Om vi säger att det är någon som inte har tillgång (behörighet) till den informationen som du har.
I3: Det skulle jag inte tycka vara särskilt bra. Sen skulle jag kanske mer känna att det inte rör sig om direkt IT-säkerhet utan mer att mitt förtroende för den kollegan skulle sjunka ordentligt.
22. R: Era backups tas automatiskt. Tycker du att ansvaret bör ligga där eller tycker du att ansvaret borde ligga hos individen (varje anställd).
I3: Nej det ska inte ligga på individen, utan på företaget. Eftersom det är så mycket information som måste sparas i varje skada så hade det varit omöjligt.
23. R: Har du en mobil företagsenhet?
I3: Du menar att jag kan använda datorn på andra ställen?
R: Om du har en företagsdator eller företagstelefon?
I3: När vi jobbar med laptops så kan jag logga in var (varifrån) jag vill.
24. R: Gör du nått mer än att logga in och logga ut för att skydda informationen (konfidentiell) på den?
I3: Nej det gör jag inte. Det är en app i telefonen som man legitimerar sig emot. Ungefär som bankid. Jag sätter inte mig på en offentlig yta på en kafé kanske och slänger upp en skada, det gör jag inte. Utan det är (i) ett slutet område i så fall.
25. R: Vi tänker oss ett scenario att du är på lunch och du får ett mejl innehållande kundinformation som du måste vidarebefordra till en kollega. Vad gör du? Väntar du till att du är tillbaka på jobb och vidarebefordrar det därifrån eller tar du upp din telefon och vidarebefordrar det direkt?

I3: Jag har inte jobbmejl i telefonen men jag hade väntat tills jag hade kommit tillbaka till jobbet om det var känslig information. Jag hade åtminstone väntat tills jag inte befunnit mig i en offentlig miljö.
M: Det spelar ingen roll om du hade gjort det bara för att du hade tjänat tid på att göra det direkt, utan du hade hellre väntat och låtit det ta längre tid och gjort det säkert ifrån kontoret?
I3: Ja om det finns risk med känslig information att någon annan skulle se det så skulle jag i alla fall gått undan eller (på annat) sätt sett till så att det var säkert. Sen vet jag inte om ni är inne på säkerheten när det gäller nätet (wifi).
R: Det är vi bland annat.
I3. Eftersom att jag inte har den jobbpositionen att jag är ute på fält på det sättet så tänker jag inte riktigt i dem banorna. Men telefonerna är väl hyfsat krypterade.
26. R: Har du några övriga funderingar eller åsikter kring IT-säkerheten här på företaget? Är det något ni är speciellt bra på eller något som du märkt att ni behöver bli bättre på?
I3: Jag tror att när det gäller inlogg och sådana saker så tror jag att det är rätt säkert.
R: Det är inget (specifikt) som du har stött på när du jobbat och tänkt att detta är speciellt bra eller detta borde göras bättre (säkrare)?
I3: Alltså jag tror att dem flesta som jobbar på ett försäkringsbolag är rätt medvetna om personuppgiftslagen osv. Så man är rätt mån om att hålla reda på saker och ting. Att inte slänga papper på skrivbordet med känslig information osv. Jag tror att det är rätt okej faktiskt. Ni pratade om studier i USA (i vår inledning till intervjun), jag vet inte om privatkunder har samma förtroende. Men det har nog inte varit några stora skandaler i Sverige vad jag vet i alla fall. Det var en för något år sedan när hon (en försäkringsförmedlare på ett annat försäkringsbolag) trodde att kunden hade lagt på när hon säger "din tjocka jävla kossa" (om kunden) eller något liknande. Det är en annan typ av fråga, telefonihantering. Men gällande datadokument och papper så anser jag att vi har bra koll på det.
R: Men du känner dig nöjd med det tekniska (på arbetsplatsen)?
I3: Rent tekniskt på de sakerna så absolut. Sen skulle det kanske vara mer användarvänlighet (i systemen) och kanske lite bättre hastighet och mindre väntetid. Men säkerheten tror jag känns helt okej.
M: Anser du att du hade velat ha utbildningar i IT- säkerhet som företaget hade stått för?
I3: Personligen hade jag jättegärna velat ha mer IT-kunskap. Jag tror inte företaget hade kunnat lägga ut det på hela massan (all personal). Det är för många som inte har något intresse och då kostar det bara pengar. Men informationsträffar om t.ex. vikten av att skydda ditt lösenord och den typen av säkerhet tycker jag absolut att de skulle lägga mer tid på. Framförallt kanske ännu mer när du är ny. Man får högar med papper att läsa igenom osv. men vad det innebär och hur du ska tänka hade jag nog tyckt skulle vara bra.

Bilaga 5 - Intervjuperson 4 (I4)

När: Utfört 22/4 - 2016
Var: På plats hos företaget.

1. M: Vilken roll har du inom företaget?
I4: Skadereglerare motor privat.
2. M: Hur god datorvana har du enligt dig själv? 1-4?
I4: 3.
3. M: Hur säkerhetsmedveten är du enligt dig själv? 1-4?
I4: 3.
4. M: Hur hanterar du dina lösenord och hur lätt eller svårt anser du att det är?
I4: Jag håller dem i huvudet. När det blir för många så måste jag skriva ner dem.
M: Får ni era lösenord genererade till er eller får ni välja dom själva?
I4: Vi väljer själva.
M: Hur lätt är det att memorera dina lösenord?
I4: Hyfsat, försöker bara ändra ett tecken åt gången så att det är lättare att komma ihåg.
M: Brukar du skriva ner dina lösenord? Hur?
I4: Försöker undvika det men ibland behövs det.
5. M: Hur autentiserar du dig mot en tjänst och hur lätt/svårt anser du att det är?
I4: Med användarnamn och kod. Vi har fler olika system så det är lite omständigt för det är olika användarnamn och koder i alla system.
M: Något utöver användarnamn och lösenord?
I4: Nej.
M: Hur många användarnamn/lösenord har du?
I4: Drygt 5 st.
6. M: Lär du dig mer om IT-säkerhet (utbildning) och anser du att det är lätt/svårt?
I4: Nej, jag lär mig inte mer.
7. M: Har företaget en tydligt uttalad ISP?/ Kan du den?
I4: Vi har det säkert men jag kan den inte.
8. M: Hur säkerhetskopierar du information? Är det lätt/svårt?
I4: Jag utgår från att arbetsgivaren säkerhetskopierar.
9. M: Anser du att det är lätt eller svårt att bryta mot er bestämda policy?
I4: Svårt. Jag följer de direktiv som finns.
10. M: Hur skyddar du viktig information (konfidentiell information) anser du att det är lätt/ svårt?
-T.ex. kryptering?
I4: Vi gör inget vad jag vet för att skydda det men antar att företaget har brandväggar mm.

11a. R: Är det viktigare att kunna autentisera sig (logga in och visa att du är du) eller är det viktigare att du hanterar dina lösenord?
I4: Det är viktigare att jag är jag (autentisering). Det första alternativet. För det blir så pass stora följder om någon annan utger sig för att vara mig och betalar ut pengar i skador som är felaktigt i mitt namn och då är det betydligt viktigare (med autentisering). Det är absolut viktigare.
11b. R: Är det viktigare att kunna autentisera sig eller är det viktigare att du lär dig mer inom IT-säkerhet?
I4: Det första (alternativet) är viktigare här med. Ja det skulle jag vilja säga är absolut viktigare där också.
11c. R: Är det viktigare att kunna autentisera sig eller är det viktigare att kunna ta backups?
I4: Jag tycker det är två helt olika saker. Men i så fall är det fortfarande viktigare med det första (alternativet).
M: Att kunna bevisa att du är du (autentisering)?
I4: Ja.
11d. R: Är det viktigare att kunna autentisera sig eller är det viktigare att företaget kan tänkas utföra övervakning av er? I form av att granska loggar eller till och med komma på besök för att kontrollera att ni gör det ni ska.
I4: Då skulle jag säga att det är något viktigare att kunna logga in. Inte absolut viktigare men något viktigare.
11e. R: Är det viktigare att kunna autentisera sig eller är det viktigare att skydda konfidentiell information?

I4: Jag skulle vilja säga att de faktiskt hänger ihop med varandra. Det beror på vad det handlar om. Då är det nog något viktigare att kunna skydda konfidentiell information. För det är ju trots allt därför vi har dem här inloggen.
12a. R: Är det viktigare att hantera lösenord eller är det viktigare att du lär dig mer inom IT-säkerhet?
I4: Nej det är det första alternativet. Jag (personligen) bryr mig inte så mycket om IT-säkerhet eller vad som ligger bakom, så länge jag får instruktioner hur jag ska göra. Alltså något viktigare att hantera lösenord.
12b. R: Är det viktigare att hantera lösenord (i form av att ändra/byta och att memorera) eller är det viktigare att ta backups?
I4: Jag tycker den är jättesvår.
R: Antingen så är det inbyggt i systemet att ni måste ändra era lösenord regelbundet men då kan ni inte ta backups. Eller så kan ni ta backups men då har ni t.ex. bara ett och samma lösenord (till alla system) under hela er anställningstid.
I4: Då är backups absolut viktigare.
12c. R: Är det viktigare att hantera lösenord eller är det viktigare att företaget utför övervakning av er?
I4: Övervakning skulle jag då säga är absolut viktigare.
12d. R: Är det viktigare att hantera lösenord eller är det viktigare att kunna skydda viktig (konfidentiell) information?
I4: Det är absolut viktigare att kunna skydda viktig (konfidentiell) information.
13a. R: Är det viktigare för dig att lära dig mer inom IT-säkerhet eller är det viktigare att du kan ta backups?
I4: Då är backups mycket (absolut) viktigare.
13b. R: Är det viktigare för dig att lära dig mer inom IT-säkerhet eller är det viktigare att företaget utför övervakning av er?
I4: Då är övervakning absolut viktigare.
13c. R: Är det viktigare att lära dig mer inom IT-säkerhet eller är det viktigare att kunna skydda viktig (konfidentiell) information?
I4: Att kunna skydda viktig information är absolut viktigare.
14a. R: Är det viktigare att kunna ta backups eller är det viktigare att företaget utför övervakning av er?
I4: Då är det absolut viktigare att kunna ta backups.
14b. R: Är det viktigare att kunna ta backups eller är det viktigare att kunna skydda konfidentiell information?
I4: Då är det något viktigare att kunna skydda den viktiga (konfidentiella) informationen.
15a. R: Är det viktigare att företaget utför övervakning av er eller är det viktigare att du kan skydda konfidentiell information?
I4: Då är det absolut viktigare att skydda den konfidentiella informationen.

16a. M: Hur lång tid tar det och anser du att det tar rimligt lång tid att autententisera sig?
I4: Jag tycker det är rimligt det vi har här. Från att jag startar datorn till att… ett par minuter tills jag har loggat in i alla systemen. Det tar kanske inte ens så lång tid. 1 minut. Det är många program som ska starta men de startar fort.
16b. M: Hur lång tid tar det och anser du att det tar rimligt lång tid att hantera lösenord? I form av att ändra, memorera och att skriva ner om det behövs.
I4: Bara själva ändringen av ett lösenord tar kanske 10 sekunder. Från det att jag får upp en ruta som säger att det är dags att byta lösenord till att jag byter det tar det 10 sekunder. Det ska gå fort.
M: Hur går det att memorera dem? (tidsmässigt)
I4: Jag har det motoriska minnet som sitter här (i fingrarna). Man knappar in det och blir det en siffra fel så vet jag vad jag ska testa istället.
M: Då tar det rimligt med lång tid?
I4: Ja.
16c. M: Hur lång tid tar det och anser du att det tar rimligt lång tid att lära dig mer inom informationssäkerhet? Även om det inte är något som utförs här på företaget (i form av utbildningar).
I4: Jag tycker inte det i alla fall (det tar rimligt lång tid).
M: Men hur lång tid tar det att lära sig mer om du skulle göra det aktivt på fritiden? Svårt att svara på kanske.
I4: Ja precis. Det tar ingen tid överhuvudtaget vill jag säga. Jag förutsätter att min arbetsgivare sköter den biten. Om det är något nytt jag ska lära mig så förväntar jag mig att jag får den informationen.
16d. M: Hur lång tid tar det och anser du att det tar rimligt lång tid att ta backups? Men det sköts ju automatiskt. Märker du av att din dator slöas ner (påverkas) ifall det tas en backup och märker du överhuvudtaget av att det tas en backup?
I4: Just vad det gäller backups så har jag inte lagt märke till någonting. Det vet jag inte. Däremot uppdateringar är dem inte så smidiga med här. Men backups märker jag inte av.
M: Du förutsätter att det sköts automatiskt?
I4: Ja.
16e. M: Hur lång tid tar det och anser du att det tar rimligt lång tid att skydda viktig (konfidentiell) information?

R: Gör du något aktivt t.ex. om du krypterar eller lägger dem i speciella filer?
I4: Nej. Vi utför ju vårt jobb enligt dem rutiner som finns men om det är aktivt för att skydda den informationen. Jo det är det ju. Det är sånt här man inte tänker på man bara gör det.
R: Men det är inget du krypterar själv?
I4: Nej jag gör ju ingenting aktivt. Jo vi har ju I-arkiv där vi sparar in allt i ett ärende. Och hur lång tid det tar att spara det är väl en rimlig tid. Det är svårt att säga rent tidsmässigt. För det gör vi ju hela tiden dagligen så fort vi får in ett dokument för då ska det ju sparas in där. Men det är inget som jag tänker på.
M: Då tar det varken för lång tid eller kort tid?
I4: Nej. Jag tycker det är en rimlig tid definitivt.

17a. R: Hur ofta eller hur många gånger skulle du säga under loppet av en arbetsdag autentiserar dig mot en applikation eller ett program?
I4: Totalt sett i alla program. 10-15. För varje gång jag lämnar min dator så låser jag den och så måste jag ju logga in i den igen. Så det beror ju också lite på hur många gånger jag reser mig (och lämnar datorn). Men någonstans mellan 10-15 gånger.
17b. R: Hur ofta hanterar du lösenord i form av att du måste byta dem?
I4: En gång i månaden kanske. En eller två gånger i månaden. Det är ju inbyggt i alla systemen att nu är det dags att byta (lösenord).
17c. R: Har du någon aning om hur ofta det tas backups?
I4: Ingen aning.
I4: (På den tänkta frågan om hur ofta det ges utbildningar i informationssäkerhet som vi hoppade över eftersom det inte gavs) Så fort det är någon spam på gång eller liknande då kommer det alltid ut mejl med information om det. Om ni räknar det som utbildning så får vi det. Men inte aktivt att i form av att vi samlas och går igenom detta eller detta.
17d. R: Hur ofta skyddar du viktig (konfidentiell) information?
I4: Inte aktivt för att skydda den men när vi sparar in det i I-arkivet, som det heter, så är det ju bara vi som har behörighet till att komma in där som kan se det så på det sättet så gör man ju någonting aktivt.

18a. M: Vad är belöningen eller vad får du ut av med att autentisera dig mot en tjänst (i form av autentisering)?
I4: Då vet jag att ingen annan är inne och gör något i mitt namn. Vi har ju sekretess emot våra kunder och våra skadeärenden. Jag vet att ingen annan loggar in i mitt namn och betalar ut pengar i ärenden. Utan då vet jag att det är jag som sköter den biten. Det som görs i mitt namn det är jag som har gjort det.
18b. M: Vad är belöningen med att du hanterar dina lösenord? Att ändra dem när de ska ändras.
I4: Jag vet inte om där är någon belöning för det är lika irriterande när det kommer varje gång.
R: Ser du någon belöning i att du krävs att byta det regelbundet?
I4: Jo definitivt. Det är ju bra ifall någon skulle ha sett mitt lösenord och att jag då har ändrat det efter en period så att ingen annan kommer åt det. Det är väl det i så fall.
M: Ser du någon belöning med att memorera dem (lösenorden) istället för att skriva ner dem?
I4: Alltså det är ju alltid en risk med att skriva ner dem. Skriver jag ner dem så kan ju någon hitta dem. Så det är definitivt en belöning med att hålla dem i huvudet med att det är mindre risk att någon kommer åt det.
18c. M: Vad är belöningen med att lära sig mer inom IT-säkerhet? Om företaget hade tillhandahållit utbildningar. Skulle du se någon belöning eller fördel med det i så fall?
I4: Det är ju alltid nyttigt med att kunna mer om det för att vi ska kunna skydda våra kunder och den informationen vi har. Men det är nog den enda (belöningen), jag har inte något större intresse av det personligen av att veta mer.
18d. M: Vad är belöningen med att ta backups?
I4: Därför att all information ligger i datorn. Skulle något hända (utan backups) så skulle det vara kört. Med tanke på att vi, varje person, reglerar mellan 100-150 skador i månaden och allt som är dokumenterat… det skulle ju inte funka (utan backups).
18e. M: Vad är belöningen med att övervakas?
I4: Därför att då vet jag att det går korrekt till. För min del får dem jättegärna gå in och granska mig för att jag vet att jag har ryggen fri. Men det förekommer ju ibland att det finns oärliga handläggare som kan sno pengar och kan man komma ifrån det genom att gå in och granska så gör det. Dem får jättegärna gå in och övervaka. Allt vi gör här det gör vi på uppdrag av vår arbetsgivare och då har dem enligt mig rätt att gå in och kolla vad jag gör. Dem betalar mig för min arbetstid här och då förväntar jag mig att man också kollar att allt går rätt till.
18f. M: Vad är belöningen med att skydda viktig (konfidentiell) information?
I4: Enligt lag måste vi göra det för våra kunder, det är inget som vi själva har hittat på. Det är finansinspektionen som går in och pekar på så här ska ni göra. Gör vi inte det (som finansinspektionen säger) så skulle det kosta oss väldigt

mycket pengar. Men sen framförallt är det för våra kunders skull. De försäkringsavtal vi har är ju mellan oss och kunden. Det handlar om att det inte ska komma i orätta händer, det handlar ju också om kunder som ringer in och vill ha information men det lämnar vi ju inte ut. Det är ju bara till den kunden som vi har avtal med.

19. R: Hade du kunnat tänka dig att bryta mot företagets ISP? T.ex. om du inte loggar ut varje gång du lämnar din arbetsstation.
I4: Självklart ifall jag går iväg tre meter för att hämta ett kuvert så låser ju inte jag min dator. Men så fort jag ska lämna så att jag inte ser min arbetsplats då ska den ju låsas. Alltså jag är ganska fyrkantig av mig, säger någon till mig att gör på det här sättet då gör jag så. För det är enklast.
20. R: Om du skulle få reda på att någon utomstående hade hackat din konfidentiella information, hur skulle du reagera då?
I4: Min personliga känsla hade varit mer åt mina kunder… om något hade kommit ut. Det är ju för jävligt om någon skulle komma åt det. Då hoppas jag att våra arbetsgivare tar tag i det hela och försöker spåra vem det är som har gjort det. Men någon personlig känsla för att jag tycker att det är jobbigt skulle jag nog inte säga att det skulle finnas. Utan det handlar ju om kundernas information.
21. R: Om en kollega skulle ta del av din konfidentiella information utan ditt godkännande och du sedan hade fått reda på det, hur skulle du reagera då?
I4: Fast dem har tillgång till samma grejor som jag så att jag har inget konfidentiellt som bara gäller mina ärenden. Det som jag har tillgång till det har mina kollegor också tillgång till.
R: Det är inte så att du tillsammans med några andra har information som t.ex. inte andra nödvändigtvis har tillgång till?
I4: Inte för min del. Jag har inte det men det finns ju kollegor här som har hand om skyddade id t.ex. Det har inte jag behörighet till att komma in i. Men där är det ju också en spärr i systemet så att jag inte kommer åt det. Men det jag jobbar med kommer mina kollegor åt också.
R: Så det hade inte spelat någon roll?
I4: Nej eftersom de kommer åt det så påverkar det inte.
22. R: Nu ligger ansvaret för att ta backups på företaget. Bör det ligga där eller bör det ligga på individen?
I4: Nej det tycker jag definitivt att det ska ligga på arbetsgivarens ansvar. För annars blir det att om jag lägger en backup på min dator så vad har jag för nytta av den egentligen? Då kommer ingen annan åt den. Det är arbetsgivarens ansvar.
23. R: Har du en mobil företagsenhet? Bärbar dator eller en företagstelefon?
I4: En bärbar dator.
24. R: Gör du något speciellt för att skydda den mer än genom ett lösenordsskydd?
I4: Nej. Alltså vi har bara bärbara datorer så dockar vi in dem så då kan vi ju sitta var som helst och jobba.
M: Om du tar hem den, skyddar du informationen på olika sätt än om du sitter här (på kontoret)?
I4: Ja det får jag ju se till att göra. För om min man är hemma så får ju inte han ha tillgång på det som finns på datorn. Men det är ju samma rutin egentligen att man låser datorn. Men inget annat mer aktivt nej.
25. R: Vi tänker oss att du har en företagstelefon när du är ute på lunch och får ett mejl innehållande kundinformation som du måste vidarebefordra till en kollega. Väntar du till du är tillbaka på jobb efter lunchen eller vidarebefordrar du mejlet med en gång via mobilen?
I4: Beror på vilket mejl det hade varit. Hade det varit något extremt akut hade jag skickat det vidare där och då men annars hade jag väntat till efter lunchen.
R: Är det några speciella säkerhetsaspekter som kanske hade fått dig att vänta (till du är tillbaka på kontoret)?
I4: Nej kanske inte säkerhetsaspekter utan snarare beroende på innehållet (i mejlet), varför de hör av sig. Men annars är det väl betydligt mer osäkert i mobiltelefonen än vad det är i en vanlig dator. Ska man ta hänsyn till det så får man vänta till när man är tillbaka (på kontoret).
26. R: Har du några övriga åsikter eller funderingar kring IT-säkerheten här? Är det något du känner att ni är speciellt bra på eller något du tycker behöver förbättras? Kanske något du märkt av när du har arbetat?
I4. Inget som jag har tänkt på vad gäller nu.
M: Hur ser du på att företaget inte tillhandahåller direkta utbildningar? Är det något som du hade velat ha?
I4: Nej. Jag har inget personligt intresse för det och jag förväntar mig att dem som är ansvariga för IT-säkerheten att de har utbildning och om det är något som vi behöver veta så kommer dem ut med den informationen. Att det faktiskt jobbas aktivt med det där (IT-avdelningen) istället. Så för min egen del nej. Jag tycker det är jätteskönt när någon annan tar hand om det.

Bilaga 6 - Intervjuperson 5 (I5)

När; Utfört 22/4 - 2016
Var; På plats hos företaget

1. M: Vilken roll har du inom företaget?
I5: Skadereglerare motor privat.
2. M: Hur god datorvana har du enligt dig själv? 1-4?
I5: 4.
M: En kommentar till det?
I5: Jag har själv läst teknikprogrammet, Data/IT inriktning när jag gick i gymnasiet. Har hållit på mycket med datorer och kan lite programmering och system och sådant, så jag har det i bakfickan.
3. M: Hur säkerhetsmedveten är du enligt dig själv?
I5: Relativt.
M: 1-4?
I5: 3,5 kanske, man kan inte vara till 100 % där. Utan det finns alltid något nytt, ja allt från fysisk hack och allting. De är alltid steget före, vi kan aldrig vara steget före dem.Och säkerheten är ju som den är, man kan hacka in sig i allt, allt från banker till kasinon och ja, det är dem som är säkrast i dagsläget. Är ju kasinon egentligen, de är säkrare än bankerna, sjukt nog men ja.
4. M: Hur hanterar du dina lösenord?
I5: Bra
M: I form av både ändring, memorering, skriver ner dem? De sitter i huvudet?
I5: Ja.
R: Det är ingenting du skriver ner eller antecknar?
I5: Nej.
M: Får du lösenord genererat till dig eller väljer du dem själva?
I5: Jag väljer dem själv.
M: Anser du det är lätt eller svårt att hantera lösenord, och då tänker jag på allt i from utav ändring, memorering?
I5: Nej, det är relativt enkelt.
5. M: Hur autentiserar du dig mot en tjänst? I form av, använder du användarnamn och lösenord, eller något smartcard?
I5: Alltså du menar i våra system?
M: Ja, för att komma in i program och så?
R: Är det något utöver användarnamn och lösenord?
I5: Det är användarnamn och lösenord, är det så att man till exempel dockar ut och har med sig datorn någon annanstans så är det genom VPN-länk som man måste ha en app via telefonen. Måste man gå in och få VPN-koden, in där, sedan är det samma procedur också, användarnamn och lösenord.
M: Hur många användarnamn och lösenord har du, på de olika systemen, uppskattningsvis?
I5: Alltså minst fyra-fem som man jobbar med dagligen. Sen finns det ju andra som man knappt jobbar med, och som kanske inte är lika. Det är ju inte mer kunduppgifter på samma sätt så att man kanske har de på mejlen eller något liknande, som man har fått från vissa tjänster. Det är mer så att man loggar in för att kunna lägga en beställning eller något liknande. Men bara system, databaser och allt sådär så är det nog fyra stycken, skulle jag säga.
6. M: Du nämnde innan att du har läst just IT-säkerhet och så? Men lär du dig mer om IT-säkerhet (utbildning) här på jobbet?
I5: Alltså på jobbet, nja inget specifikt mot mig eller så generellt. Det är ju mer information kommer ut från våra IT-säkerhetskillar och drift och lite så. Om man ska akta sig, om man ska vara försiktig hit, och då kanske om det har kommit in några fejkmejl eller någonting, att man inte ska klicka hit eller dit, så att det är den informationen vi får rent jobbmässigt. Men rent privatmässigt är det ingenting jag håller på med, om man säger så.
M: Om man tänker jobbmässigt, anser du att det är lätt eller svårt då att lära dig mer och ta del av den informationen?
R: Är det något du aktivt gör, alltså försöker du lära dig mer på fritiden?
I5: Som person i fråga eller jobbrelaterat?
R: Ja nu är det personligt.
I5, Personligt, visst man läser lite, det är kul att veta så man är målmedveten, man ska ju akta sig och visst, man har ett litet intresse för det, absolut.

7. M: Har företaget en tydligt uttalad ISP? Kan du den?
I5: Ja den finns, absolut. Den finns på vårt intranät, och den är tillgänglig för alla.
M: Kan du vad den innebär så att säga?
I5: Alltså det är många punkter, det är ingenting man memorerar i huvudet direkt, utan det är något man bara har lärt sig sen sitter det i bakhuvudet om man säger så.
R: Men du skulle du säga att du är väl medveten om vad som är tillåtet och vad som inte är tillåtet?
I5: Absolut, det är man.
8. M: När det gäller säkerhetskopiering och backups, hur sköter du det?
I5: Det finns inget som jag håller på med som behövs säkerhetskopieras eller behövs som backuper. Utan jag har för mig att våra datorer sköter det automatiskt via servern. Alltså att de har en separat backup där på det, så det är ingenting som vi aktivt gör om man säger så. Det är mer om man till exempel skulle ha med sig ett egen USB-minne, att man kör de i krypteringsläge och lite annat sådär, men det är ingenting som jag använder heller, och jag har heller aldrig använt det.
M: Så då är det svårt att säga om det är lätt eller svårt.
I5: Ja, det är svårt att bedöma det då.
9. M: Anser du att det är lätt eller svårt att bryta mot er bestämda policy som ni har (inga stora övertramp)?
R: Om det är något som kan tänkas hända på daglig basis?
I5: Lätt och lätt, det är svårt att säga, det beror på vem man är som person. Tar jag det personligen så skulle jag säga nej på den. Det är inte lätt att bryta mot den, det beror på vem man är som person och vad är det för information man ger till kunderna, vem är det som ringer in. Man identifierar det, vem är det jag talar med? Man hör det direkt, har de uppgifter och vet de lite, är det någon som sitter sidan om. Lite sådant. Nej skulle jag säga på den.
M: Om man tänker mer på dig personligen, hur lätt har du för att bryta mot policyn som företaget har satt upp, du som medarbetare hos företaget?
I5: Ingenting alls.
10. M: Hur skyddar du viktig information (konfidentiell information)?
R: Gör du något aktivt för att skydda den, tex kryptering?
I5: Man följer de riktlinjer som vi har på vårt intranät, som jag tidigare sa med USB-kryptering. Om jag som person gör det aktivt, det är till exempel när jag jobbar hemma eller vart jag sitter någonstans att jag aktar mig vem jag har runt omkring mig. Lite sådana småsaker, försiktig när jag skriver in mina lösenord. Man får ju inte visa för mycket information, jag har till exempel inte grejor på bordet eller något sådant där eller personuppgifter och lite sådant. Det skiljer också, för att jag kan sticka in på toaletten eller hämta en kopp kaffe eller någonting, det är inte så bra om någon annan kommer. Det är lite sådana småsaker eller smådetaljer som man bara gör.
M: Anser du då att det är lätt eller svårt att göra det?
I5: Det är lätt att skydda det, absolut.

11a. R: Är det viktigare att kunna autentisera sig (logga in och visa att du är du) när du utför ditt arbete eller är det viktigare att du kan hantera dina lösenord i form av att du kan memorera dem lätt, kan ändra de när det behövs osv? Vad är viktigast: Att du kan autentisera dig att du är du eller att du kan byta lösenord till exempel.
I5: Att jag är jag, för då har jag ansvar för det. Och då kan jag skydda mina handlingar.
M: Absolut eller något viktigare?
I5: Jag tycker det är lite viktigare faktiskt, sen att man ska kunna byta lösenord. Systemen genererar och har ett visst antal månader, dagar eller veckor eller hur det är, så får man upp att det är dags att byta lösenord så utifrån det så anser jag det är viktigare då. Och man har ju den påminnelsen.
11b. R: Är det viktigare att kunna autentisera sig eller är det viktigare att du lär dig mer inom IT-säkerhet? Här på jobbet då, inte privat.
I5: Den är svår, för det är både och där faktiskt, skulle jag vilja säga. Fortfarande lite ja ja för att det är jag som är handläggaren och det är jag som jobbar med mina egna skador, det är jag som är ansiktet utåt mot kunderna också. Så den får man inte glömma, det är ju en stor bit i just den branschen jag jobbar i. Men sen samtidigt, så måste jag också tänka på att man måste ju lära sig säkerhet, för vi jobbar med säkerhet dagligen och det är det som kan förstöra ett helt företag i slutändan. Så den kan man inte svara rakt på egentligen.
R: Men om du hade fått välja?
I5: Då får jag nog köra på den första faktiskt.
R: Det är något viktigare att du kan autentisera dig?
I5: Ja.
11c. R: Är det viktigare för dig att du kan autentisera dig eller är det viktigare att du kan ta backups? Om du gör det själv eller att det sköts automatiskt med backups, men vad är viktigare?

I5: Självklart så måste man kunna logga in, så om man skulle vara lite hård med det, så skulle man säga att du kan inte logga in men du kan ta backups.
R: Funktionen att du kan autentisera dig att du är du, vi tänker också att ni inte hade behövt logga in på datorerna här. Alla hade haft sin dator men man hade inte behövt logga in utan bara att starta datorn och så är datorn igång. Vad är viktigare då?
I5: Det är kaos, jag skulle nog säga att man ska kunna logga in faktiskt, för den är skitviktig.
R: Absolut viktigare då eller?
I5: Ja jag tycker det, tillbaka till samma sak, det är nästan fråga. Systemen gör automatiskt backups så det är inget jag heller gör aktivt, så därför håller jag mig nog till den första.
11d. R: Är det viktigare för dig att du kan autentisera dig eller är det viktigare att företaget kan tänkas utföra övervakning av er, i form av att granska era logga eller till och med komma på besök?
I5: Jag kan nog inte svara på den frågan faktiskt.
R: Ser du någon fördel med att ledningen skulle göra övervakning på er?
I5: Absolut finns det en fördel, för det är ju en säkerhet både företagsmässigt mot kunderna men samtidigt mot oss, för att skulle vi göra ett misstag att det syns så att vi kan lära oss av de misstagen. För vi hanterar ju mot ett x antal miljoner per handläggare per år, så det är inga småbelopp vi snackar om. Så absolut, jag tycker att det är viktigt att det granskas och att skulle man göra någon miss eller fel, man kan ändra på det och förbättras och att det syns. Men sen samtidigt, det är också viktigt att man alltid ska veta vilken person är det som gör det, vem är det som loggar in, vem är det som är ansvarig. För att oavsett vad, när jag kommer hit på dagen och när jag slutar, det jag har gjort är det jag som är ansvarig för, ingen annan.
R: Kan du svara på den nu?
I5: Något viktigare att kunna autentisera sig.
11e. R: Är det viktigare att du kan autentisera dig eller är det viktigare att du kan skydda konfidentiell information?
I5: Jag skulle köra tvåan på den faktiskt.
R: Något viktigare eller absolut viktigare?
I5: Det är något viktigare.
12a. R: Är det viktigare för dig att du kan hantera lösenord än att du lär dig mer inom IT-säkerhet?
I5: Personligen till jobb, att kunna logga in där.
R: Hantera lösenord, i form av att memorera, att du kan byta lösenord ifall det skulle behövas?
I5: Ställ frågan en gång till.
R: Är det viktigare för dig att du till exempel kan byta lösenord när det behövs eller är det viktigare att du kan lära dig mer om IT-säkerhet?
M: Alltså är hantering av lösenord viktigare eller är det att lära sig mer om IT-säkerhet?
R: För dig personligen, du kanske känner att du kanske tillräckligt om IT-säkerhet.
I5: De tär viktigare att jag kan byta lösenord isåfall.
R: Något viktigare eller absolut viktigare?
I5: Det är något viktigare där.
12b. R: Är det viktigare att du kan byta lösenord än att du kan ta backups? vad hade du helst valt?
I5: Då hade jag nog kört backup faktiskt. Något viktigare att du kan göra det för att skulle det skita sig så är det illa. Backup skulle jag säga på den då.
12c. R: Är det viktigare att du kan hantera lösenord än att företaget utför eventuell övervakning av er?
I5: Något viktigare att hantera lösenord.
12d. R: Är det viktigare att hantera lösenord än att du kan skydda viktig information?
I5: Skydda viktig information.
R: Absolut viktigare?
I5: Ja.
13a. R: Är det viktigare för dig att du kan lära dig mer inom IT-säkerhet eller att ta backups?
I5: Fortfarande till jobbfrågan, då är det backups.
R: Något viktigare eller absolut?
I5: Det är viktigare, absolut.
13b. R: Är det viktigare för dig att du kan lära dig mer inom IT-säkerhet eller är det viktigare att företaget utför övervakning av er?
I5: Det är något viktigare att företaget utför övervakning. Anledningen till varför dem gör det, då lär man ju sig säkerhet och då får man information osv. Man får två flugor i en smäll.
13c. R: Är det viktigare att du lär dig mer inom IT-säkerhet eller är det viktigare att du kan skydda viktig (konfidentiell) information?

I5: Det är mycket (absolut) viktigare att skydda konfidentiell information.
14a. R: Är det viktigare för dig att det tas backups eller är det viktigare att företaget utför övervakning av er?
I5: Backups är absolut viktigare.
14b. R: Är det viktigare att kunna ta backups eller att skydda viktig (konfidentiell) information?
I5: Det är något viktigare att kunna skydda viktig (konfidentiell) information.
15a. R: Är det viktigare att företaget utför övervakning av er eller är det viktigare att du kan skydda konfidentiell information?
I5: Det är mycket (absolut) viktigare att skydda konfidentiell information.

16a. M: Hur lång tid tar det och anser du att det tar rimligt lång tid att autentisera sig mot en tjänst (system)?
I5: Alltså vi har många system så det är svårt att svara på den frågan. Hade vi bara haft ett system så hade det gått relativt snabbt. Men eftersom att vi startar flera olika system där vi har olika saker (information) att ha tillgång till.
R: Tycker du ibland att det tar för lång tid eftersom att du behöver starta flera system?
I5: Nej jag tycker det är relativt (bra). För att med tanke på hur många system och program du öppnar där du måste logga in för att identifiera dig på varje system tycker jag att det är relativt okej.
16b. M: Hur lång tid tar det och anser du att det tar rimligt lång tid att hantera lösenord i form av att ändra och memorera?
I5: Det går relativt snabbt.
M: Hur lång tid tar det anser du, att byta lösenord?
I5: Ett par sekunder. Du får upp en liten ruta där du skriver ditt användarnamn och gamla lösenord och ditt nya lösenord två gånger. Oftast skriver du ditt nya lösenord två gånger men ibland en gång och sen är det klart.
16c. M: Hur lång tid tar det och anser du att det tar rimligt lång tid att lära dig mer inom informationssäkerhet?
I5: Det kan ta tid. Det är brett och stort. Det är inte ren svenska om man säger så.
16d. M: Hur lång tid tar det och anser du att det tar rimligt lång tid att ta backups?
I5: Nu hanterar inte jag backups själv.
R: Men det är inget du märker påverkar era datorers prestanda?
I5: Nej. Ingenting jag har lagt märke till. Jag har ingen aning om hur lång tid det tar.
16e. M: Hur lång tid tar det och anser du att det tar rimligt lång tid att skydda viktig (konfidentiell) information?
I5: Det tar ingen tid alls.
R: Det är inget du lägger i specifika mappar som ska vara mer skyddade än andra?
I5: Nej. Vi har ju speciella handläggare som har hand om skyddade identiteter. Dem har speciella rutiner för det.

17a. R: Hur ofta skulle du säga att under en arbetsdag autentiserar dig mot en tjänst? Hur många gånger?
I5: En gång. Ett system loggar ut dig ifall du inte är aktiv. Det beror lite på hur du använder det systemet (hur aktiv man är). Tre till fyra gånger kanske. Nej lite mer eftersom man låser datorn, om man ska räkna med det, när man ska hämta kaffe eller gå på toaletten. Det blir ändå tio gånger kanske på en dag. Räknat med när man börjar dagen och alla raster och toalettpauser.
17b. R: Hur ofta byter du lösenord?
I5: Det vet jag faktiskt inte.
R: På ett ungefärligt snitt?
I5: Nej det vet jag faktiskt inte. Per år? En gång varje månad eller varannan månad skulle jag säga. Jag vet inte exakt vad det är för tidsintervall men något sådant.
17c. R: Företaget tillhandahåller inga utbildningar men ni brukar få meddelande om när det är något ni ska vara vaksamma över. Ungefär hur ofta sker det?
I5: Det får vi av våra IT-killar. Det är inte så ofta det händer. Dem har en relativt bra brandvägg men ibland så slinker vissa saker igenom. När det händer så skickas direkt ut en varning till alla fast det bara kanske är en person som har stött på det. Då är alla medvetna om det och aktsamma.
17d. R: Har du någon aning om hur ofta det tas backups?
I5: Nej.
17e. R: Har du någon aning om hur ofta företaget kan tänkas övervaka er? Era loggar?
I5: Nej.
17f. R: Hur ofta skyddar du viktig information? Det kanske du har svarat lite på tidigare.
I5: Ja det gör man automatiskt.

18a. M: Vad är belöningen med att autentisera sig mot en tjänst? Själva autentiseringen av dig.

I5: Att det är jag som är jag och jag som jobbar. Man kan ta ut statistik på mig, man har ju ett användarid. Jag skulle vilja säga (att fördelen) är statistikmässig.
18b. M: Vad är belöningen med att hantera lösenord (memorera)?
I5: Ingen kan komma åt mina lösenord.
18c. M: Vad är belöningen med att lära sig mer om IT-säkerhet? Om det hade skett på företaget.
I5: Ja då hade man kanske tagit det på den privata sidan också. T.ex. att man är mer aktivt försiktig när man slår in koden när man handlar eller tar ut pengar eller vad man nu än gör. När man loggar in med sitt bankid och ska betala räkningar. Utifrån det man får från jobbet kan man utnyttja privatmässigt också ju.
R: Du menar att det hade hjälpt dig mer generellt sett? I det vardagliga livet?
I5: Absolut.
18d. M: Vad är belöningen med att ta backups?
I5: Ingen aning.
18e. M: Vad är belöningen med att det sker övervakning av er?
I5: Belöningen kan vara att man förbättras ifall man gör misstag. Det är väl det jag skulle säga.
18f. M: Vad är belöningen med att skydda viktig (konfidentiell) information?
I5: Nöjda kunder. Nöjda medarbetare också för då slipper man tjafs. Man skriver klart och tydligt vem som ringer in och vem man har talat med tidigare. Om någon annan ringer in (angående ett specifikt ärende) så är man försiktigare.

19. R: Hade du kunnat tänka dig att bryta mot ISP? Det kan handla om att t.ex. inte logga ut från din station om du ska ta en kopp kaffe. Har något sådant hänt?
I5: Det har hänt att man kanske bar sprungit iväg på toaletten och glömt låsa datorn. Man har bara glömt det. Men det är man ganska försiktig med ändå men det har säkert hänt några gånger.
20. R: Om du skulle få reda på att någon utomstående hade hackat din konfidentiella information, hur hade du reagerat då? Hade det varit kritiskt?
I5: Det hade varit kritiskt. Jag hade tagit tag i det direkt med min chef till IT-killarna. Det är farligt skulle jag säga.
21. R: Om en kollega hade tagit del av din konfidentiella information. Hur hade du reagerat då?
I5: Samma sak där. Oavsett om det är någon utifrån eller någon kollega. Det här är min information och det är jag som loggar in och ingen annan.
22. R: Nu ligger ansvaret att ta backups på företaget, det sköts automatiskt. Tycker du att det bör ligga där (och inte på individen)?
I5: Det bör ligga där (på företaget).
23. R: Har du någon mobil företagsenhet?
I5: Den mobila enheten är ju laptopen.
24. R: Gör du något speciellt för att skydda den mer än med lösenord?
I5: Det är bara användarnamn och lösenord. Du kommer inte in annars. Jag sparar ingenting på skrivbordet t.ex. eftersom det är inte lika säkert än om man gör det på servern. Den är ju mer krypterad än skrivbordet.
M: Om du t.ex. har med dig datorn hem och jobbar på den, skyddar du den på något annat sätt då?
I5: Nej jag skyddar den på samma sätt (som datorn på jobb). Det spelar ingen roll var jag är någonstans, samma rutiner gäller.
25. R: Vi tänker oss ett scenario där du har en företagstelefon som är kopplad till din företagsmejl. Du är ute på lunch och du får ett mejl med kundinformation som du måste vidarebefordra till en kollega. Väntar du till du är tillbaka på jobb efter lunchen eller vidarebefordrar du det direkt?
I5: Om du tänker på krypteringssynpunkten så kanske man inte kan kryptera telefonen på samma sätt som datorn.
R: Hur känslig informationen är kan också spela roll?
I5: Ja lite så. Beror på vad det är för information.
R: Som du sa tidigare så kanske du tänker på vem som står bredvid dig?
I5: Ja det skulle jag vilja säga. Jag förmodar att det finns lösenordsskydd på telefonen och att ingen på det sättet kan ha åtkomst till den. Då är dem tillräckligt säkra.
M: Väljer du då att göra det på plats för att det ska gå snabbt eller väntar du med det så det tar längre tid.
I5: Är det inget akut så får det vänta.
M: Om det hade varit något akut så hade du gjort det på plats?
I5: Det är en tolkningsfråga. Det beror på vad det är för typ av information, är det bara generell information eller är det kontouppgifter och personuppgifter så man måste vara mer försiktig med. Sen vet jag inte vad det är för typ av kryptering på de telefoner, för dem som har företagstelefoner. Men jag förmodar att det inte är riktigt samma mejlsystem. Det är svårt att säga där.

26. R: Har du några åsikter eller funderingar kring IT-säkerheten här? Hur tycker du att det funkar? Är det något ni är speciellt bra på eller något ni borde bli bättre på?
I5: Jag skulle vilja säga att det är tillräckligt säkert.
M: Det finns inget som du tycker borde förbättras?
I5: Nej inget jag kommer på nu på rak arm.
M: Hade du velat att företaget tillhandahöll utbildningar i IT-säkerhet?
I5: Absolut. Det är alltid bra och intressant det finns inget negativt med det. Det hade dem kanske kunnat lägga lite mer resurser på. Men samtidigt så har dem sina IT-killar som styr hela den biten så att vi inte behöver tänka på det. Det (ansvaret) ligger på dem. Det är ju inte många som har åtkomst till administrationsuppgifter om du t.ex. ska installera eller ändra något på laptopen. T.ex. här i X (hålls anonymt) är det ingen som har det. Därför tycker jag ändå att det är så pass säkert. Det är inte många personer som har den åtkomsten. Desto fler som har det ju mindre säkert blir det ju. Det är det vi som medarbetare kan se, det finns säkert andra saker. Rent generellt skulle jag vilja säga att det är tillräckligt säkert.

Referenslista

Adams, A & Sasse, M.A. (1999). Users are not the enemy, *Communications of the ACM*, Vol 42, No 12, sid 40-46.

Alvarez, C. (2013). *Cintas Study Finds Two Thirds of U.S. Adults Would Not Return to a Business Where Their Personal Information was Stolen*, URL: http://www.marketwatch.com/story/cintas-study-finds-two-thirds-of-us-adults-would-not-return-to-a-business-where-their-personal-information-was-stolen-2013-10-21?reflink=MW_news_stmp Hämtad: 2016-02-01.

Bulgurcu, B, Cavusoglu, H, Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, *MIS Quarterly*, Vol. 34 No. 3, sid. 523-548.

Busson, K. (2008). Best Practices for Backup Security, *The Journal of Financial Services Technology*, Vol 2, No 1, sid. 47-51.

Byun, J-W& Li, N. (2008). Purpose Based Access Control for Privacy Protection in Relational Database Systems, *The VLDB Journal*, Vol 17, No. 4, sid 603-619.

Chen, C, Shaw, R & Yang, S. (2006). Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System, *Information Technology, Learning, and Performance Journal*, Vol. 24, No. 1.

D'Arcy, J, Hovav, A & Galletta, D. (2008). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach, *Information Systems Research*, Vol 20, No 1, sid. 79-98.

Diesburg, S. M. and Wang, A. A. (2010). A survey of confidential data storage and deletion methods, *ACM Computing Surveys*, Vol 43, No 1.

Gaw, S, Felten E.W. (2006). Password Management Strategies for Online Accounts, *SOUPS '06 Proceedings of the second symposium on Usable privacy and security*, sid 44-55.

Herath, T & Rao, H.R. (2009). Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness, *Decision Support Systems*, Vol 47, No 2, sid 154-165.

Huang, D, Zhang, X & Jim Luo, MK. (2010). MobiCloud: Building Secure Cloud Framework for Mobile Computing And Communication, *Service Oriented System Engineering (SOSE), 2010 Fifth IEEE International Symposium on*, sid. 27-34.

If. (u.å.,): *Databrott och IT-säkerhet*. URL: https://www.if.se/web/se/foretag/radochtips/databrott/pages/default.aspx Hämtad: 2016-03-03.

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

Knapp, K, Franklin Morris, R, Marshall, T & Byrd, T. (2009). Information security policy: an organizational-level process model, *Computers & Security*, Vol 28, No 7, sid 493-508.

Lee, J & Lee, Y. (2002). A holistic model of computer abuse within organizations, *Information Management & Computer Security*, Vol 10, No 2, sid. 57-63.

Monterosso, J & Ainslie, G. (1999). Beyond discounting: possible experimental models of impulse control, *Psychopharmacology*, Vol 146, No 4, sid. 339-347.

Ni, Q, Bertino, E, Trombetta, A & Lobo, J. (2010). Privacy-aware Role Based Access Control, *ACM Transactions on Information and System Security (TISSEC)*, Vol 13, No 3.

Oscarson, P, Öberg, W & Rystedt, B. (2009). *Modell för klassificering av information,* Version 1, Myndigheten för samhällsskydd och beredskap 0040-09.

Puhakainen, P & Siponen, M. (2010). Improving employees compliance through information systems security training: an action research study, *MIS Quarterly*, Vol. 34, No. 4, sid. 757-778.

Selvarani, D.R & Ravi, Dr.T.N. (2013). Issues, Solutions and Recommendations for Mobile Device Security, *International Journal of Innovative Research in Technology & Science (IJIRTS),* Vol 1, No 5, sid 9-14.

Siponen, M & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations, *MIS Quarterly*, Vol. 34, No 3, sid. 487-502.

Stamp, M. (2006). *Information security principles and practice*, John Wiley & Sons, Inc., Hoboken, New Jersey, sid. 1-18.

Steel, P & König, C. (2006). Integrating Theories of Motivation, *The Academy of Management Review*, Vol. 31, No 4, sid. 889-913.

Steel, P. (2007). The Nature of Procrastination: A Meta-Analytic and Theoretical Review of Quintessential Self-Regulatory Failure, *Psychological Bulletin*, Vol. 133, No 1, sid. 65–94.

Vance, A & Siponen, M. (2012). IS Security Policy Violations: a rational choice perspective, *Journal of Organizational and End User Computing*, Vol 24, No 2, sid. 21-41.

Vaughn, R, Dampier, D & Warkentin, M. (2004). Building an Information Security Education Program, *Proceeding InfoSecCD '04 Proceedings of the 1st annual conference on Information security curriculum development. ACM, New York,* sid. 41-45.

von Solms, R & van Niekerk, J. (2013). From information security to cyber security, *Computers & Security*, Vol 38, sid. 97-102.

Warkentin, M & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat, *European journal of information systems*, Vol 18, sid. 101-105.

Workman, M, Bommer, H & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test, *Computers in human behavior*, Vol 24, No 6, sid. 2799-2816.

Yan, J, Blackwell, A, Anderson, R & Grant, A. (2004). Password Memorability and Security: Empirical Results, *IEEE Security & Privacy*, Vol 2, No 5, sid. 25-31.

Yngström, L & Björck, F. (1999). The Value and Assessment of Information Security Education and Training, *Proceedings of the IFIP TC11 WG11*.