LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Informationssäkerhet hos företag

En studie i hur företag arbetar med CIA-triadens komponenter och hur detta påverkas av mänskliga faktorer

Kandidatuppsats 15 hp, kurs SYSK02 i informationssystem

Författare: Victoria Lidvall
Anna Strandberg

Handledare: Miranda Kajtazi

Examinatorer: Björn Johansson
Anders Svensson

Informationssäkerhet hos företag: En studie i hur företag arbetar med CIA-triadens komponenter och hur detta påverkas av mänskliga faktorer

Författare: Victoria Lidvall och Anna Strandberg

Utgivare: Inst. för informatik, Ekonomihögskolan, Lund universitet

Dokumenttyp: Kandidatuppsats

Antal sidor: 103

Nyckelord: Informationssäkerhet, CIA-triad, Mänskliga faktorer, Teknisk säkerhet, Strategisk säkerhet

Sammanfattning (Max. 200 ord):
Säkerhet ses oftast som en del av en teknisk lösning vilket gör att företag har en tendens att dedicera mer resurser till teknisk säkerhet, snarare än strategisk säkerhet. Mänskliga faktorer kan ha en avgörande negativ roll för informationssäkerheten inom företag om grunden till informationssäkerheten inte hanteras på rätt sätt. Uppsatsen undersöker kopplingen mellan modellen CIA-triadens olika delar; *confidentiality*, *integrity* och *availability,* var för sig men också som helhet, och de mänskliga faktorer som kan påverka dessa. Forskningsfrågan söker svar på hur mänskliga faktorer påverkar hur företag arbetar med CIA-triaden där litteraturstudien utreder tidigare forskning gjorda om CIA-triaden och tillhörande tilläggsmodeller, mänskliga faktorers påverkan på informationssäkerhetsystem och användares systemsäkerhetsmedvetande och beteende. Den empiriska studien innefattade en kvalitativ undersökning hos tre olika företag, med olika affärsinriktning och placering i kedjan informationssäkerhet, som placeras in i en figur för att illustrera hur de är sammanlänkande. Resultatet av undersökningen utmynnar i en diskussion som sammanfattas i en slutsats som visar att företag uppnår målen av varje komponent enskilt och ser inte CIA-triaden som en helhet. När det kom till mänskliga faktorer fokuserade två företag utav tre företag mer på utbildning och policys för att öka anställdas säkerhetsmedvetande. I slutsatsen presenteras hur väl den empiriska studien stämmer överens med redan etablerad informationssäkerhetsstandard, och hur eventuellt funna problem kan tacklas.

Innehåll

Figurer

Tabeller

1 Introduktion

För att skydda sin information lägger företag numera större vikt vid att stärka säkerheten gentemot externa attacker, genom att införa bättre tekniska lösningar, vilket resulterar i att en stor del av attackerna som kommer från interna aktiviteter glöms bort (Stanton, Stam, Jolton &Mastrangelo, 2004). Informationssäkerhet involverar både teknologi och människor, och ju starkare den tekniska säkerheten blir desto tydligare blir det att det är hos användaren säkerheten brister (Gonzales & Sawicka, 2002). Gonzales & Sawicka säger följande att "mänskliga faktorer är involverade i 80-90% av organisatoriska olyckor", och vidare att företag kan implementera tekniska lösningar men att de fortfarande misslyckas med att ta hand om den mänskliga faktorn. Att ha fungerade teknologi i en verksamhet är viktigt men både organisatoriska och mänskliga faktorer har en stor och avgörande roll för informationssäkerhet (Dutta & Roy, 2008). Stanton m.fl. (2004) nämner att "75% av kostnaderna för säkerhetsmisslyckanden är på grund av interna aktiviteter." Detta kan tyda på en bristande medvetenhet bland anställda om vad strategisk säkerhet är, samt att mänskliga faktorer kan vara en avgörande faktor när det gäller att lyckas med säkerhet.

Oavsett hur väl utformade eller implementerade säkerhetssystem är, förlitar sig alla säkerhetssystem på människor (Gonzalez & Sawicka, 2002). För att teknologi ska fungera så måste det användas (Siponen, 2000) – en teknisk lösning har i de flesta fall en användare, och är användandet fel och oaktsamt kan det innebära stora risker. De mänskliga faktorerna som anses kunna påverka informationssäkerheten inom företag handlar till en stor del om anställdas beteenden inom olika situationer (Siponen, 2000; Stanton m.fl., 2004; Warkentin & Willison, 2009) vilket påverkar deras sätt att hantera information. I deras studier, Siponen, 2000, Stanton m.fl., 2004, Warkentin & Willison, 2009, är oaktsamhet, brist på säkerhetsmedvetenhet och utbildning, felanvändning av teknik, arbetsroll, arbetslivserfarenhet och tilldelning av sekretessbelagd information till obehöriga bevisade faktorer som har en påverkan på informationssäkerhet.

Mänskliga faktorer och "den mänskliga faktorn"
I litteraturen omnämns *human factors* som fritt översatt till svenska blir *mänskliga faktorer*. Detta kan länkas till uttrycket "den mänskliga faktorn", vilket Nationalencyklopedin definierar som "benämning på mänskligt felhandlande som olycksorsak".[1]

Mänskliga faktorer, eller human factors på engelska, definieras av Human Factors and Ergonimics Society enligt följande *"[...] Human Factors is concerned with the application of what we know about people, their abilities, characteristics, and limitations to the design of equipment they use, environments in which they function, and jobs they perform"* (Human Factors and Ergonomics Society, 2016) - vilket kan tolkas som att överallt där människan är och utför uppgifter, dess egenskaper och kunskaper, är detta den en mänsklig faktor.

I vår undersökning och vidare diskussion har vi valt att, i likhet med exempelvis Stanton m.fl. (2004) och Siponen (2000), använda mänskliga faktorer som en benämning på olika beteenden

[1] *Nationalencyklopedin*, 'mänskliga faktorn'. http://www.ne.se.ludwig.lub.lu.se/uppslagsverk/encyklopedi/lång/mänskliga-faktorn (hämtad 2016-05-12).

en användare har i ett system, samt andra faktorer som bland annat säkerhetsmedvetande, delning av sekretessbelagd information till utomstående eller allmän oaktsamhet. Saker som kan påverka detta är till exempel utbildning inom företaget, arbetsroll och policys.

Säkerhetsutbildningar

"Säkerhetsutbildning och säkerhetsmedvetande höjer förståelsen för säkerhetsrutiner och viljan att följa dessa metoder" (LeVeque, 2006). En form av strategisk säkerhet är *SETA-programmet* (Security Education, Training & Awareness) "(…) vars syfte är att minska antalet säkerhetsbrott på grund av anställdas brist på säkerhetsmedvetenhet" (Hight, 2005). Företag som antingen förespråkar SETA eller liknande kurser är medvetna om vikten av att informera anställda om deras roll inom organisationen och informationssäkerhet för att undanvika attacker. Att införa obligatoriska säkerhetskurser hjälper företag att säkerhetsställa graden av säkerhetsmedvetande som anställda förväntas ha och, och förståelsen för de policys de förväntas följa.

Att definiera säkerhet

Det finns olika definitioner av säkerhet, vilket kan vara en anledning till missförstånd kring skillnaden i de olika betydelserna av säkerhet och säkerhet (safety och security). I det engelska språket syftar ordet "safety" på skydd mot fara, skada och olyckshändelser medan "security" inom organisationer syftar på skydd mot oönskade gärningar av tredje part (Dynabyte, 2016). Då många företag arbetar med det engelska språket som grund, kan en allmän okunskap och fel översättning vara avgörande. Den typen av säkerhet som uppsatsen kommer att fokusera på är informationssäkerhet. Konceptet informationssäkerhet har visat sig vara svår att fastställa (Katsikas, Backes, Gritzalis & Preneel, 2006), eftersom det kan tydas på olika sätt. Nedanför presenteras olika definitioner av konceptet.

I sin bok definierar Katsikas m.fl. (2006, s. 531) informationssäkerhet enligt följande:

Information security: *The process of ensuring information confidentiality, integrity and availability (CIA).*

Cambridge Dictionary definierar informationssäkerhet som följande:
Security (noun): *The protection of information against being stolen or used wrongly or illegally*.[2]

Baserad på de olika definitionerna av säkerhet kommer uppsatsen att utgå ifrån både Katsikas och Cambridge Dictionarys definition.

Ökandet av internetbrott har uppmärksammat konceptet informationssäkerhet inom företag (Dutta & Roy, 2008), då de överlag har en stor mängd konfidentiell information. Siponen (2000) påpekar att graden av medvetenhet bland anställda kan påverka hur informationssäkerhetsteknik används och om medvetenheten är låg kan teknik missbrukas och därefter förlora sin mening. Om företag ser till att deras anställda har hög medvetenheten, genom att exempelvis hålla obligatoriska säkerhetskurser, minskas riskerna för sårbarhet och användarrelaterade fel.

[2] *Cambridge Online Dictionary*, 'security'. http://dictionary.cambridge.org/dictionary/english/security (hämtad 2016-03-31).

Grunden till informationssäkerhet är tre komponenter som tillsammans utgör CIA-triaden (Confidentiality, Integrity och Availability). Triaden och dess komponenters syfte är att uppnå säker användning, flöde och lagring av information inom organisationer, men principen har visat sig ha en del begränsningar. Dhillon & Backhouse (2000) beskriver CIA-triadens begränsningar som endast applicerbart på teknisk säkerhet vilket leder oss till att undersöka både tekniska och strategiska säkerhetsproblem inom CIA-triadens ramar.

1.1 Problemställning & frågeställning

Som tidigare nämnt har företag en tendens att spendera en stor del av säkerhetsresurserna på teknisk säkerhet, snarare än strategisk säkerhet. Anledningen till detta är att säkerhet oftast relateras till som en del av en teknisk lösning, vilket innebär att vikten som läggs vid strategisk säkerhet inte är lika tung som den bör vara. Detta skapar en sårbarhet hos företag för externa attacker, eftersom deras interna organisation inte är tillräckligt undervisad om vikten av säkerhet och riskerna som kan uppstå baserad på deras beteende i relation till säkerhet.

Ett exempel på hur säkerhet påverkar alla delar av kedjan mellan tillhandahållandet, implementering, distribuering, administrering och slutanvändning är fallet med säkerhetsläckan i betalfunktionen Swish, ett samarbete mellan Sveriges sex största banker där användare enkelt kan överföra pengar genom att ange varandras mobiltelefonnummer. Bloggen Nullbyte gjorde en undersökning om vad för sorts information som kunde extraheras om koden undersöktes, vilket resulterade i avslöjandet om att hela transaktionshistoriken, inklusive summan och mottagare, för en användare kunde extraheras på ett enkelt sätt (Nullbyte, 2014). Detta verkliga exempel visar hur lätt människor förlitar sig på att den tekniska säkerheten fungerar utan att ha uppmärksammat den strategiska säkerheten.

Utgångspunkten i undersökningen kommer att vara CIA-triaden och hur de olika komponenterna tillämpas hos företag. Detta eftersom det är en vedertagen metod för att säkerställa säkerhet, som bland annat finns med i informationssäkerhetstandarden ISO/IEC 27002, publicerad av International Organization for Standardization (ISO) och the International Electrotechnical Commission (IEC), vid namn *Information technology – Security techniques – Code of practice for information security management*.[3] Eftersom CIA-triaden alltjämt anses vara en standard inom informationssäkerhet och rekommenderas, kommer empirin inte att ta i beaktande några andra modeller eller påbyggnadsmodeller än just CIA-triaden, då vi vill undersöka om det finns några problem med standarden och basen till de andra modellerna.

Nytt kunskapsbidrag
I uppsatsen utförs en undersökning som kan beskrivas som en undersökning i tre lager, vad gäller informationssäkerhet. Företagen som undersöks har alla olika funktioner i kedjan informationssäkerhet där undersökningen kommer fokusera på CIA-triadens komponenter och hur dessa appliceras hos de olika lagren inom informationssäkerhet. Undersökningen ämnar att skapa en lupp för att kunna undersöka samtliga lager med. Uppsatsen gör också skillnad på teknisk och strategisk säkerhet, där utgångspunkten, hämtad från tidigare litteratur, är att det

[3] *IsecT Ltd. (n.d.).* ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls (second edition). http://www.iso27001security.com/html/27002.html (hämtad 2016-05-16).

generellt läggs mer resurser på den tekniska biten. Vi använder oss utav både det strategiska och det tekniska perspektivet då vi undersöker komponenterna i CIA-triaden, där fokus läggs på att undersöka och förstå samband vad gäller den strategiska aspekten.

För att undersöka hur informationssäkerhet påverkas inom företag har en frågeställning tagits fram och lyder följande:

Hur arbetar företag med komponenterna inom CIA-triaden och hur påverkar mänskliga faktorer detta?

1.2 Syfte

Uppsatsen ämnar undersöka hur välinformerade anställda är om säkerhet inom respektive företag och hur företag arbetar med säkerhet. Undersökningen kommer att resultera i en jämförelse av användningen av informationssäkerhet mellan tre olika företag, och om graden av deras säkerhet har något med appliceringen av CIA-triadens komponenter på verksamheten att göra, för att säkerställa hög grad av informationssäkerhet. I empirin kommer tre utvalda företag att delta vars användarspektrum av säkerhet är inom levererandet, administrerandet och slutanvändandet.

1.3 Avgränsningar

För denna uppsats finns det två avgränsningar som är viktiga och bör övervägas. För det första kommer uppsatsen att avgränsas till informationssäkerheten inom tre undersökta företag och kommer således inte att beakta informationssäkerhet utanför företagsområdet. Urvalet av företag är begränsat till tre stycken för att få en så rik och detaljerad uppfattning om hur företag med olika fokusområden hanterar säkerhet, då detta kan anses vara en vital del i deras affärsutveckling.

För det andra kommer vi att avgränsa vår studie utifrån CIA-triadens teori. Trots att vi har undersökt ett flertal olika teoretiska perspektiv som fokuserar på anställdas säkerhetskunskap och beteenden inom organisationer, finner vi att CIA-perspektivet kan ha hamnat i skymundan och blivit förbisett. Vi anser att CIA-perspektivet har möjlighet att bringa jämvikt mellan det tekniska- och strategiska säkerhetsarbetet och kommer därför avgränsa vår studie till att utgå från just CIA som teori.

1.4 Uppsatsens översikt

Kapitel 1 presenterar bakgrunden till frågeställningen med fokus på teknisk och strategisk säkerhet samt betydelsen för säkerhet. Här ingår syftet med undersökningen och de avgränsningar som har bestämts för att skala ner problemområdet.

Kapitel 2 presenterar ett teoretiskt ramverk, utifrån CIA-triaden, som introducerar en litteraturstudie. Studien ämnar granska tidigare verk inom informationssäkerhet och den utvalda teorin

som senare kommer att användas som referensram till den empiriska studien. I kapitlet introduceras även ytterligare modeller till informationssäkerhet, som inte kommer att användas i studien men som expanderar CIA-triaden.

Kapitel 3 presenterar metoder och tillvägagångssätt som den empiriska studien kommer att innehålla för att utföra undersökningen. I detta kapitel presenteras även de tre utvalda företagen och hur de sammankopplas i relation till deras arbetsinriktning och användning av program.

Kapitel 4 presenterar resultaten från den utförda empirin, vilket består av nio stycken intervjuer utförda på tre olika företag inom olika affärsområden. Kapitlet tar upp olika faktorer som uppstår samt hur företagen arbetar inom varje komponent.

Kapitel 5 presenterar en diskussion av resultaten med kopplingar till det teoretiska ramverket. Diskussionen innehåller likheter och skillnader som finns mellan de olika företagen i samband till CIA-triadens komponenter och förekommande mänskliga faktorer.

Kapitel 6 presenterar en slutsats där författarna presenterar vad de kommit fram till för att sedan svara på frågeställningen. Slutsatsen inkluderar även hur undersökningen kan utvecklas i framtida verk.

2 Teoretiskt ramverk

Tidigare forskning visar att beteendet inom organisationer, både sett till hela organisationen och individuellt, har en väsentlig faktor vad gäller säkerhet (Stanton m.fl., (2004), Siponen (2000) och Hedström, Kolkowska, Karlsson & Allen (2011)). Vår litteraturstudie fokuserar på studier som forskar kring säkerhet med fokus på mänskliga beteenden inom verksamheter samt sambandet mellan CIA-triadens komponenter. I relation till CIA-triaden har ingen av de följande studierna utforskat hur triaden appliceras i organisationer, men komponenterna analyseras med utgångspunkt i deras samverkan. Stanton m.fl. (2004) studie har komponenterna i åtanke för att se om de påverkas enskilt av individerna inom organisationen, men resultatet fokuserar inte på detta. Tillskillnad från studierna ämnar uppsatsens studie handskas med företags grad av informationssäkerhet genom anställdas säkerhetsmedvetande och om komponenterna inom CIA-triaden har någon applicering inom företagens säkerhet.

2.1 Litteraturstudie

Stanton (2004)
En studie utförd av Stanton m.fl. (2004) undersöker hur de tre komponenterna inom informationssäkerhet – confidentiality, integrity och availability – påverkas av slutanvändare, genom deras beteende och motivation gentemot mot säkerhet. På grund av mänskliga beteende skriver Stanton (2004) att det har uppstått begränsningar inom användandet av tekniska lösningar. Stanton m.fl. (2004) påpekar att säkerhetens framgång inom informationssystem beror på de inblandande individernas, och deras effektiva beteende vid, användning.

Studien innefattar två separata enkätstudier där den ena fokuserar på organisatoriska faktorer inom säkerhet och den andra fokuserar på individuella faktorer. Inför studierna skickades skilda enkäter ut till individer; i den första studien skickades 4000 enkäter ut, men endast 1167 av dessa var användbara. I den andra studien skickades 800 enkäter ut inom organisationen Study-Response, varav 298 gick att använda. Enkäterna visade resultatet: “[...] Organisationens typ, jobbroll, trivsel och organisatoriskt engagemang påverkade säkerhetsbeteendet hos slutanvändarna” (Stanton, m.fl., 2004). Ju högre inkomst, bättre arbetsroll och engagemang inom organisationen, desto högre medvetenhet inom säkerhet hade individerna.

En begränsning som studien har är att beteendet överlag inte är applicerbart på alla typer av verksamheter. Istället skulle ett teoretiskt perspektiv, som beaktar vikten av beteende inom specifika situationer som uppstår i särskilda organisationer (regeringen, militären och finansiella sektorn), granskas för hur de betonar säkerhet. Denna uppsats skiljer sig från artikeln genom att Stanton m.fl. (2004) slutsats inte fokuserade nämnvärt på CIA-triadens komponenter. Istället fokuserade resultatet mer på hur särskilda beteenden påverkade säkerheten utifrån graden av position och arbetsroll individer har inom organisationer.

Wilson (2013)
Wilsons (2013) studie fokuserar på att analysera hur de fem benen inom informationssäkerhet ibland kan ha svårt att samarbeta; tillgänglighet, integritet, autentisering, konfidentialitet och oavvislighet. Vid förbättring av ett ben, kan behovet hos ett annat ben glömmas bort. Författaren

visar grafiskt hur detta kan gå till. Till exempel kan tillgänglighet skapa konflikter med konfidentialitet, integritet och autentisering, medan konfidentialitet och integritet ofta inte har några problem att samarbeta.

Artikeln kan vara ett bra komplement till vår studie då den kan hjälpa till att förklara varför vissa ben i CIA-triaden ibland är starkare än andra.

Siponen (2000)
Siponen (2000) verkställde en konceptuell analys av säkerhetsmedvetande inom verksamheter som innehåller olika teorier och riktlinjer, vilka fokuserar på att förstå mänskliga beteenden. Teorierna som undersöks är allt från normativa och strikta riktlinjer till användarnas motivation och attityd mot acceptans av teknik. Författaren nämner att när användare har introducerats till medvetenhet, finns det olika stadier av medvetenhet som människors sinnen fastnar på. Dessa stadier kan medföra komplikationer om flera användare är vid olika stadier i en verksamhet, eftersom det påverkar framgången eller misslyckandet av säkerhetsmedvetenhet, genom utveckling eller regression (Siponen, 2000). Artikeln fokuserar endast på olika aspekter av medvetenhet för att skapa en grund och ett ramverk för framtidsforskning då artikeln inte innehåller en empirisk studie.

I relation till vår studie är artikeln utanför vårt fokusområde men har intressanta teorier angående mänskliga beteende mot medvetenhet. Eftersom en begränsning av artikeln är att det inte finns någon empirisk studie är det svårt att avgöra hur teorierna står sig i praktiken.

Hedström (2011)
Ett företags information är en av de viktigaste tillgångar som finns, och skyddandet av detta är i högsta grad en strategisk punkt (Hedström, m.fl., 2011). Författarna undersöker spänningarna som kan uppstå mellan säkerhetspolicys och hur det praktiskt går till genom case-undersökningar hos två sjukvårdsinstitut. Traditionellt hanteras informationssäkerhet utifrån en *Control-based Compliance Model*, som menar att mänskliga beteenden bör kontrolleras och regleras (Hedström m.fl., 2011). Istället för att använda en kontrollbaserad metod, introducerar författarna en annan typ av teoretisk modell: *Value-based Compliance Model*.

Författarna beskriver att målet med den nya modellen är att se till att åtgärdsstrategier och mål anpassas efter aktuella situationer, genom att tillåta värderingarna en aktör har bestämma vilka åtgärder som bör prioriteras i konflikter. Vad gäller organisatoriska åtgärder används olika former av rationalitet parallellt vilket kan orsaka potentiella värdekonflikter och ge strategiska konsekvenser inom hanteringen av informationssäkerhet (Hedström m.fl., 2011). Med hjälp av modellen anser författarna att sjukvårdsinstitutionerna kan hantera sina vårdsituationer och informationssäkerhet på ett mer effektivt sätt, genom att identifiera nuvarande värdekonflikter och omvärdera deras prioritet.

Artikeln introducerar en annorlunda princip att utgå från vad gäller säkerhetspolicys och hur folk beter sig. Här har ett case undersökt, dock på två olika sjukvårdsinstitut, och vi kommer undersöka andra sorters företag. Vår metod kommer bygga på intervjuer, i stället för som i detta fall - ett case.

Dhillon & Backhouse (2000)
En artikel skriven av Dhillon & Backhouse (2000) fokuserar på förståelsen av informationssystem i det nya milleniet och föreslår sin utvecklade princip RITE (Responsibility, Integrity, Trust och Ethicality), som hjälpmedel för hanteringen av informationssäkerhet. Precis som

CIA-triaden nämner författarna att komponenterna i RITE är "av stor vikt och första stegen till att säkra organisationers information i framtiden" (Dhillon & Backhouse, 2000).

Utveckling av teknik växer i en snabb takt, och företag måste se till att verksamheten håller samma takt vad gäller strategiska säkerheten, såväl som den tekniska säkerheten. Skillnaden mellan triaden och RITE är att funktionerna i CIA begränsas till information som refereras till "data" inom system och RITE inriktar på organisatoriska sammanhang där data används och tolkas. Efter en genomgång av varje komponents funktion, sammanfattar Dhillon & Backhouse att utöver CIA-triaden kan ökad informationssäkerhet uppnås genom att implementera RITE.

Artikelns innehåll är ett komplement till uppsatsen då den introducerar nya principer som påverkar mänskliga och sociala utföranden i verksamheter, i form av säkerhet. Eftersom uppsatsen kommer att fokusera på CIA-triaden är det väsentligt för författarna av uppsatsen att vara medvetna om andra möjliga riktlinjer som stärker informationssäkerhet, samt ha det i åtanke.

Warkentin & Willison (2009)
Warkentin & Willison (2009) belyser med en litteraturstudie "the insider threat" - hotet inifrån. Attacker från utsidan kan orsaka stor skada, men det är på insidan, vare sig det är medvetet eller inte, som det största hotet finns. Slutanvändaren, som är en "trusted agent" inom organisationen med inloggningsuppgifter och tillgång till systemet, kan orsaka skada på de tre komponenterna inom CIA-triaden.

Artikeln tar upp en rapport gjord av Ernst & Young från 2008 där en undersökning visar att medvetenhet och personalfrågor är det största hindret mot att leverera framgångsrik informationssäkerhet. Rapporten tar också upp att endast 19% av arbetsgivare testar beteendet hos de anställda i förhållande till säkerhet, medan 85% testar sin internetsäkerhet.

Författarna argumenterar för att större vikt bör läggas vid anställning, utbildning och motivation, vilket säkert kommer generera utdelning. Författarna ställer sig även frågan varför vissa anställda väljer att följa uppsatta säkerhetspolicys, och andra inte, och hur detta bör tacklas.

Nedan följer en tabell som sammanfattar alla artiklar och dess inriktning.

Författare (Datum)	**Kontext**	**Metod**	**Beskrivning**	**Teori**
Al-Hamdani (2009) (Använd i 2.3.1 Andra modeller)	Anställda/ Verksamhet	Undersökning av gällandes standard inom informationssäkerhet	Författaren argumenterar för att gällande standard, CIA-triaden, inte räcker till som säkerställare av säkerhet utan undersöker vad för tillägg som kan göras.	Diligence Model
Dhillon & Backhouse (2000)	Anställda/ Verksamhet	N/A	Inför det nya millenniet, introduceras principen RITE som anses vara ett tillägg till CIA-triaden för att uppnå både strategisk och teknisk säkerhet.	N/A

Hedström m.fl., (2011)	Anställda/ Verksamhet	Fältstudie: uppgifter samlas in via intervjuer, dokument och iakttagelser.	Undersöker två sjukvårdsinstitut och de spänningarna som kan uppstå mellan säkerhetspolicys och hur det praktiskt går till. Resultatet visar att sjukvårdsinstitutionerna kan hanteras på ett bättre sätt med den givna teoretiska modellen.	Value-based compliance model
Layton Sr, (2005) (Använd i 2.3.1 Andra modeller)	Anställda/ Verksamhet	Analys av tidigare forskning utmynnande i egen modell	Författaren undersöker sex nyckelaspekter vad gäller mänskligt beteende och diskuterar hur dessa relaterar till, och påverkar, informationssäkerhetsprogram. Undersökningen utmynnar i en egen modell, kallad POST.	POST
Siponen (2000)	Anställda/ Verksamhet	Konceptuell analys	Konstruerar en grund för systemsäkerhetsmedvetande genom att analysera mänskliga beteenden utifrån teorier. Föreslår en övertalningsstrategi för att öka användares engagemang till användningen av säkerhetsriktlinjer.	Beteendevetenskapligt ramverk; Teori om planerat beteende, Teknisk acceptansmodell
Stanton m.fl., (2004)	Anställda/ Verksamhet	Fältstudie: uppgifter samlas in via enkäter.	Undersöker anställdas beteende och motivation mot säkerhet och ifall triadens komponenter berörs i beteendet. Resultatet visar att ju bättre jobb, roll, inkomst och engagemang i organisationen, desto högre medvetenhet och bättre beteende har användaren mot säkerhet.	Organizational Citizenship Behavior (OCB), Counterproductive Workplace Behavior (CWB)
Warkentin & Willison (2009)	Anställda	Analys av tidigare skrivna artiklar	Undersöker och förklarar varför ”endpoint”- användarna i ett system är de som utgör det största hotet mot säkerheten. Artikeln fokuserar på användarnas beteende och tar upp hur	N/A

			”insider threats” kan tacklas.	
Wilson (2013)	Verksamhet	N/A	Undersöker interaktionen mellan ”fem ben” inom informationssäkerhet och vad som händer om ett ben prioriteras mer över ett annat. Resulterar i att förståelsen för alla ben och dess interaktion med varandra kan hjälpa företag att analysera existerande informationssäkerhet och eventuella brister.	N/A

Tabell 2.1 Sammanfattning av strategisk och teknisk säkerhetslittaratur.

Sammanfattningsvis kan det konstateras att CIA-triaden tidigare i större utsträckning har applicerats på den tekniska sidan av CIA. Vår undersökning kommer fokusera på den strategiska sidan av säkerhet i samband med applicerandet av CIA-triadens komponenter. Vår undersökning är vidare en tre-lagersstudie som undersöker tre olika typer av företag, som alla finns i kedjan informationssäkerhet.

2.2 CIA-triad

CIA-triaden, en erkänd teori som används inom informationssäkerhet, innehåller tre komponenter; confidentiality, integrity och availability. Dessa komponenter anses vara grunden för alla säkerhetsprogram, då de är sammankopplade genom idén om informationssäkerhet (Wylder, 2003). Idén om information beskrivs av Wylder (2003) som en tillgång som kräver skydd och är grundläggande för att förstå CIA-begreppen. Denna teori kommer att vara en central och vital del i undersökningen, då den kan hjälpa att avgöra var i företagets säkerhet det finns brister och om det är mänskliga faktorer som påverkar den.

2.2.1 Confidentiality

Den första komponenten inom informationssäkerhet, confidentiality (konfidentialitet), beskrivs av Wylder (2003) som att förhindra att göra information tillgänglig för obehöriga. Konfidentialitet är nära besläktad med sekretess, och data kräver en adekvat design som förhindrar tillgången till känslig information för obehöriga, men som samtidigt tillåter åtkomst för behöriga. Data kan kategoriseras efter både mängden och typen av skada som kan inträffa vilket avgör graden av konfidentialitet och säkerhet data är i behov av.

För att säkerställa konfidentialiteten av data rekommenderas det att företag har följande: nätverkssäkerhetsprotokoll, nätverksautentiseringstjänst och krypteringstjänster (Agarwal & Agarwal, 2011). Inom företag rekommenderas anställda att ha svårgissade inloggningsuppgifter, med fokus på lösenordet, och gå en säkerhetskurs. En säkerhetskurs kan ingå i anställdas

arbete för att se till att de är medvetna om säkerhetsrisker och hot som kan påverka dem och företaget, om intern information läcks ut.

2.2.2 Integrity

Den andra komponenten i triaden är integrity (integritet) vilket fokuserar på att "upprätthålla korrekt och fullständig information som inte har ändrats av obehöriga användare eller processer" (Wylder, 2003). Det viktiga i denna komponent är att se till att data inte kan ändras av obehöriga användare när den överförs, och om ändringar har skett från obehöriga bör det finnas en backup för att kunna återställa data.

För att kontrollera detta bör det finnas åtkomstkontroll och rättigheter till viss data. Det är viktigt för användare med tillgång att inte felanvända data, då det är en stor risk för skadegörelse och påverkar integritet. Agarwal & Agarwal (2011) nämner intrångsdetektering, brandväggar och kommunikationssäkerhet som säkerhetsställare för integritet. I vissa fall kan intrångsdetektering vara nödvändigt där datasäkerheten kan känna av ändringar i data från elektromagnetiska pulser (EMP) för att motstå permanent data- och mjukvarufel.

2.2.3 Availability

Den sista komponenten, availability (tillgänglighet), fokuserar på att se till att användarna har aktuell och tillförlitlig tillgång till information (Wylder, 2003). För att användare ska komma åt information måste tre komponenter fungera och vara sammankopplade: kommunikationskanaler för tillgång, säkerhetskontrollerna som skyddar informationen och datasystemet som lagrar informationen (Agarwal & Agarwal, 2011). För att säkerställa tillgänglighet bör företag konstant upprätthålla nätverkssäkerhet och hårdvara med uppdateringar och utföra reparationer när det är i behov.

Phoenix TS är ett träningscenter som erbjuder säkerhetscertifiering till företag via deras säkerhetsutbildningar. En av dessa certifieringar är CISSP där Phoenix TS förklarar, i en av deras video:n *CIA Triad (Security Triad) - CISSP Training Series*, de olika kontrollstegen för implementationen av CIA-triaden. Enligt Phoenix TS (2012) är dessa administrativa, tekniska och fysiska kontroller.

- Administrativa kontroller fokuserar på att skapa säkerhetspolicys som anställda ska följa och vara medvetna om.

- Tekniska kontroller fokuserar på att implementera brandväggar, datakryptering och behörighet i system.

- Fysiska kontroller fokuserar på fysiska föremål som höger säkerhetsgraden så som accesskort, vakter, nycklar och höga murar för att hindra utomstående inträde.

2.2.4 Annan aspekt

CIA-triadens komponenter fokuserar enligt Gollmann (2011) på förebyggandet av ovälkomna händelser. Problem kommer att uppstå hur bra det förebyggande arbetet än ser ut. Därför argumenterar Gollmann för att man kan utöka CIA-triaden med ytterligare säkerhetskrav. Gollmann föreslår bland annat *Accountability* som ett extra tillägg. *Accountability*, eller ansvar, ser till behovet att någon bör hållas ansvarig om säkerheten inom ett företag bryts.

> *"**Accountability** – Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party."*
> *Gollmann (2011)*

För att kunna utföra denna aspekt krävs det att man kan identifiera och autentisera användare, och till detta bör en logg hållas över beslut som fattas i systemet.

2.3 RITE

Vid granskning av tidigare litteratur låg RITE närmst CIA som alternativ informationssäkerhetsmodell, eller utökad modell. Vid undersökningar av tidigare författade artiklar var det denna modell som stöttes på mest frekvent. Tidigare nämnt utvecklade Dhillon & Backhouse (2000) RITE, vars funktionalitet skulle agera som ett hjälpmedel vid tillämpningen av CIA-triaden inom verksamheter för att utöka säkerhet. Utsett att funktionen av CIA är ett säkerhetsspråk som ger en överenskommelse mellan industri och vetenskap genom riktlinjer, har Dhillon & Backhouse (2000) iakttagit nackdelar med CIA inom det strategiska perspektivet. Genom att införa RITE, som fokuserar på det strategiska perspektivet, trodde författarna att nackdelarna skulle elimineras och där med komplettera säkerheten.

Principen har funnits innan tilliten till teknik förekom (Dhillon, 2001, p. 176), och vikten att inkludera helheten av komponenterna och dess funktionalitet är stor, då Dhillon & Backhouse (2000) påpekar att det är de första stegen mot informationssäkerhet. Även om principen inte kommer att användas inom ramverket för intervjuerna, anses komponenterna vara värdefulla då de fokuserar på mänskliga och sociala utföranden, vilket kan förekomma hos informanterna. Principen innehåller fyra komponenter som används för organisatoriska sammanhang inom säkerhet vilket Dhillon & Backhouse (2000) nämner i sin artikel.

Responsibility
Den första komponenten, responsibility (ansvar), inriktar sig på förståelsen av ens roll i en verksamhet och det ansvar som tillkommer med rollen (Dhillon & Backhouse, 2000). Här är det viktigt att veta hur brett ens ansvarsområde är när fel uppstår i en verksamhet, och för anställda att stå till svars för händelser inom deras ansvarsområden.

Integrity
Den andra komponenten, integrity (integritet), beskrivs av Dhillon & Backhouse (2000) som en anställds integritet inom en verksamhet. Eftersom information inom företag är av störst vikt är det viktigt för företag att veta vilka människor som har tillgångar till viss information och möjligheterna för dem att bryta integriteten.

Trust
Den tredje komponenten, trust (förtroende), fokuserar på ett företags förtroende till sina anställda som en form av kontroll när alla medarbetare i en stor organisation inte kan övervakas samtidigt.

Ethicality
Den sista komponenten, ethicality (etik), inriktar sig på medarbetares "agerande i enlighet med etiska metoder" (Dhillon & Backhouse, 2000). Detta agerande är inte regler inom företag, utan anses vara informella normer och beteenden som förväntas av anställda.

Varför används inte RITE?
Anledningen till att RITE inte kommer att sammanfogas med CIA-triaden i vår undersökning, är att principen endast är en förlängning med ett begränsat antal nuvarande studier. Eftersom uppsatsen kommer att fokusera på säkerhetsgrunden (C, I och A) och spekulationerna kring deras funktionalitet, kommer RITE principen inte att användas inom ramverket för intervjuerna.

2.3.1 Andra modeller

Utöver RITE finns det ett antal andra modeller som förlänger CIA så som POST, Value-based Compliance Model och Diligence Model.

2.3.1.1 POST
Psychology of Security & Technology, POST, identifierar ett psykologibaserat ramverk utifrån sex olika komponenter som underlättar för informationssäkerhetschefer (Layton Sr, 2005). De sex komponenterna är följande; motivation, attityd, övertygelser, personlighet, moral och etik.

POST går ut på att utifrån dessa sex komponenter skapa sin en större förståelse för hur användare i ett informationssystem agerar, men framförallt varför de agerar som de gör. Det här är viktigt att ta reda på då en organisation vill röra sig mot en större acceptans av riktlinjer och policys. När de sex komponenterna analyseras tillsammans utgör de en grund för att utvärdera organisationen på ett nytt sätt. Eftersom en direkt fråga av en chef till en underordnad, gällande om de exempelvis följer policys eller ej, ofta får ett övervägande jakande svar, kan POST erbjuda ett sätt att komma runt detta. POST har användaren i centrum och bygger på tron att människor i system är den främsta källan till framgång.

2.3.1.2 Value-based Compliance Model
Modellen utvecklades av Hedström m.fl. (2011) utifrån en aktörs förmåga att agera utifrån sina värderingar inom en organisation. Genom att respektera aktörers värderingar inom organisationer där värderingar inte alltid delas, agerar modellen som grund till professionell "på platsreflektion" som kan förbättra en organisations informationssäkerhet. Genom modellen anpassas en organisations mål efter aktuella konflikter där olika aktörers värderingar bestämmer vilka värderingar som ska prioriteras.

Syftet med Value-based Compliance Model är att kunna hantera spänningar mellan informationssäkerhetspolicys genom att identifiera värdekonflikter som uppstår inom organisationer. Genom att tillämpa modellen kan en identifiering av värdekonflikter avslöja vad som orsakar problem inom informationssäkerhet, som oftast pekar på mänskliga beteende. Utifrån konflikterna kan organisationer genomgå interna ändringar för att förbättra och undvika framtida säkerhetsproblem.

2.3.1.3 Diligence Model

Al-Hamdani (2009) presenterar idén om att CIA-triaden inte alltid räcker till som bevarare av säkerhet, utan argumenterar för att det finns utrymme till tillägg till denna. Författaren presenterar "The Diligence Approach" som löser problem som kan uppstå med endast CIA genom att utöka den. Ett exempel på detta är när information uppfyller alla krav i CIA, men ändå inte kan användas. Al-Hamdani ger exemplet då en laptop blir stulen och informationen är konfidentiell, integriteten finns kvar då informationen inte har ändrats och informationen är tillgänglig att användas, användaren innehar dock inte laptoppen. I det fallet gäller inte den traditionella CIA-triaden.

För att tackla detta adderar "The Diligence Model" tre extra element, vilka är; utility (användbarhet), possession or control (innehav eller styrning) samt authenticity (autenticitet). Dessa element är tillagda för att hantera händelser som kan uppstå i vardagen då en användare arbetar med informationssäkerhet.

Varför används inte dessa modeller?

Anledningen för att inkludera dessa modeller var för att utöka kunskapen om ytterligare teorier som presenterar tillägg till komponenterna inom CIA. Dock existerar det redan problem med teorin som ligger till bas för utökningen – CIA-triaden – och därför anser vi att en undersökning som har endast CIA som grund har en större relevans, då det är nödvändigt att undersöka problem som kan uppstå i grunden innan fokus läggs på ytterligare tillägg.

3 Metod

I början av arbetet utformades en frågeställning som tillsammans med avgränsningar skapade en inriktning. Att utföra avgränsningar är nödvändigt för att kunna genomföra en empirisk undersökning då avgränsningar visar vad undersökningen inriktar sig på och vilka saker som kommer att bortses ifrån (Jacobsen, 2002). För att utöka och fördjupa den erhållna kunskapen inom det utvalda undersökningsområdet utfördes en litteraturstudie som fokuserade på tidigare forskning inom informationssäkerhet. Litteraturstudien grundades utifrån tidigare skrivna artiklar som undersöker och diskuterar säkerhet, CIA-triaden samt strategisk säkerhet vilket är vad den empiriska undersökningen kommer att innehålla.

Den typ av undersökningsmetod som har valts ut för insamling av empiri är utifrån en kvalitativ ansats vilket fokuserar på individuella intervjuer. Denna typ av metodval grundades från typen av problemställning och var mest lämplig för att se ett samband mellan individ och kontext (Jacobsen, 2002). Eftersom valet av insamlingsmetod kan påverka validiteten av data, måste utformningen av intervjufrågorna vara noga för att se till att undvika ledande frågor. Utifrån tre utvalda företag blev tre personer som arbetar inom respektive företag individuellt intervjuade, totalt nio intervjuer skedde alltså. Undersökningen innehöll informanter som har olika ansvarsområden, där två av dem arbetar med utveckling och resten endast är användare i systemet. Intervjufrågorna inriktades på hur de arbetar med IT-säkerhet från ett tekniskt och strategiskt perspektiv, och deras egna perspektiv på hur de ser på IT-säkerhet. Intervjuerna användes som grund till diskussionen om huruvida synen på strategisk säkerhet skiljer sig mellan olika typer av företag.

3.1 Urval av företag

För att undersöka hur företag behandlar säkerhet (både tekniskt och strategiskt) inom deras verksamhet intervjuades tre företag. Ett krav vid urvalet av företagen var att deras belägenhet var i Sverige och att de hade starka kopplingar till säkerhet, oavsett typ. På grund av att de utvalda företagen vill förbli anonyma kommer de refereras till som: Företag A, Företag B, Företag C. Företagsinformationen är sekundär data hämtad från respektive företags hemsida.

3.1.1 Företag A

Företag A arbetar internationellt inom affärssystem i form av mjukvarurelaterade tjänster och tillverkningen av mjukvara. Företaget är känt för deras system inom Enterprise Recource Planning (ERP), Customer Relationship Management (CRM) och Supply Chain Management (SCM) med hög kvalité, men erbjuder även säkerhetssystem till deras kunder. Baserat på deras börsvärde har företaget blivit en av världens topp tre största programvarutillverkare.

Valet att inkludera Företag A i den empiriska studien är på grund av deras stora framgång inom deras arbetsinriktning, tillverkningen och försäljningen av mjukvara, till en mångfald av kunder och användare runt om i världen. Företagets produkter är tillverkade för att hjälpa kunder att driva deras verksamhet på ett mer effektivt sätt, vilket innebär att alla produkter erhåller någon form av säkerhet. Denna typ av säkerhet är inte vad intervjuerna kommer att fokusera kring, utan istället är det den interna säkerheten som anställda måste vara medvetna om för att det

förtaget ska undvika externa attacker. I dagsläget finns det inget publicerat angående företagets syn på säkerhet vilket är varför de är en intressant kandidat för studien. Med tanke på storleken av både företaget och deras framgång, bör de ha hög medvetenhet angående både teknisk och strategisk säkerhet.

3.1.2 Företag B

Företag B arbetar inom Sveriges finansiella sektor där de riktar sig till både privatpersoner och företag samt har konstant fokus på ständig tillväxt. Företaget erbjuder finansiell rådgivning i Sverige och runt om i Europa där de satsar på en totallösning för företagskunder.

För en bank är informationssäkerhet otroligt viktig och vikten av beteendet mot detta bör vara större som Stanton m.fl. (2004) nämner och annorlunda till skillnad från Företag A och Företag C, vilket är varför de har valts ut till undersökningen. Bankverksamhet bygger på tillit och existerar inte detta har banken svårt att överleva. På deras hemsida ger Företag B råd och tips till kunder om hur de bör bete sig när de använder systemet, på exempelvis publika datorer.

3.1.3 Företag C

Med visionen att skapa det ledande IT-konsultföretaget i Sverige, arbetar Företag C med systemutveckling och applikationssäkerhet för kunder runt om i landet. Inom deras kunderbjudan ingår det konsulttjänster och säkerhet, med fokus på IT-infrastruktur, säkra informationshantering- och användarapplikationer.

Anledningen till att företaget har valts ut för studien är på grund av deras starka relation till säkerhet då det är en stor del av deras arbete. Inom deras kunderbjudan ingår det utbildningar inom säkerhet och rådgivning. Då företaget kan utbilda deras kunder inom säkerhet kan det tyda på att företagets interna medvetenhet om säkerhet ligger på samma eller även en mer avancerad utbildningsnivå.

3.1.4 Sammankoppling av företag

De utvalda företagen kan sammankopplas ur ett teoretiskt perspektiv i form av arbetsinriktning. Sammankoppling mellan företagens tjänster och användningen av respektive program kan visuellt beskrivas i figur 3.1, där pilarna visar riktningen av tjänster som erbjuds av företag till kund. Företagen kan sättas in i två olika nivåer: säljare och användare, som förespråkar företagens roll i sammankopplingen. Företag C placeras högst upp under säljare då företaget erbjuder applikationssäkerhetstjänster till kunder så som både Företag A och Företag B för antigen intern användning (Företag A) eller extern användning (Företag B).

Utifrån perspektivet skulle Företag A placeras under både säljare och användare då teoretiskt sett kan de ha intern användning av Företag C:s program för att tillverka egna program, men också agera som säljare då de säljer deras program till kunder som Företag B.

Företag B placeras under användare då de i sin tur använder Företag A:s eller Företag C:s program för att erbjuda kunder, vanliga människor, finansiella tjänster.

Figur 3.1 Visuell beskrivning av företagens sammankoppling ur ett teoretiskt perspektiv.

3.1.5 Säkerhetsrelation mellan inom företagen

I relation till säkerhet skiljer det något mellan företagen. Företag B, som kund hos Företag A och Företag C, lägger sin tillit på mjukvaruprogrammets säkerhet som företaget själv erbjuder via deras tjänster till deras kunder. Om något skulle hända Företag B:s kunder, exempelvis identitetsstöld eller externa attacker på kunders bankkonton, skulle kunderna klandra företaget som företag för bristen på säkerhet. Hursomhelst hade Företag B, som kund hos Företag A och Företag C, klandrat på systemets säkerhet på grund av framgångsrika externa attacker. Om företaget skulle attackeras av externa parter som påverkade deras kunder hade de förlorat tilliten hos tusentals kunder och fått ett dåligt rykte.

Ur Företag A och Företag B:s synvinkel som programutvecklare hade de nog inte tagit ansvar för externa attacker mot deras kunder eftersom det oftast inte är systemet det är fel på, utan användandet av systemet.

3.2 Urval av informanter

Enligt Jacobsen (2002) bör urvalsprocessen för informanter inom en kvalitativ ansats utgå ifrån den utvalda problemställningen. Ett krav för urvalsprocessen var att informanterna hade någon form av kontakt med säkerhet och IT inom deras arbete. För att se till att urvalsprocessen täckte undersökningens fokusområde, valdes informanter efter deras roller inom företagen.

- På Företag A intervjuades tre personer vars roller var maintenance sales manager, global account executive och local legal counsel.
- På Företag B intervjuades tre personer vars roller var kundansvarig, assistent och avdelningsansvarig.
- På Företag C intervjuades tre personer vars roller var projektledare/lösningsarkitekt, konsult/projektledare/systemutvecklare och utvecklare.

Den nedanstående tabellen sammanfattar informationen om de utvalda informanterna. I tabellen ingår det ett givet id-nummer för identifieringen av var och en i resultaten samt deras arbetsroll och åldersspann.

Företag	**Informant (*id-nummer)***	**Informant (*arbetsroll*[4]*, åldersspann)***
Företag A	I1	Global Account Executive, 50-60.
	I2	Maintenance Sales Manager, 50-60.
	I3	Local Legal Council, 30-40.
Företag B	I4	Kundansvarig, 50-60.
	I5	Assistent, 60-70.
	I6	Stiftelseansvarig, 60-70.
Företag C	I7	Konsultchef/Projektledare/Systemutvecklare, 40-50.
	I8	Projektledare/Lösningsarkitekt, 20-30.
	I9	Utvecklare, 20-30.

Tabell 3.1. Sammanfattning av utvalda informanter till undersökning.

3.3 Utformning av individuella intervjuer

Nedanför presenteras hur utformningen av de individuella intervjuerna utfördes med fokus på intervjuguiden och intervjufrågorna.

3.3.1 Utformning av intervjuguiden

Med individuella intervjuer som metod för datainsamling, skapades informationsdokument om undersökningens avsikt, och intervjuerna samt sekretessavtal. Eftersom Företag A arbetar internationellt och använder engelska som arbetsspråk behövde alla dokument översättas från svenska till engelska för att utföra intervjuerna på engelska. Översättningen av dokumenten och intervjufrågorna utfördes väldigt noga av författarna och skickades sedan till olika kontakter till författarna som har mycket goda engelskkunskaper för verifiering. Intervjufrågorna skickades till handledaren, som har expertis i intervjuer, för godkännande. Efter verifieringen och godkännandet skickades dessa dokument till informanterna för att få deras individuella samtycke till deltagandet i undersökningen.

[4] Arbetsrollerna är angivna på det språk som används inom organisationen.

Inom en kvalitativ ansats kan engångsintervjuer utföras, det vill säga att samma intervjufrågor upprepas till flera intervjuobjekt (Jacobsen, 2002). När utformningen av intervjuguiden ägde rum fokuserade vi på att skapa en öppen och strukturerad guide, eftersom avsikten med undersökningen är att intervjua ett fåtal anställda på tre olika företag. Genom en öppen och semistrukturerad intervju kommer den insamlade data hjälpa med att bredda jämförelse om deras uppfattningar om hur dem själva och företaget arbetar med säkerhet.

3.3.2 Utformning av intervjufrågor

Strukturingen av intervjufrågorna är en viktig aspekt att tänka på för att undvika redundant insamlingsdata och tidsslöseri. För att se till att tiden för intervjuerna hann samla in relevant data diskuterades intervjuernas tidslängd. Det är sällan klokt att ha intervjuer som är kortare än 30 minuter och längre än en timme (Jacobsen, 2002). Baserat på detta bestämdes det att tidslängden för intervjuerna var runt 40 minuter och intervjuguiden innehöll öppna, men till en viss grad, strukturerade frågor.

Jacobsen (2002) nämner vissa punkter att tänka på när en intervju och dess tillhörande frågor utförs. De individuella intervjufrågorna strukturerades ifrån Jacobsen (2002) följande punkter:

Inled med en översikt om intervjuns avsikt
Innan intervjufrågorna inleddes fick alla informanter information om intervjuns avsikt och fokusområde. Tidigare nämnt fick både företagen och informanterna information om undersökning där båda parter var tvungna att ge samtycke innan intervjuer bokades. När sekretessavtalen skickades ut till informanterna fick de möjligheten att få en kopia av intervjufrågorna för att förberedda sig.

Inled med allmänna frågor
Strukturen på intervjufrågorna inleddes med allmänna frågor om avdelningens och informantens roll på företaget, informantens syn på säkerhet och övrigt innehåll angående säkerhetsutbildning. Med allmänna frågor, där informanten alltid byttes ut, blev varje intervju annorlunda och det skapade en större bredd på den insamlade data.

Fördjupa ämnet och frågorna
Eftersom undersökningen fokuserade på komponenterna C, I och A på en teknisk och strategisk nivå, fördjupades frågorna efter ett tekniskt och strategiskt perspektiv. För varje komponent ställdes ett antal frågor som var endast relaterat till den komponenten. Valet att utföra frågorna på detta sätt var för att skapa en balans mellan de två perspektiven för att se vilket företag som är starkare i respektive komponent.

Efter att intervjufrågorna hade skapats på svenska behövde de översättas till engelska. För att se till att frågorna innehöll samma grad av detalj, översattes dem noggrant av författarna. Intervjuguiden till de individuella intervjuerna som genomfördes på alla tre företag finns under Bilaga 1.

3.4 Genomförande av individuella intervjuer

Under undersökningens gång utfördes det både personliga intervjuer och telefonintervjuer. Telefonintervjuerna utfördes för informanterna som inte var inom nära pendelavstånd vilket endast var från Företag A. Jacobsen (2002) påpekar att valet av plats för en intervju kan påverka hur människor uppträder, vare sig det är ett arbetsrum med lugn stämning eller ett café med hektiskt stämning. Med detta i tanke valdes platserna för de personliga intervjuerna med omsorg vilket hos Företag B och Företag C resulterade i ett enskilt mötesrum. Inför telefonintervjuerna valde både författarna och informanterna på Företag A på egen hand tysta omgivningar för att undvika högljudda distraktioner.

Innan de individuella intervjuerna tog plats, kontrollerades det att informanterna var informerade om undersökningens avsikt och intervjufrågorna. I de fallen där informanterna inte var informerade eller inte hade fått chansen att se över frågorna gavs det en kort presentation på vad som skulle utföras och varför, samt en stund att se över frågorna. Utöver introduktionen, beroende på typen av intervju som utfördes, signerade informanterna enskilda sekretessavtal som gav deras personliga samtycke för deltagande. I fallen där personliga intervjuer utfördes signerade informanterna avtalen innan intervjun började, och i fallen där telefonintervjuer utfördes skickades avtalen till informanterna för signering via e-mail.

Författarna hade en förbestämd roll när intervjuerna skulle börja: en intervjuade och en antecknade. När all pappersarbete var avklarat påbörjade intervjuerna där ljudupptagning och anteckningar användes. Båda metoderna utfördes för att senare kunna extrahera data från intervjuerna när de skulle transkriberas. Under intervjuerna följde författarna den intervjuguide som hade skapats noga men med diverse formuleringar beroende på informantens förståelse av frågan.

Inom intervjuer påpekar Jacobsen (2002) fördelen att gräva djupare i strukturerade frågor och ställa följdfrågor för att fördjupa svaren och möjligtvis besvara problemställningen. För att se till att alla frågor svarades ställdes följdfrågor frekvent där det var nödvändigt för antigen vidare utveckling eller klargöra informantens svar. Vid slutet av varje intervju fick varje informant chansen att tillägga något de kände de inte fick chansen att ta upp eller kände var värt att ha med.

3.5 Bearbetning av data

Undersökningen utgick från en kvalitativ ansats där metoden för bearbetning av den insamlade data från de individuella intervjuerna hanterades på följande sätt:

Intervjuerna transkriberades
Det första steget för att bearbeta den insamlade data från de individuella intervjuerna var att transkribera alla intervjuer. Fördelen med detta beskriver Jacobsen (2002) är att kunna extrahera all information som en intervju innehåller på ett effektivt sätt för vidare analys. För att se till att all data återgavs fullständigt, transkriberades varje intervju i sin helhet. För intervjuerna där informanter nämnde kunder eller företaget i sig användes de givna pseudonymerna för företagen samt Kund 1.

- Transkriberingen för de utförda individuella intervjuerna från Företag A finns i Bilaga 2, 3 och 4.

- Transkriberingen för de utförda individuella intervjuerna från Företag B finns i Bilaga 5,6 och 7.
- Transkriberingen för de utförda individuella intervjuerna från Företag C finns i Bilaga 8,9 och 10.

3.6 Reliabilitet och validitet av data

När en empiri utförs ska den inte endast ha en insamlingsmetod utan också uppfylla två krav (Jacobsen, 2002). Det första kravet är att empirin ska vara giltig och relevant, där med valid, och det andra kravet är att den ska vara tillförlitlig och trovärdig, där med reliabel. Det första kravet fokuserar på att se till att det som mäts i empirin uppfattas som relevant och det andra kravet ser till att undersökningen är pålitlig. Vid genomföringen av empirin följdes dessa krav för att erhålla så hög kvalitet på den insamlade data.

För att säkerställa reliabiliteten och validiteten av den insamlade data från de individuella intervjuerna, utfördes intervjuerna med personer som har varierande roller inom respektive företag. Genom att utöka informanternas roller, där vissa har hand om IT och vissa endast arbetar med IT, blev resultaten betydligt varierande. Eftersom undersökningen fokuserar på anställdas säkerhetsmedvetande låg inte prioriteten på att intervjua människor som arbetar med säkerhet, utan mer av anställda utanför säkerhetsramen som lätt kan begå misstag.

För att säkerställa det empiriska materialets tillförlitlighet och trovärdighet signerade varje informant och författarna ett sekretessavtal som bevisar deras deltagande. Under varje intervju användes ljudupptagning och genom att följa en färdigställd intervjuguide hade informanten ingen möjlighet att styra intervjun vilket gjorde att valid och trovärdig data kunde samlas in.

3.7 Etiska aspekter

För att utföra undersökningen korrekt har ett antal etiska aspekter tagits i beaktning från Jacobsen (2002) centrala begrepp gällande etik. Vid utformningen av intervjuerna kommer alla frågor granskas och godkännas av handledaren till författarna av uppsatsen.

Informerat samtycke och frivillighet
Jacobsen (2002) nämner att den som undersöks ska ha informerats om riskerna och vinsterna som ingår i deltagandet innan de ger deras frivilliga samtycke. Innan undersökningen börjar måste författarna av undersökningen få ett skriftligt godkännande från informanterna som ska intervjuas. De informanter som har gett samtycke att undergå en intervju är frivilliga.

Rätt till privatliv
Jacobsens (2002) punkt om rätt till privatliv är av stor vikt och inget som intervjuerna kommer att beakta så som informantens identitet eller kön. I presentationen av data kommer informationen endast bestå av ett åldersspann och en arbetsroll innehållande en ungefärlig hierarkisk ställning. Informanterna kommer att förbli anonyma och ges pseudonymerna “I1, I2, In...”.

Full information
Jacobsen (2002) argumenterar för att informanten inte bör ges full information, utan tillräcklig information. Om full information skulle ges skulle informanten inte bara bli överöst med information utan också kanske bete sig annorlunda än om endast tillräcklig information hade getts; något som kan komma att påverka slutresultatet av intervjun.

Krav på riktig presentation av data
Med riktig presentation syftar Jacobsen (2002) på att data och resultat inte får förfalskas och att data ska återges fullständigt och i rätt sammanhang. Att manipulera data kommer inte ge författarna någon vinst vilket är varför krav på riktig representation av data har ställts för att se till att den insamlade data hanteras på rätt sätt.

3.8 Tillvägagångssätt för litteraturstudie

För att utföra en litteraturstudie användes Google Scholar för att hitta tidigare artiklar och studier inom informationssäkerhet. Då Google Scholar har en extremt stor databas som innehåller tusentals artiklar användes olika sökord som "CIA triad", "Confidentiality, Integrity, Availability" och "Information Security CIA". Eftersom resultatet på sökordet "CIA triad" gav över 11,700 artiklar, var vi tvungna att begränsa resultatet genom att kombinera och specificera sökordet med "Confidentiality, Integrity, Availability" som gav ett resultat på 1,700 artiklar. Inför Gurpreet Dhillons verk inom RITE, användes nyckelorden "Gurpreet Dhillon RITE" vilket gav ett sökresultat på 42 artiklar där av den som refereras i litteraturstudien var högst på resultatlistan.

Utifrån sökorden hittades fyra av de utvalda artiklarna och med en rekommendation från handledaren, valdes artikeln av Gurpreet Dhillon ut. Artiklarna innehåller relevant fakta och studier som kan användas som grund till uppsatsen.

Utöver litteraturstudien utfördes även en kort analys av olika modeller som expanderar CIA-triadens teori. Eftersom två av de utvalda modellerna (RITE och Value-based Compliance Model) redan fanns i två artiklar inom litteraturstudien, användes både litteratur och Google Scholar för att hitta två till. Utifrån ett möte med handledaren rekommenderades en bok av Layton Sr (2005) som diskuterade modellen POST. För att komma åt en sista artikel användes Google Scholar med sökorden "Information security models, confidentiality, integrity, availability" som gav resultat för Al-Hamdanis (2009) verk.

4 Resultat

Utifrån de individuella intervjuerna kan en resultatsammanställning utföras från ett individuellt perspektiv för att sedan analysera potentiella beteendemönster hos informanterna. Sammanställningen kommer att bestå av utdragna citat från intervjuerna med tillhörande bilagsnummer och styckesnummer citatet befinner sig i.

4.1 Företag A

I kapitel 3 introducerades Företag A, vars arbetsinriktning är inom affärssystem där fokus ligger på mjukvarurelaterade tjänster och tillverkningen av mjukvara. Företaget använder sig av engelska som koncernspråk och från företaget intervjuades tre anställda med pseudonymerna I1, I2 och I3.

4.1.1 Faktorer inom företaget

4.1.1.1 Utbildning

På en säkerhetsnivå fokuserar företaget mycket på utbildning för att säkerställa anställdas kunskap och medvetenhet genom att hålla obligatoriska utbildningar. I sin intervju nämner I1 att *"[...]these are mandatory trainings that we need to take because it is a certification that the company has to ensure for each and every one of us [...]"* (Bilaga 2, rad 13). I1 förklarar att alla anställda varje år genomgår en obligatorisk "Code of conduct" utbildning for att uppdatera sig. Beroende på rolltypen en har och vilken typ av information en har tillgång till, går sedan inte alla anställda alltid igenom samma utbildning, då deras arbetsroll avgör om det behövs ytterligare certifieringar vilket tyder på mer utbildning (I1, Bilaga 2, rad 13 & I2, Bilaga 3, rad 14).

Utbildningarna som företaget erbjuder, vilka utökar anställdas medvetenhet, är allt från olika typer av lagligheter som de måste vara medvetna om, säkerhet, informationssäkerhet, eller utgör erbjudanden och löften till kunder (I1, Bilaga 2, rad 86). I3 nämner att *"We also have online trainings as well that are mandatory to be passed and followed up and the training attendance information is visible for all the responsible managers"* (Bilaga 4, rad 21).

Syftet med utbildningarna är inte endast att ge vägledning hur man bör tänka i olika situationer, utan utbildningarna som erbjuds pågår varje år och flera gånger under året. Anledningen till att utbildningarna är så ofta förklarar I1 som *"[...]it's new information of course because within new information security area new things happen all the time and without a doubt the infiltration that takes place on a global level"* (Bilaga 2, rad 21). I3 beskriver att de årliga utbildningarna är *"[...]it is continuously improved and followed-up"* (Bilaga 4, rad 15). På detta sätt uppdateras alla anställda konstant om ny information och nya sätt att hantera information på ett mer ansvarsfullt och säkrare sätt.

Bortsett från utbildningarna kan företaget även ge ut information om nya händelser. I2 nämner att om *"[...]something big hits the news or something then maybe you get additional sort of information that you may be aware of and have to make sure that it doesn't happen"* (Bilaga 3, rad 21) Denna typ av information kan agera tillägg till deras befintliga utbildning och certifikat.

4.1.1.2 Policys

Företaget har en mängd olika policys som alla anställda ska känna till, specifikt de policys som angår ens arbete. I1 nämner *"[...]we do have the security policies that we have to follow and especially when it comes to information security"* (Bilaga 2, rad 13). I de fallen där anställda arbetar med kundrelationer påpekar I1 att *"we are very respectful about the policies that our customers have"* (Bilaga 2, rad 44) eftersom om anställda skulle bryta mot sina kunders kontrakt genom att dela med sig information till obehöriga, förlorar företaget både förtroende och relationen till kunden försämras. Det finns en viss gräns för vad anställda får säga till kunder om andra kunder, men endast om det står i kundkontraktet. På det här sättet kan anställda använda sig av en generell överblick av kundinformation för att hjälpa och inspirera andra kunder.

I1 nämner att när de blir anställda undertecknar de papper som lovar att följa alla typer av policys som företaget har och detta gäller även informationsdelning. I3 beskriver processen för informationsdelning som komplex och *"controlled quite heavily"* (Bilaga 4, rad 42). På samma sätt förklarar I1 att *"[...] information confidentiality is strictly governed and if someone goes outside of those boundaries of what the boundaries allow, then one could literally be fired [...] It's a consequence if a certain type of behaviour is transgressed"* (Bilaga 2, rad 49). I de fallen där anställda är osäkra vad gäller informationsdelningspolicys ser de till att information som är sekretessbelagd inte nås ut på något sätt, säger I2. Precis som företagets utbildningar nämner I3 att företaget *"[...]frequently improve and renew the training and reviewing the policies so that the knowledge is continuously maintained"* (Bilaga 4, rad 47).

4.1.1.3 Säkerhetsmedvetande

Företaget har tydliga riktlinjer för hur anställda ska bete sig och vad konsekvenserna är om dessa riktlinjer inte följs. Informanterna visar stort säkerhetsmedvetande vad gäller både deras arbete gentemot kunder och det interna arbetet på företaget vilket kan vara resultatet av deras utbildningar. De känner till alla policys som angår deras arbete och konsekvenserna om de skulle gå emot sagda policys. I1 förklarar hur hög graden av medvetenhet är bland anställda: *"[...]if we break these rules and potentially do things without intending to but do things that can result in commercial and business disruption, or legal suits, then literally people understand that they can be fired because that is the type of severity that is transgressed and it's a consequence"* (Bilaga 2, rad 86).

På företaget använder folk mycket sunt förnuft och det dem har lärt sig från tidigare utbildningar när det gäller hur folk arbetar. *"[...] be aware of things that could affect the way that we do business"* (Bilaga 3, rad 65) förklarar I2 vilket är extremt viktigt på företaget som arbetar internationellt. Själva tanken att inte göra saker man inte har lov att göra, vare sig det är att ändra information, söka upp olovlig information eller dela med sig information till obehöriga är inget som anställda stöter på. När det gäller informationstillgång är folk medvetna om vad de bör ha tillgång till för att genomföra ändringar och vad som inte angår deras arbete. I1 ger ett exempel på vad man bör göra om en skulle få tillgång till något som inte har med dem att göra: *"Even if you should get access to something that you should not have access to, then you actually should a) close it and not look into it further perhaps"* (Bilaga 2, rad 65). Detta är ett tydligt tecken på hur säkerhetsmedvetna anställda är på företaget och deras respekt mot varandra samt det givna policys.

4.1.2 Confidentiality

På en teknisk nivå använder företaget en mängd olika lager för säkerhetsprogram och anti-virus program för att skydda både intern och extern information. Förutom att företaget använder sig av VPN-tunnlar och brandväggar berättar I1 om företagets egna säkerhetsprogram:

"[...]we as a company also have security programs for our own applications [...] these are special programs which don't exist on the market place, they're literally provided by Företag A to protect Företag A applications or to definitely increase the level of security." (Bilaga 2, rad 39).

Utifrån informanterna hade alla tillgång till information som behövs för att kunna utföra sitt arbete. För att få tillgång till information har företaget skapat en kontrollerad process. I1 och I2 förklarar att om anställda inte har tillgång till en viss typ av information behöver dem skicka en förfrågan om en viss typ av "access right" eller "permission" med en förklaring om varför den tillgången behövs. I2 beskriver processen för att få tillgång till information som:

"So you would fill in various forms and ask for permission and say why you actually would need certain things. And depending on how much security information that you actually get access to, [...] it depends who needs to verify this information and who needs to approve or disapprove it." (Bilaga 3, rad 43).

På en strategisk nivå arbetar företaget enligt skapade policys som även hänvisar till deras kunders egna villkor. När det gäller informationsdelning tar företaget sekretess väldigt seriöst för att undvika att information hamnar i orätta händer. I2 nämner att om en anställd markerar information som sekretess, då måste de vara extremt försiktig med att informationen inte försvinner (Bilaga 3, rad 47). Detta påverkar även hur och var anställda lagrar sekretessbelagd information.

Tidigare nämnt sträcker företagets policys även ut till deras kunder där kundernas sekretessavtal avgör graden av informationsdelning företaget får utföra. I2 går vidare i intervjun och säger *"There are certain customers that are very limited and are very security sensitive"* (Bilaga 3, rad 49). Här är både företaget och de anställda noga om informationsdelning där I1 påpekar *"[...]we never reveal something that the customer has not signed off."* (Bilaga 2, rad 46). Förutom informationsdelning inom kundrelationer har företaget även vissa regler när det gäller informationsdelning till utomstående så som familj och vänner. I2 nämner att inom deras arbetsroll finns det vissa regler som säger att anställda inte får prata om vissa saker vid en viss tidpunkt. *"[...]we can't actually tell friends or family to go on on the stock market at a certain blackout time for instance."* (I2, Bilaga 3, rad 52).

4.1.3 Integrity

Företag A har en tydlig metod för teknisk säkerställning av information genom automatisk eller manuell backup. Både I1 och I2 anger att detta förekommer, medan I3 inte är säker. I1 anger att: "*We have an automatic backup that takes place. So every day while I'm working, a backup is performed. In my case it's automated, I have asked them to do that otherwise I would have to manually do it in that case*." (Bilaga 2, rad 54).

När det kommer till den strategiska biten av att säkerställa att informationen som finns tillgänglig är rätt, finns det ett gediget tänk kring behörigheter och versionshantering. Det finns enligt I1 tydliga regler för vad man får redigera och inte, samt olika klassificeringar av dokument; "*If you alter information it is because you have the right to publish in a certain document. So if I for example publish, let's say a certain document, an official document where only a few people have the right to edit it then I would have to have those rights to do that. Otherwise if I for example take a powerpoint presentation that says "Confidential" and it comes from the project management group, and it also say "Internal confidential", then that is a piece of paper that I don't own and I don't have any rights to edit that even if it's in a powerpoint format and not PDF."* (Bilaga 2, rad 57).

I2 fyller i att om det är så att man använder något som man inte bör är det något som det ses allvarligt på: "*So [they] treat that really quite seriously if there is something that's not supposed to be altered and you try to use it in another way without permission you know it's not a good thing*." (Bilaga 3, rad 66).

I3 anger att det endast är tillåtet att ändra information som man arbetar med direkt: "*Only if I am directly involved in a certain project otherwise I don't have any kind of rights to change information. It's only the person that is owning the respective task or initiative."* (Bilaga 4, rad 58). I3 anger också att man anger datum på sina utkast för att säkerställa att det är rätt information.

I1 pratar vidare om hur de säkerställer att ingen ändrar på något med versionshantering. *"[...] Usually documents have a tracking history so you do have an understanding of when it was last altered or edited and by whom, and which version it's in."* (Bilaga 2, rad 61).

I2 pratar också om att de har en inofficiell "4 eyes policy" som betyder att minst två personer ska undersöka om information som används i kommersiellt syfte är riktig, "[...] *But if it's something of significance then we've got this "4 eyes" policy and it's sort of better to have a few people looking at this rather than just one."* (Bilaga 3, rad 70).

4.1.4 Availability

När det gäller tillgängligheten till information på en teknisk nivå har företaget full kontroll. Alla informanter förutom I3 har upplevt någon gång att de inte har tillgång till specifik information och anledningen till detta förklarar I1 är att information alltid flyttas omkring, länkar är inte längre i funktion eller att något program har ett tillfälligt tekniskt problem. När detta händer säger I1 att *"[...]sometimes you'll get an error message."* (Bilaga 2, rad 70) vilket I1 går vidare med att förklara hur enkelt det är att lösa: *"[...]you log a service ticket and then you can also grade the severity of that issue."* (Bilaga 2, rad 72).

Åtkomsten till information skyddar företaget med hjälp av olika säkerhetsprogram och antivirus program vilket bara I1 och I2 kunde svara som har McAfee färdig installerat på arbetsdatorn. Företagets fysiska säkerhet är väldigt strikt där endast anställda har individuella accesskort. I intervjuerna har informanterna skilda åsikter och förklarar lite mer på djupet.

I1 förklarar företagets policys mot utomstående och hur långt de kommer in på kontoret i Stockholm: *"[...]for external people nobody can come in unless they are going in through the reception so they have to register and so on. It is strictly forbidden to take anybody, [...] into a part of the company where they're not meant to be."* (Bilaga 2, rad 79).

I2 känner inte likadant vad gäller graden av fysisk säkerhet företaget har investerat i: *"It's pretty good but to be perfectly honest I think that these things can always be better than what they are. [...]we've got cards and codes and we've got cameras [...] - certain doors that have got different codes in. I still think on the whole that we're way behind [...] It really should be better than it is, definitely."* (Bilaga 3, rad 83).

Den strategiska nivån på informationstillgänglighet hade likt företagets fysiska säkerhet skilda åsikter bland informanterna vilket kan bero på deras arbetsroller. I I1:s arbetsroll arbetar de mycket med kundinformation som bara har ett värde under en viss tid så länge projektet är igång vilket innebär att informationen tappar sitt värde i längden. Under tiden som kundinformation har ett värde säger I1 *"[...] there is an agreement between companies to guard the information and to safeguard it when it comes to confidentiality."* (Bilaga 2, rad 83). I samma rad berättar I1, när det gäller utskick av information till kunder, att det finns väldigt mycket tillit mellan de anställda och kunderna. Om I1 skickar information så som företagets prislista, ska de lita på att kunden inte skickar listan vidare till företagets konkurrenter (Bilaga 2, rad 83).

I2, som jobbar som Maintenance sales manager, känner inte till några policys angående utskick av information till rätt mottagare. De påstår i intervjun *"I don't think there is any policy [...] I think you have the common sense prevail."* (Bilaga 3, rad 89). I I3's fall nämner dem att alla är ansvariga för att förstå vem man skickar e-mail till (Bilaga 4, rad 83) vilket lutar sig åt sunt förnuft vilket är vad I2 också påpekade.

4.2 Företag B

I kapitel 3 introducerades Företag B, vars arbetsinriktning är inom den finansiella sektorn med fokus på finansiell rådgivning till kunder som är både privatpersoner och företag. Företaget använder sig av det svenska språket och från företaget intervjuades tre anställda med pseudonymerna I4, I5 och I6.

4.2.1 Faktorer inom företaget

4.2.1.1 Utbildning

De utvalda informanterna på företaget har haft lite säkerhetsutbildning när det har varit relevant. I6 påpekar *"vi har blivit informerade hur vi ska bete oss"* (Bilaga 7, rad 8). Företaget vill inte att deras anställda ska veta hur deras IT och säkerhet ser ut av en anledning, vilket är varför utbildningen de har fått har varit angående SecureMail, det vill säga hur man skickar e-mail på ett säkert sätt och hur man läser av riktigheten av e-mails innehåll. I5 beskriver hur det går till när de får in e-mail som måste kontrolleras: *"Vi får inte ta uppdrag på mail hursomhelst, utan då får vi kontakta uppdragsgivaren och fråga om han eller hon har skrivit det här mailet till oss och hon vill att vi ska göra detta för dem"* (Bilaga 6, rad 8).

4.2.1.2 Policys

Företaget erhåller extremt många policys som varje avdelning och anställd måste följa. När en ny anställd börjar arbeta på företaget skriver de under ett sekretessavtal eller som I6 beskriver det som *"total sekretess"* (Bilaga 7, rad 30), vilket I4 nämner är ett avtal som *"gäller tills man dör [...]"* (Bilaga 5, rad 12). I det avtalet ingår det också banksekretess vilket innebär att alla anställda har tystnadsplikt mot företagets kunder och företagets interna arbete.

Säkerhetsmässigt har företaget en policy som I6 beskriver är för utskick av information och innehåller riktlinjer för typen av information som e-mail får innehålla - och inte innehålla. *"Ingenting får skickas utan SecureMail."* (Bilaga 7, rad 8) men I5 tillägger att *"När det gäller mail ska man inte skicka personuppgifter och sådana saker, som eventuellt kan hamna i orätta händer"* (Bilaga 6, rad 22). Det är extremt viktigt att alla anställda följer de givna policys för att undgå attacker. Genom att ha tystnadsplikt samt flertal arbetspolicys och policys med riktlinjer för vad anställda får skicka och inte skicka kan företaget säkerställa att alla anställda är säkerhetsmedvetna. Vikten att hålla tystnadsplikt både internt och externt är både företaget och alla anställda medvetna om, som I5 uttrycker det *"där är vi väldigt stränga, att vi inte röjer vad vi har för kunder"* (Bilaga 6, rad 24).

4.2.1.3 Säkerhetsmedvetande

Eftersom informanterna endast har blivit utbildade inom säker hantering av e-mail och följer extremt strikta policys, visar det ett tydligt tecken på deras medvetenhet mot säkerhet och beteende i vissa situationer. De anställda har väldigt bra koll på den strategiska säkerheten genom att vara extremt säkerhetsmedvetna angående informationsdelning och konsekvenserna ifall ett katastrofalt misstag hade uppstått.

4.2.2 Confidentiality

På en teknisk nivå kan alla anställda på företaget komma åt behörig information via företagets intranät och interna system. Beroende på vad man arbetar med finns det begränsningar för åtkomsten till information. I4 arbetar som kundansvarig och meddelar i intervjun *"Jag har tillgång till information som rör mina kunder."* (Bilaga 5, rad 32). När det gäller typen av säkerhetsutrustning företaget använder för att skydda information kan ingen av informanterna svara på grund av banksekretess och allmän okunskap.

Angående informationsdelning på en strategisk nivå har banken, som tidigare nämnt, banksekretess vilket I4 förklarar innebär att anställda *"[...] får absolut inte prata om våra kunder med någon."* (Bilaga 5, rad 36). Alla informanter är extremt medvetna om denna policy. Man måste vara väldigt försiktig med vad man skickar ut där I5 tillägger att man inte skickar personuppgifter på e-mail. Ytterligare riktlinjer nämner I6 är *"Allt som har med kund att göra måste vi skicka med SecureMail."* (Bilaga 7, rad 26).

Företaget har extremt strikta och tydliga regler kring informationsdelning med utomstående. Om det är arbetsrelaterad information har anställda lov att dela med sig till sina kunder på ett säkert sätt samt relevanta kollegor för att, som I4 säger i intervju, *"ge kunden bästa service."* (Bilaga 5, rad 42). Om det är information som ska delas med till främmande utomstående berättar I4 *"Jag får i princip inte dela med mig någonting med någon, utom den det rör."* (Bilaga 5, rad 42). Eftersom alla informanter arbetar med kunder är de alla väldigt restriktiva. En viktig del av banksekretessen som angår informationsdelningspolicyn säger I5 är *"Vi talar till exempel inte om vad vi har för kunder*." (Bilaga 6, rad 24).

4.2.3 Integrity

Företaget uppdaterar och gör automatisk backups varje dag där I4 tror att det även görs backups en gång i timmen. Enligt I4 kan de spara information som sedan *"sparas ju omedelbart och sedan finns det tekniska lösningar för att hämta upp det där."* (Bilaga 5, rad 48).

Företagets strategiska säkerhet angående integriteten av information är väldigt strikt. För att ändra information har företaget satt upp vissa regler vilket både I4 och I6 berättar är att man inom vissa ramar får ändra information och mer specifikt säger I4 *"[...] de dokument som jag själv har skrivit och som jag själv har gjort - det kan jag ju ändra i."* (Bilaga 5, rad 50). Men gränsen för informationsändringar stannar vid undertecknade avtal med kunder. I4 tillägger *"[...] skulle vi ändra i någon information som vi lämnat till vår kund, då måste vi ju kontakta vår kund och berätta det."* (Bilaga 5, rad 50).

Informanterna hade svårt att svara på säkerställningen av informations riktighet. I4 som är kundansvarig säger: *"Jag har ju ett uppdrag med mina kunder att se till att det jag skriver till dem och det jag säger till dem, att det är rätt. [...] Vi är noggranna i det vi gör, redan från början."* (Bilaga 5, rad 52-54).

I5 som arbetar som assistent säkerställer information genom att motringa. *"[...] om vi får uppdrag utifrån kunder så måste vi motringa och säkerställa att det verkligen är korrekt avsändare."* (Bilaga 6, rad 26).

I6 arbetar som avdelningsansvarig och har experthjälp till hands i situationer där riktigheten av information måste fastställas. I de fallen där I6 har fått in en kundfråga måste svaret på frågan fastställas då I6 nämner att svaret kan ha ändrats under tiden (Bilaga, rad 40). De beskriver vidare hur de fastställer information som kommer från rätt mottagare som de är osäkra på: *"I det fallen får man ju titta på det och se hur det se ut och ibland känner man ju igen namn och dylikt."* (Bilaga 7, rad 42).

4.2.4 Availability

Inom företaget har alla informanter upplevt att de någon gång under sin arbetstid inte har haft tillgång till en viss information. I4 ger en tanke kring anledningen om varför sådant händer: *"[...] det beror antagligen på att det finns någon kodning någonstans som gör så att jag inte har tillåtelse [...] Men då får man lösa det genom att prata med en kollega som har behörighet att ta fram det."* (Bilaga 5, rad 57). I5 tillägger i sitt svar att behörigheten kan bero på vilken avdelning man arbetar inom, om den behörigheten är nödvändig eller inte vilket I5 kommenterar är väldigt strängt kontrollerat.

I och med att företaget är en bank har ingen av informanterna någon aning om, eller får inte meddela, vilken typ av säkerhetsprogram företaget använder. Den fysiska säkerheten på kontoret i Malmö är mycket kontrollerat där anställda använder passerkort som I4 kommenterar loggar var man befinner sig. De tillägger: *"Man kommer inte in [...] utan att ha passerkort. [...] det är jättenoga med att man inte kommer åt våningsplan som man inte har anledning att vara på. [...] vi får inte ta med oss utomstående in heller."* (Bilaga 5, rad 65-67). Eftersom ens tillgång inom kontoret är beroende på arbetsrollen anställda har berättar I5 *"[...] vi har inte access till att komma in överallt i huset, [...] utan då får man ansöka om behörighet att komma in på*

en speciell avdelning om man har där att göra. Så det är faktiskt rätt så strängt." (Bilaga 6, rad 36).

Företaget har som tidigare nämnt strikta policyers när det gäller utskick av information till rätt mottagare. Beroende på arbetsrollen man har kan det variera hur man skickar ut information. I4 som kundansvarig har hand om bland annat viktiga kundavtal och meddelar i intervjun *"Vi skickar väldigt mycket via post fortfarande.[...] Vi vet att det inte är säker att skicka mail."* (Bilaga 5, rad 69-71). Både I5 och I6 som använder e-mail for att utföra en del av sitt arbete känner att man får lita på att man har fått korrekt e-mailadress till kunder och att alltid skicka e-mail via SecureMail.

4.3 Företag C

I kapitel 3 introducerades Företag C som ett IT-konsultföretag vars arbetsinriktning är inom systemutveckling och applikationssäkerhet. Företaget använder sig av det svenska språket och från företaget intervjuades tre anställda med pseudonymerna I7, I8 och I9.

4.3.1 Faktorer inom företaget

4.3.1.1 Utbildning

Utifrån den insamlade data från intervjuerna gav informanterna olika svar kring utbildning. I sin intervju säger I7 att *"Jag har aldrig blivit 'preppad' med någon sorts säkerhetstänk. Det är nog mer att man lutar sig mot sunt förnuft"* (Bilaga 8, rad 14). Från I7:s intervju gavs det ett intryck att företaget inte använder sig av någon form av utbildning alls för deras anställda. Tillskillnad från kontoret i Stockholm där det finns en hög kunskapsnivå kring IT-säkerhet, nämner I7 att den enda utbildningen som erbjuds på kontoret i Malmö är säker programmering för deras programmerare. Utan utbildning går I7 vidare med att förklara hur de arbetar med sunt förnuft i situationer där ytterligare hjälp och avancerad kunskap behövs:

"[...]när vi känner att "Ja men här vill vi nog vara väldigt säkra på att det här blir bra och korrekt och rätta krypteringsmetoder" då ringer vi till någon i Stockholm som tar ner någon från Stockholm. Men det är någon sorts fingertoppskänsla när det behövs." (Bilaga 8, rad 16).

Förutom I7 svarade I9 på frågan om de har fått någon utbildning med *"Policys och säkerhetsutbildningar är ingenting som har nämnts för mig direkt"* (Bilaga 10, rad 14). Med två svar som riktar sig åt ena hållet förklarar I8 att det finns olika typer av utbildningar på företaget som anställda går. I Bilaga 9, rad 23 säger I8 *" [...] den generella utbildningen i projekten [...] då får man läsa på och lära sig. Sen har vi våra kompetensutbildningar på företaget två gånger om året och det är ganska mycket IT-säkerhet [...]"*. Anledningen till varför informanterna har gett olika svar kan antigen tyda på brist på medvetenhet eller så har deras arbetsroll inget med de givna utbildningarna att göra. Oavsett om det finns utbildningar eller inte så hjälper anställda varandra inom respektive område. I7 nämner att *"[...] finns det så många unga hungriga som behöver liksom lite guidning och vägledning [...] så jag kände att jag kunde bidra lite där eftersom jag har programmerat sedan -82 [...]"* (Bilaga 8, rad 8).

4.3.1.2 Policys

Kontoret i Malmö använder sig av väldigt få policys som många anställda inte känner till. *"[...] vi har ju metoder för alla nyanställda och det finns riktlinjer för vad vi skickar i mejl och inte skickar i mejl[...]"* (I7, Bilaga 8, rad 18). Det kan vara svårt att avgöra hur väl anställda följer policys när det inte finns så många men eftersom folk arbetar i projekt tillsammans minskar risken att göra fel. Det viktigaste som anställda måste vara medvetna om är att inte skicka känslig och användbar information till kunder på e-mail. Detta förklarar I7 som *"[...]lösenord och annat som man känner krävs för att logga in någonstans, det skickar vi inte i mejl."* (Bilaga 8, rad 36). Detta har gjort att många får tänka kritiskt när de ska skicka iväg information: "Vem är det till och vad är det för typ av information?".

När folk arbetar i projekt för en kund begränsas informationsdelningen till utomstående. Alla informanter har liknande berättelser angående informationsdelning där I7 berättar i intervjun *"Vi har många kunder som vi får fylla in en 'form' angående fullständig tystnadsplikt och då får jag egentligen inte prata med någon"* (Bilaga 8, rad 38). Med få företagspolicys kan alla anställda följa sina kunders policys närmre för att se till att de levererar exakt vad kunden önskar och på kundens villkor.

4.3.1.3 Säkerhetsmedvetande

Utan utbildning och med få företagspolicys är informanterna på företaget väldigt säkerhetsmedvetna, speciellt i relation till deras kunders policys. Att arbeta efter sunt förnuft lär de sig själva och från andra hur man bör bete sig i olika situationer och exempelvis vad som är lämpligt att skriva i e-mail till kund. För att vara ett IT-konsultföretag med ingen intern företagsinformation kommer de långt på sunt förnuft.

Användandet av sunt förnuft som en "policy" sträcker sig även inom informationsdelning. I7 förespråkar i rad 36 i relation till policyn, att känner en anställd sig tveksam så bör de inte skicka ett e-mail om det.

4.3.2 Confidentiality

De anställda på företaget har inte så stor koll på vilka säkerhetsutrustningar som företaget använder, men för det mesta är de medvetna om att det finns brandväggar och förkrypterade diskar som skyddar information. I7 informerar att företaget inte har satt några krav på anställda att förkryptera sina diskar, utan det gör man självmant. En ytterligare säkerhetsutrustning är molnet som I8 tar upp och påpekar att det man delar ut är vad folk har tillgång till (Bilaga 9, rad 37).

Tillgången till information beror för det mesta på arbetsroll och typen av projekt man arbetar med. Som administratör har I7 tillgång till all information som behövs för att utföra sitt arbete. I7 berättar *"Det är jag som administrerar rättigheterna till kodbanken [...] Jag kan använda och administrera så att andra når den koden de ska nå."* (Bilaga 8, rad 34). Precis som I7 har I8 och I9 tillgång till allt som de behöver, men mer specifikt det kunder tillåter dem att se under projekt. Genom att vara ett konsultbolag kommenterar I8 nackdelarna med att få tillgång till kundinformation *"[...] Konsulter är nog ofta den svaga länken när det delas ut behörigheter. Du får nycklarna till slottet. [...] det är oftast den bristande källan till informationssäkerhetsförluster."* (Bilaga 9, rad 39).

På en sekretessnivå av informationsdelning är ingen av informanterna medvetna om det finns någon aktuell policy. I7 tar upp tanken om att det kanske finns en policy med tanke på företagets

affärsinriktning: *"[...] lösenord och annat som man känner krävs för att logga in någonstans, det skickar vi inte i mejl. [...] Ja, det kan jag tänka mig göra personligen fast om Företag C står för säkerhet känns det ganska dumt att gå emot det."* (Bilaga 8, rad 36).

I8 berättar istället att informationsdelningen är mer kundspecifikt och att varje anställd skriver på ett avtal när de börjar jobba på Företag C: *"När du blir anställd av kunder, inhyrd, får du skriva på non-disclosure agreement som säger att du får inte ens prata om det här med någon på kontoret. [...] generellt är det så när vi börja jobba. Det skriver vi på vid anställningsavtalet att det vi pratar om här, det pratar du inte någon annanstans."* (Bilaga 9, rad 45). I9 syn på policyn var mer osäker och funderade mer på att det är "är vett och etikett där" (Bilaga 10, rad 67) som gäller för anställda.

Till sist håller alla informanter med om att informationsdelningen till utomstående fortfarande är väldigt kundspecifikt. När anställda går med i projekt med en kund, beroende på kunden, ska ett dokument angående fullständig tystnadsplikt fyllas i. I7 tillägger i samma svar *"Jag får inte prata med någon om det på kontoret. Om jag sitter i ett projekt där dem har dem kraven, [...] då får jag inte ventilera det till någon mer än dem som är med i projektet."* (Bilaga 8, rad 38).

4.3.3 Integrity

Företaget utför automatiska backups varje dygn som I7 berättar om i mer detalj: *"Det som vi har markerat som väsentlig information för oss själva backas varje dygn och åker upp i molnet. [...]"* (Bilaga 8, rad 40). Eftersom företaget utvecklar program berättar både I8 och I9 i deras intervju att koden de arbetar med är versionshanterad. I8 säger *"Det är den backupen som finns och det är mer än tillräckligt för att allting som är versionshanterad på GitHub, det är backat och kan bara hämtas ner om datorn går sönder."* (Bilaga 9, rad 49).

När det kommer till informationsändring beror det på vilken kund det är och vad ändringen gäller. De anställda är medvetna om avtalen de undertecknar hos kunden där I8 meddelar *" [...] jag har ju tillgång till mina kunders databas. Om de vill att jag ska ändra någon data där så får jag göra det. Men igen, det är upp till projektet [...]"* (Bilaga 9, rad 53). Både I7 och I9 har möjlighet att ändra all information som de har tillgång till men gäller det en specifik kund så gäller ändringarna inom vissa ramar. I9 svarar på frågan med *"Jag kan ändra jättemycket saker och sen så finns det mycket - vi har tillgång till alla saker som hade varit jättedumt att göra, både för mig personligen och för hela företaget [...]"* (Bilaga 10, rad 98). Även om ändringarna är för kunder, meddelar I9 att det finns en stor tillit i de anställda från företagets sida för att se till ändringarna som utförs inte utgör något katastrofalt för kunderna eller företaget själv.

Företaget använder sig inte av någon policy när det gäller säkerställning av informations riktighet. Informanterna meddelar istället att anställda använder sig av versionshantering och filrättigheter till information. Genom att använda versionshantering känner I7 att man kan säkerställa riktigheten av information för att som de säger *"man kan alltid se vem som har ändrat senast [...]"* (Bilaga 8, rad 44). När det gäller e-mail och vad som skickas till informanterna finns det andra åsikter om säkerställningen. I8 säger *"Det mejlas information och du vet inte om någon har varit emellan men någonstans får man lita på att den kedjan är intakt [...]"* (Bilaga 9, rad 55).

4.3.4 Availability

Tillgången till information har visat sig vara lite annorlunda för de anställda på Företag C, eftersom de inte erhåller mycket intern företagsinformation utan mer extern kundinformation. I I8 och I9:s fall har det blivit allt mer vanligt att de inte har fått tillräckligt med tillgång till kundinformation på grund av externa faktorer som ligger hos kunden. Både I8 och I9 beskriver svårigheterna med den begränsade tillgången men förklarar att man arbetar vidare med det man har fått (I8, Bilaga 9, rad 57 & I9, Bilaga 10, rad 107).

Användandet av säkerhetsprogram är lite olika beroende på arbetsrollen man har och vilket arbete som utförs. I7 kan inte direkt svara på vad företaget använder men är medveten om vilken typ av mjukvara som är krypterad samt att det är väldigt kundbaserat. I fallen där känslig information ska skickas, så som inloggningsuppgifter och lösenord, används LastPass och I8 meddelar även att företaget har en VPN-tunnel som används för att kunna arbeta hemifrån (Bilaga 9, rad 59). Som nyanställd på företaget använder I9 programmet GitHub för att spara kod och har en stor tillit till sina kollegor att de använder något anti-virus program på respektive dator för att förhindra utomstående att ta sig in till deras kod. Synen på anti-virus program är inte väldigt positivt där I9 kommenterar i intervjun: *"[...] det fångar ju bara det lilla och det kända egentligen. Det finns inget anti-virus program idag som kan fånga dem bästa och dem nya - det finns för många virus. [...] det skulle inte förvåna mig ifall någon inte har ett anti-virus program i överhuvudtaget"* (Bilaga 10, rad 120-122).

Eftersom företaget nyligen bytt lokal har deras fysiska säkerhet inte färdiginstallerats. I7 nämner *"Nu har vi precis flyttat hit så här är vi inte så nöjda. Det kommer att komma upp nya lås, el-lås, och vi har själva brickor för att komma in, larmkoder och så vidare. Just nu är det fritt blås så det är ganska många som bara kan gå rakt in."* (Bilaga 8, rad 58). Både I7 och I9 tycker inte om den känslan alls:

"Det känns inte bra alls. Det är ganska mycket spring här för det har legat ett annat företag här innan [...]" (I7, Bilaga 8, rad 62).

"Det känns inte alls bra, speciellt inte när man har datorer och sådant som ligger här. Man vill på något sätt känna sig helt säker här och kunna vara lite glömsk kanske utan att det ska kunna straffa sig." (I9, Bilaga 10, rad 129).

Företag C använder sig mycket av sunt förnuft kring den strategiska nivån vad gäller tillgängligheten till information vilket alla informanter känner sig lugna med. Ingen av dem känner till en uttalad policy angående utskick av information till rätt mottagare vilket I7 tillägger *"Vi faller nog tillbaka på använd ditt sunda förnuft liksom och om du tänker dra iväg en massa känslig information så är kanske inte just ett helt vanligt mejl är det rätta sättet att göra det på."* (Bilaga 8, rad 64).

5 Diskussion

Stanton m.fl. (2004) har tidigare argumenterat för att företag har en tendens att lägga ner en större del resurser på tekniska lösningar för att förbättra säkerheten. Tillsammans med Gonzales & Sawicka (2002), Dutta & Roy (2008), Siponen (2000), och Warkentin & Willison (2009), påpekar studierna att mänskliga faktorer har en inverkan på informationssäkerheten inom företag. I och med att mänskliga faktorer har en stark påverkan innebär det att faktorerna indirekt har en påverkan på CIA-triadens komponenter som tidigare nämnt är grunden till informationssäkerhet.

De identifierade mänskliga faktorer som anses vara avgörande för informationssäkerheten hos de utvalda företagen är arbetsroll, utbildning och policys. I Stanton m.fl. (2004) studie konstaterades det att ens arbetsroll, engagemang inom organisationen och organisationens typ påverkade anställdas säkerhetsmedvetande. Utifrån informanterna anses det att resultaten från Stanton m.fl. (2004) studie stämde överens med resultaten från samtliga företag där typen av arbetsroll en har och organisationsengagemang var två förekommande faktorer. På Företag A påverkades dessa faktorer av mängden utbildning och policys företaget erhåller vilket tyder på att säkerhetsmedvetandet hos anställda håller en hög grad. Utbildningsmässigt ser Företag B till att anställda informeras och utbildas i områden som anses vara relevant för deras roll. Detta gör att mer fokus läggs på att följa strikta policyers för att undvika säkerhetsrelaterade problem och öka säkerhetsmedvetandet.

Företaget som står ut i mängden när det gäller säkerhetsbeteende i förhållande till mänskliga faktorer är Företag C som varken utbildar anställda eller erhåller formella policyers. Istället utgår företaget från sunt förnuft som en policy vilket påverkar anställdas säkerhetsmedvetande. Policyn kan ha sina nackdelar om folk har olika bedömningar om sunt förnuft vilket kan avgöra anställdas säkerhetsbeteende. För att vara ett IT-konsultbolag som arbetar med applikationssäkerhet känns det märkligt att företaget inte erhåller lika stark teknisk och strategisk säkerhet som Företag A och Företag B när de erbjuder säkerhet till kunder. Med anledningar att utbildning inte behövs och att endast utgå från sunt förnuft lyckas företaget gå i vinst och undvika säkerhetsproblem.

5.1 CIA-triaden

Nedanför kommer det teoretiska ramverket och materialet från den empiriska undersökningen analyseras och diskuteras utifrån varje komponent inom CIA-triaden.

5.1.1 Confidentiality

I Figur 3.1 agerar Företag A och B ur ett teoretiskt perspektiv som användare av tjänster, och där med säkerhetstjänster. Denna sammankoppling mellan företagen och resultaten från intervjuerna har visat att användare av säkerhetstjänster har en större fokus på sekretess då de använder säkerhetstjänsterna för att skydda information. Utifrån resultaten kan det konstateras att både Företag A och Företag B lägger mycket fokus på teknisk och strategisk sekretess, tillskillnad från Företag C, som anses fokusera mer på strategisk sekretess men upprätthåller ändå god teknisk säkerhet.

Wilson (2013, p. 47) nämner att "Confidentiality measures function properly if authorized users can retrieve information, while attempts by unauthorized users are denied." Det Wilson (2013) nämner i sin artikel kan kontrolleras på ett tekniskt sätt. Hursomhelst påpekar Dhillon & Backhouse (2000) att ett problem inom teknisk hantering av sekretess är att teknologi håller på gå att i motsatt riktning från Wilson (2013) beskrivning. Författarna hänvisar till att utveckling börjar rikta sig mot att göra data tillgänglig för många istället för ett fåtal (Dhillon & Backhouse, 2000).

Inom den tekniska aspekten av sekretess är graden av säkerhetsprogram som används inom företagen olika men Företag A och Företag B lägger mycket fokus på detta område. Företag A använder både interna och externa säkerhetsprogram som endast är anpassade för Företag A:s programvaror och vissa säkerhetsprogram som inte finns på marknaden. Företaget ligger i framkant när det gäller säkerhetstänk genom att konstant uppdatera systemvaror och informera anställda. På grund av Företag B:s banksekretess är det otydligt vad för säkerhetsgrad företaget har. I och med att företagets affärsinriktning är inom den finansiella sektorn bör det finnas ett extremt starkt säkerhetsskydd för företagsinformation mot utomstående. Tillskillnad från de två företagen har Företag C ingen stor mängd företagsinformation att skydda. Detta resulterar i att företaget endast använder sig av några brandväggar, förkrypterade diskar och en VPN-tunnel som säkerhetsskydd vilket signalerar att dem inte fokuserar mycket på teknisk sekretess med tanke på den lilla mängden information de erhåller.

Tillgången till information och tillhörande processer är extremt kontrollerat på Företag A och Företag B. Genom att kontrollera tillgången har företagen full makt och visuell kontroll över anställdas behörigheter, vilket innebär att om interna användare har en svår tillgångsprocess är processen för utomstående nästintill omöjlig. Med ett sådant kontrollerat system och Wilson (2013) beskrivning av komponentens funktion bevisar företagen att Dhillon & Backhouses problem är felaktig och uppnår komponentens mål på ett korrekt sätt ur ett tekniskt säkerhetsperspektiv. I Företag C:s fall, på grund av att dem är ett IT-konsultföretag, är mycket av deras informationstillgång kundbaserad. Med anledningar till att företaget inte erhåller egen information kan de inte uppnå komponentens mål fullständigt.

Från ett strategiskt perspektiv på sekretess arbetar samtliga företag på samma sätt när det gäller informationsdelning. Stanton m.fl. (2004) nämner att ett resultat av deras studie var att en anställds organisatoriska engagemang hade en relation till vissa viktiga säkerhetsbeteenden från slutanvändaren. Alla anställda på respektive företag skriver på anställningsavtal som hänvisar till tystnadsplikt som en policy vilket innebär att anställda inte får kommunicera vidare om både intern företags- och kundinformation till obehöriga. Hos Företag A och Företag C arbetar anställda även efter kundavtal där kunden själv bestämmer graden av informationsdelning anställda får ta del av. I relation till Stanton m.fl. (2004) resultat har samtliga informanter visat ett djupt organisatoriskt engagemang via sitt beteende gentemot sekretess där alla känner till konsekvenserna som uppstår om företagens uppsatta policys angående informationsdelning inte följs. Genom att ställa strikta krav på anställda värderar samtliga företag sekretess extremt högt för att dels skydda företaget i sig men också deras kunder.

5.1.2 Integrity

Wylder (2003) beskriver integrity som "upprätthållandet av korrekt och fullständig information som inte har ändrats av obehöriga användare eller processer", vilket de tre företagen på teknisk

väg säkerställer med hjälp av backup av information. Samtliga tre företag arbetar med teknisk backup av information, vilket tyder på ett gediget säkerhetstänk vad gäller den tekniska biten. Ett annat tecken på att företagen ser teknisk säkerhet som någonting viktigt är användandet av versionshantering på olika vis, antingen via GtitHub eller interna system.

När det kommer till redigerandet av information är detta tillåtet hos alla företag, där Företag A och B är väldigt strikta när det kommer till vilken information som får ändras. Företag C har knappt någon information hos sig själva som hade varit kritisk att ändra, men har istället regler hos sina kunder för vad de får och inte får göra.

Företagen har alla olika metoder för att säkerställa att informationen de har är riktig, där Företag A använder sig av olika markeringar för att visa på vad som får ändras i vilken utsträckning - vilket sedan kan kontrolleras mot versionshanteringen. Företaget har också en "4 eyes policy", vilket innebär att minst två personer bör undersöka informations riktighet. Företag B använder SecureMail som lösning, motringer vad gäller extern information och förlitar sig helt enkelt på att intern information de får är riktig. Företag C förlitar sig slutligen på att deras kunder håller en adekvat säkerhetsnivå för förhindrande av information. Internt använder sig Företag C mest av sunt förnuft när det gäller riktighet av information i e-mail, till exempel.

Även om företagen är noga med att hålla informationen intakt och säkerställa att den inte ändrats, finns det ytterligare problem som kan uppstå när data sedan skall tolkas. Dhillon & Backhouse (2000) argumenterar för att inte bara informationens integritet är essentiell utan, också för att tolkandet av denna information är något som företag bör fokusera på. Författarna tar upp exemplet då en kund skall ansöka om kredit hos ett företag, då behövs det både information om själva låntagaren men även en korrekt tolkning av informationen av långivaren enligt företagets regler. På Företag B, som är en bank, uppger två informanter att de ibland motringer när de får information och undersöker namn och dylikt när de är osäkra på vem som skickat. Att tolka information som ges till användarna av systemet på ett korrekt sätt är en mänsklig faktor som bör ta stor plats i tänket kring strategisk säkerhet. Även företag A och C bör kunna tolka information de har tillgång till, då främst när det kommer till mail och utskick.

5.1.3 Availability

Wilson (2013) beskrivning av komponentens syfte är att garantera snabb och tillförlitlig tillgång till data. För att uppnå komponentens mål har Agarwal & Agarwal (2011) tidigare nämnt tre tekniska komponenter som måste vara sammankopplade: kommunikationskanaler, säkerhetskontroller och datasystem. Utifrån resultaten har det varit svårt att identifiera om företagen har sammankopplat de nödvändiga komponenterna för att uppfylla kraven för tillgänglighet som komponent.

Precis som i *Confidentiality* upprätthåller Företag A och Företag B en hög teknisk kontrollerad process på informationsrättigheter. Dhillon & Backhouse (2000) argumenterar för ett problem inom komponenten som fokuserar på hur systemfel kan vara ett säkerhetsproblem för organisationer. Företag A använder en process som hanterar så kallade "permissions" där anställda måste skicka och specificera anledningen till deras rättighetsbehov till viss information. I systemets formulär kan anställda klassificera graden deras permission har är vilket innebär att företaget enkelt kan lösa rättigheter och potentiella systemfel fort, för att undvika framtida säkerhetsproblem. På Företag B kan ens informationsrättighet vara beroende av avdelningen man arbetar på och om deras rättighetsbehov anses vara nödvändiga. Inom teknisk säkerhet erhåller

båda företagen även en väldigt stark fysisk säkerhet som försvårar åtkomsten till information för både interna och externa användare där accesskort avgör internas tillgång inom företaget. Baserad på Wilson (2013) och Agarwal & Agarwal (2011) beskrivningar anses båda företagen uppnå komponentens krav genom deras kontrollerade processer och fysiskt höga säkerhet för att erhålla en god säkerhetsgrund för tillgängligheten av information.

Från Företag C:s perspektiv är graden av ens informationsrättigheter beroende på typen av projekt som utförs hos kunder och kunders vilja att dela med information. Företaget erhåller inget system eller processer som kontrollerar anställdas rättigheter, utan det utförs av antigen en administratör eller kund. Företaget har för tillfället väldigt svag fysisk säkerhet, vilket kan innebära stora säkerhetsrisker om obehöriga skulle få tillgång till företagets system. Utifrån komponentens syfte enligt Wilson (2013) anses det att företaget arbetar på ett annorlunda sätt när det gäller tillgänglighet tillskillnad från de andra två företagen. Företaget uppnår kraven för komponenten men på så sätt att garantin för snabb och tillförlitlig tillgång avgörs av kunden.

Att skicka information till rätt mottagare har visat sig vara olika processer hos företagen vilket försvårar avgörandet om uppfyllelsen av komponenten helt. Det teoretiska ramverket nämner inte detta, men resultaten var extremt intressanta för att se hur företag bearbetar detta på ett säkert sätt. Företag A förlitar sig på sina kunder att den givna kundinformationen är korrekt och genom att underteckna avtal har företagen ett juridiskt dokument på samarbetet. När det kommer till personlig information så som avtal och inloggningsuppgifter använder både Företag B och Företag C posten med skälet att e-mail inte är säkert nog. Hur företagen väljer att arbeta med utskick av information visar hur säkerhetsmedvetna de är genom att tänka ett extra steg för att undvika säkerhetsproblem.

6 Slutsats

Även om företagen överlag i stor utsträckning uppfyller kraven för alla tre komponenter i CIA-triaden, är just CIA som modell inget uttalat hos de anställda. Eftersom företagen har olika affärsinriktningar och olika positioner i kedjan informationssäkerhet, ser de enskilt på säkerhet på lite olika sätt. Enligt vår undersökning upprätthåller företagen både teknisk och strategisk säkerhet i en mycket hög grad, även om brister finns som i fall där det inte finns någon uttalad policy.

Resultatet att de tre företagen upprätthåller CIA-komponenterna var för sig stärker tesen att detta är en standard som bör användas inom informationssäkerhet. Vi anser, med vår grunda undersökning, inte att det finns några större brister i upprätthållandet av CIA-triaden, även om studien inte är tillräcklig för att säkert avgöra detta hos företagen. Problemet som vi dock kan se är att synen på CIA-triaden som helhet saknas, även om de tre komponenterna uppfylls. Detta helhetstänk bör ligga till grund så policys skrivs, utbildningar utförs och beteendet i systemet regleras.

För att återknyta till vår frågeställning; *hur arbetar företag med komponenterna inom CIA-triaden och hur påverkar mänskliga faktorer detta?*, kan det konstateras att de tillfrågade företagen genomgående har ett säkerhetstänk som tickar av de olika delarna var för sig, men tycks sakna ett övergripande tänk som medvetet inkorporerar de tre delarna i CIA-triaden som en helhet. Ett sätt att motivera för anställda varför en viss säkerhetsåtgärd tas kan vara att förklara det som en del i ett större säkerhetstänk där alla delars behov skall tillgodoses. Ur en användarsynpunkt kan det vara värdefullt att inte bara få reda på *vad* som skall göra, utan också *varför* - i den bredare kontexten än endast "för att det skall vara säkert", eller något liknande.

Vad gäller de mänskliga faktorerna som påverkar vid upprätthållandet av CIA-triaden är policys som användarna följer ett tydligt exempel på hur beteende i ett system kan kontrolleras. På de två företagen A & B fanns det tydlig policys för hur beteendet i systemet bör se ut ur en säkerhetssynpunkt, medan det i Företag C:s fall inte var lika tydligt med klart uppsatta regler för beteende. Även om Företag C inte anser sig ha värdefull information som kan stjälas, till skillnad från de andra företagens mycket viktiga information, bör det ändå anses viktigt att ett företag som tillgodoser behovet av säkerhet hos andra företag har en uttalad policy om hur säkerhet bör skötas, även om det mesta beror på vilken kund de för tillfället har (se Figur 3.1). Ett företag som tillhandahåller säkerhet bör ha en uttalad intern säkerhetspolicy.

Strategisk säkerhet är något som inte förändras över en natt, utan något som tar tid att undervisa användare om, och med ett gedigen, uttalad policy i ryggen är det lättare att försvara beslut som tas men också att hålla individer ansvariga för brytandet av dessa. Att just företaget som arbetar med att skapa säkerhet har minst koll på vilka policys som finns kan anses bakvänt, men kan med hjälp av mänskliga faktorer i samråd med informationssäkerhetsstandarden CIA-triaden lätt tacklas.

6.1 Framtida forskning

I vår undersökning har vi kommit fram till att om säkerheten haltar någonstans, så är det oftast vad gäller den strategiska biten. För att komma till rätta kan företag införa ett tydligare 50/50-

tänk, där lika stora resurser bör läggas på teknisk, såväl som strategisk. Genom att utbilda användare i hur säkerhet fungerar kommer deras beteende också att ändras, om de tar i beaktande det de har lärt sig. För att göra detta krävs en etnografisk undersökning, där undersökaren blir en av användarna av systemet och också får insyn i hur användarna beter sig för att kunna dra en slutsats för att kunna sätta upp de strategiska riktlinjer som behövs. Ett förslag är att göra en longitudinell undersökning, där uppgifter samlas ihop om samma individer vid ett flertal olika tillfällen för att kunna skapa sig en rättvis helhetsbild. För att få så stor insyn i systemet har undersökningen störst möjlighet att lyckas om den sker internt, för att trygga informationssäkerheten från läckage till utomstående.

Appendix 1: Intervjuguide

Kära informant,

Vi är två studenter på det Systemvetenskapliga kandidatprogrammet vid Lunds Universitet, som tillsammans skriver en kandidatuppsats inom informationssäkerhet och hur den kan påverkas av mänskliga faktorer, inom företag. I vår uppsats kommer vår empiriska studie bestå i intervjuer av anställda hos företag för att samla in data angående medvetenheten och användandet av säkerhet inom företag. Tidslängden för intervjuerna kommer att vara runt 40 minuter och spelas in. Informanterna kommer att förbli anonyma och endast deras ålder och arbetsroll kommer att användas som väsentlig information i jämförelsen.

Intervjun börjar med allmänna frågor angående företaget och informantens roll inom organisationen. Sedan kommer vi att diskutera informationssäkerhetsaspekterna inom organisationen: vad känner ni till om det och hur förutser ni förbättringar, om det finns. Detta gör vi genom att tackla tre väldigt viktiga informationssäkerhetsaspekter: confidentiality (sekretess), integrity (integritet) och availability (tillgänglighet).

1. Beskriv din avdelnings uppgift inom företaget.
2. Berätta om din arbetsroll (vad den omfattar, hur länge har du haft den).
3. Berätta hur företaget arbetar på säkerhetsnivå (Går ni någon utbildning, policys).
4. Vad innebär informationssäkerhet för dig?
5. Har företaget utbildat dig inom IT-säkerhet?
6. Hur ser ni på IT-avdelningen? Vad tycker du är IT-avdelningens roll?
7. Hur ser fördelningen av resurserna mellan strategisk och teknisk säkerhet ut?

Confidentiality

Tekniska frågor	**Strategiska frågor**
Vilken sorts information har du tillgång till och med vilket tekniskt redskap?	Vad har företaget för policys angående informationsdelning?
Vad använder företaget för säkerhetsutrustning till information?	Inom sekretess policys, vet du om vilka policys som finns? Vad får du dela med dig till utomstående och var går gränsen?

Integrity

Tekniska frågor	**Strategiska frågor**
Hur arbetar ni med backup av information?	I vilken grad får ni ändra information? Om ni får, hur gör ni det?
	Hur säkerställer ni riktigheten av information?

Availability

Tekniska frågor	**Strategiska frågor**
Utifrån de teknologiska systemen du har tillgång till, har du någonsin upplevt att du inte kommer åt information som du behöver?	Vad har er avdelning för policys när det gäller utskick av information till rätt mottagare?
Vad använder ni för säkerhetsprogram?	
Hur ser företaget på säkerhet mot utomstående? (Murar, tillgångskort till byggnaden)	

Appendix 2: Företag A, Individuell intervju, I1

F1 = Författare 1
I = Informant

*Informanten identifieras som **Global account executive, 53.***

1. **F1: I'll begin by asking you what your age is and what language is used within the organization?**
2. I: So I am almost 53 years old, and English is our corporate language.

3. **F1: Super. Could you describe what your department's role is within the company?**
4. I: Our department's primary role is to sell, so we sell software. And we're also responsible for a certain number of global customers, so besides having the target to sell new licenses to these customers, to enable greater business support we also serve them from a customer relationship perspective so that we are holistically responsible for the Företag A:s relationship with these customers.

5. **F1: Okay. Could you explain what your role is within the department - what do you work with and how long have you had that role?**
6. I: I've had my role now for 3 years to be exact and I work as a global account manager for a few customer accounts.

8. **F1: Okay, what does that work entail?**

9. I: Well it entails being really - ultimately the single point of contact for these customers and because they are large global corporations. I interact with their departments which are also spread all over the world. Primarily from the IT side but even from their business organizations. Ultimately, you know I see to it that their needs are met, that from our company we are not only responsive but that we're also proactive in our relationship with them. That we share with them information about things that other customers do that is of interest and value to them also. And ultimately, I am responsible for the selling of more software from the company's interests and from the portfolio of both existing as well as new software that has come to the market within the lasts you know, months and perhaps a year.

9. **F1: What is the name of your business role?**

10. I: Global account executive.

11. **F1: Super.**

12. **F1: How does the company work on a security level? Do you guys receive any training, or are there any policies that you have to follow?**
13. I: Yes, we do receive training and we do have the security policies that we have to follow and especially when it comes to information security. So these are mandatory trainings that we need to take because it is a certification that the company has ensure for each and every one of us, and then depending on what type of role one has, there

could be perhaps additional type of certification compared to other people that have other roles.

14. **F1: Alright super.**

15. **F1: We define information security as the following: "The protection of information from being stolen or used wrongly or illegal." What does information security mean to you?**
16. I: Exactly, just what you said, it means exactly that. So that we have to ensure that the information we share with others internally as well as externally is correct. And that people who receive information from us can also be sure in understanding the information they should have received is properly viewed and reviewed before it being sent.

17. **F1: Yeah**.

18. **F1: This question is a little bit repetitive, but has the company given you any training within IT-security?**
19. I: Yes it has, absolutely. On a yearly basis and I just recently got training about 2-3 months ago.

20. **F1: Alright, do they constantly update you with new information and stuff or is it the same training?**

21. I: No it's new information of course because within new information security area new things happen all the time and without a doubt the infiltration that takes place on a global level. I work for a company which is well-known and it's a very important company to most of our customers so it's incredibly important for the company to ensure that the information that we handle is obviously handled in a legally and responsible way. And that also when it comes to even application security that we have, when we send information and how we send it and so on that it's also secure.
22. **F1: Mm. That's perfect.**

23. **F1: From a personal view, how do you perceive the IT-department? What do you think is the role of the IT-department?**
24. I: Well there are different parts of the IT, or sub-organisations you could say in the IT-department. So perhaps some parts of the IT-department see to it that the users such as myself can be up and running with the tools and the applications that we use. So that's kind of like the local IT-departments role. But when it comes to information security and application security then there are other organisations within the company that handle that. They are not locally present but we know where we're supposed to turn to. So should perhaps I feel like, and yes the other thing is to - recently I had a case where I felt like "Is it somebody or like a virus that is trying to attack my application?" when I was doing some work and then especially from the extra sites that one goes out to. So I went and I contacted my local IT-department, they came over and looked at it and no it wasn't that. So they can be used in different ways and they are a conduit to the people that work with information security and who work with securing our applications performance.

25. **F1: Mm. When you mentioned applications, do you mean - are you referring to the programs that you use to conduct your work?**

26. I: Yes exactly. It could be Word, it could be Excel or other types of applications. Adobe and so on that we use in order to work with the documents that we work with and the types of format that they are saved in.

27. **F1: The last question on the general overview or aspects and stuff, how does the distribution of resources between strategic and technical security look like at the company?**
28. I: I don't really know.

29. **F1: Mm, that's fine.**

30. I: But I would think that when it comes to strategic that there would be very few resources compared to the technical security resources. Because the technical security resources are the ones that are actually preventing, they are both perhaps developing and preventing certain types of information infiltrations. But the people that work with the strategic, I would assume that they would be fewer, that they would be updated on the types of let's say, viruses that are out there and what the means are to control them and prevent them and to ensure that the people in the company - that there is a program in terms of how we can get that information so that we immediately can act in a different way should we need to do so.

31. **F1: Yeah.**

32. I: Based on the types of attacks that are happening in the background.
33. **F1: Yeah, would you say - it's not a 50/50 balance, but is it closer to 50/50 rather than an 80/20 division?**

34. I: Yeah, if I was to guess I would probably 80/20 or 20 strategic and 80 technical security. Yeah I would say something like that.

35. **F1: It is a good estimation. We are going to move onwards towards the 3 components within the CIA-triad. The first component is confidentiality and the question first is:**

Confidentiality

Technical questions:

36. **F1: What security equipment, from a technical perspective, does the company use towards information? Do you know if they user firewalls, VPN tunnels?**
37. I: Yes, they definitely use that plus of course certain types of virus programs and what have you not. So yes we have software that's installed like for example McAfee but then in the background, I'm sure that they would use all of the latest technology in order to fight off any sort of attacks.

38. **F1: Yeah. So they would have pretty high security programs.**

39. I: Yes absolutely. And we as a company also have security programs for our own applications so the types of, these are special programs which don't exist on the market place, they're literally provided by Företag A to protect Företag A:s applications or to definitely increase the level of security.

40. **F1: Okay.**

41. **F1: What sort of information do you have access to and with what technical resources? This question focuses on in order to do your job, what information are you in need of?**
42. I: Well there is certainty in my role - I obviously have to have access to to certain type of information. So for example one of the most sensitive types of information is pricing, so and you know customer information and so on, and whatever is needed for my role - I have access to. And then the types of documents that we work with, it's everything from confidential to you know general public type of classification. It depends on my role but I have access to everything that I need and in case I'm missing something, then I just ask for a certain type of access right and explain why I need it.

Strategic questions:

43. **F1: You mentioned earlier that depending on your customers you might share information of other customers to get inspiration. What policies does the company have towards information sharing?**
44. I: Mm and here also we are very respectful about the policies that our customers have. So when it comes to customer information, we reveal for example if we're talk about a customer in a certain context, we don't necessarily say what the customer's name is. But we could say that we have a customer who has a system setup that looks like this and then this is what they did in order to make certain improvements, in order to get better efficiency. So without giving any customer information, we just describe a scenario, a business scenario that the customer improved through the help of our products of our software.

45. **F1: So you give a general overview?**

46. I: Exactly, so some customers it could be that and we're not even allowed to say what the customer's name is and that's because of the type of confidentiality agreement that we have with these customers. Other customers are perfectly fine if you mention their name in a certain context and so on because to them that's not considered to be confidential information of the highest grade. But we never reveal something that the customer has not signed off. So we have for example customers' success stories and those are descriptions of the customer's business transformation which the customer has signed off. So it's just as though you were interview a customer and write an article to publish somewhere, and the customer approves that article and the content in it. It's the same sort of level. So it depends but it's very much in conjunction with what the customer is okay that we communicate.

47. **F1: It's good. I notice that you're aware of the current policies which is excellent.**

48. **F1: Continuing on within confidential policies, what are you allowed to share with external parties (such as family and friends) and where does the limit go?**
49. I: Again, everything that is considered to be company confidential or customer confidential we don't share with family or friends outside of the company or even other customers. So confidential information, because we're privy to it, it's just that it's confidential. And we all know when we start working at this company, we sign off papers promising to uphold the types of policies that the company has. It doesn't matter if it's coded, it's a code of conduct what this falls under and what type of category it is. But information confidentiality is strictly governed and if someone goes outside of those boundaries of what the boundaries allow, then one could literally be fired and that's also something that one understands. It's a consequence if a certain type of behaviour is transgressed.

50. **F1: Is the amount of confidential information the same when you talk about one customer who allows you to - they don't need to be anonymized - , in contrast to a customer that wants to anonymous? Is it still the still the same level of confidentiality when you step outside the office?**

51. I: No it's not the same level of confidentiality, that's correct. Because if you do have, and of course I can talk about customers and use their name in certain contexts. But it's still, for example for me, unless I'm speaking with colleagues, I rarely speak about my customers unless it is with people that perhaps know the customer or work with the customer from their company perspective. So then it's a little bit different and especially if they know, for example I could be speaking with let's say Customer 1, is a partner with Företag A, and if I speak with Customer 1 about a customer which is both mine and their customer, and the customer knows it then that's fine. You see, so then the customer is also okay that we have an open dialogue internally between us. So it really depends but one has to be very very careful.

52. **F1: That's understandable. We'll be moving onwards with the second component of the triad which is integrity where the first question is as followed.**

Integrity

Technical questions:

53. **F1: How do you work with information backup?**
54. I: We have an automatic backup that takes place. So every day while I'm working, a backup is performed. In my case it's automated, I have asked them to do that otherwise I would have to manually do it in that case. But for my part it's always backed up so that way I can be rest assured that the majority of information that I'm working with will not be lost. Potentially it could be a couple of hours of something but it's automatically backed up.

55. **F1: That's really good.**

Strategic questions:

56. **F1: To which degree can you alter information? If you can, how do you do it?**

57. I: If you alter information it is because you have the right to publish in a certain document. So if I for example publish, let's say a certain document, an official document where only a few people have the right to edit it then I would have to have those rights to do that. Otherwise if I for example take a powerpoint presentation that says "Confidential" and it comes from the project management group, and it also say "Internal confidential", then that is a piece of paper that I don't own and I don't have any rights to edit that even if it's in a powerpoint format and not PDF.

58. **F1: Oh okay.**

59. I: Do you see what I mean? And I can definitely not share that piece of information, that document, with for example customers because that is an internal confidential document. But we can for example create, I can create a confidential document which I send to a customer and perhaps it's a document that I share with another colleague, then the two of us can update it as needed based on the dialogue that we have with the customer. But the customer cannot for example update such document so it really depends.

60. **F1: Since you can alter information that you have access to, how can you assure the accuracy of information? How do you know it hasn't been altered by anyone else when you use it or send it to a customer?**
61. I: Well usually documents have a tracking history so you do have an understanding of when it was last altered or edited and by whom, and which version it's in. So if the version that you're working with is the latest version, when you edit it you put it in a table or whichever way, because a lot of this is done electronically, you know it's like a stamp basically that stamps when you're editing it and of course it has to be saved in another version.

62. **F1: I'm thinking that since you said that before you send anything of to customers you always look over the documents to make sure that everything is the way it's supposed to be. With track changes people can log into other users' accounts and alter information but do you still feel that the information that's in the document is still as accurate that it's supposed to be?**

63. I: I assume that it is. I can't be 100% sure but somebody else should not be able to access somebody else's account and make for example changes. Because that is literally then an infiltration and that is not allowed. If I make a change into a document that is perhaps centrally stored somewhere, I go through my own computer or through my own access rights, right? And those are all tracked and traced. So it's a little bit of that "Big brother is watching you" -effect but I mean there is traceability when it comes to all of these sort of sensitive information accesses.

64. **F1: So the company still has really high security in regards to track changes and tracing devices?**

65. I: Yeah. I mean I don't know personally because then one would literally have to speak with the IT-department that works with these issues and questions to see what level of security it is. But yes, we are definitely aware of the fact that, you know, you're not allowed to do things that you're not permitted to do and you should not be

trying to access information. Even if you should get access to something that you should not have access to, then you actually should a) close it and not look into it further perhaps. Let's say if I were for example able to get access to stuff that actually my manager is supposed to have access to but not me, that's not correct then that I should keep on looking at that information and so on. So naturally those types of weaknesses that can occur but it's rare because it's role-based access rights. I mean to me personally it has not happened but I know of somebody that this has happened to in a previous company.

66. **F1: Oh okay.**

67. I: Yeah, that is why I take it up as an example.

68. **F1: That's a really good example. We are going to on to the last component which is availability and the first questions follows:**

Availability

Technical questions:

69. **F1: Based on the technical systems you have access to, have you ever experienced that you cannot access information that you need?**
70. I: Yes and that sometimes you'll get an error message. So you press a certain link or want to get into something and there is an error message - perhaps "that link is no longer active", "the document has been moved" or "certain type of information has been moved" or maybe perhaps also there is a system instability. So things can happen but it's typically some sort of error message in terms of "that link is no longer an active link to that information" and then you need to find out "Okay where has that document been moved?". For example pricing, I mean some of that stuff has changed place and sometimes it can be difficult when you press a certain link and there is no content behind it.

71. **F1: Is it easy for you to fix those issues?**

72. I: Yes because you log an IT-ticket. So you log a service ticket and then you can also grade the severity of that issue. Is it low or medium or high or critical? For example for me when I'm working with the job that I have, if I have to do certain things in the system in terms of getting approvals before I can go out and present an offer to a customer, for me it's critical that those links and that information flow works and I have had problems when some things have not worked the way they should and so on. I've logged a ticket and then put in "Critical" and literally you will have a call within just a few minutes. So it's like a red alert that goes off to the people that work with solving those issues because it is business critical.

73. **F1: That's really good. It seems like the company really has thought of how to handle both critical issues and security issues.**

74. I: Absolutely, and for us, for example e-mail/Outlook, I mean for me it is incredibly important that Outlook works and that I can get my e-mails and that I can send e-mails

because so much of my work is working with the tool called Outlook. So if I have issues with Outlook then that's a very high severity issue that needs to be looked at a.s.a.p. And either the local IT can try and help or they have to put in a ticket and send it off to the next level of IT support. And that is because things like this have happened.

75. **F1: The next question is a little bit repetitive, but it's just to ask again what security programs do you use or does the company use internally? You mentioned McAfee which is a great program, are there any more other than McAfee?**
76. I: McAfee is at least what I know of because it does a virus scan and search and so on constantly. But I'm not 100% sure. I think we obviously have corporate programs and I could look into it and see if I can find out but I say it's McAfee because this is what's installed on the computer right from the beginning.

77. **F1: Yeah that's not problem, that's great.**

78. **F1: What is the company's view on security towards external parties? This question focuses more on physical security. Do you have access cards to get into the office, do you have high gates? What's the level of security they have towards external parties?**
79. Yes it is access cards and so for employees it's access cards and also to example printers and different types of tools. So it's a networked environment. And then for external people nobody can come in unless they are going in through the reception so they have to register and so on. It is strictly forbidden to take anybody, for example like family member or friends. It is forbidden to take them into a part of the company where they're not meant to be.

80. **F1: Okay.**

Strategic questions:

81. **F1: Finally which is the last question for availability, what policies does your department have when it comes to sending information to the right receiver?**

82. **F1: This goes a little bit towards you mentioning that you send a lot of information to your customers, and how do you know that the information you're sending is the right amount of information and not to much or confidential**
83. I: Well if we are sending confidential information it is visibly marked "Confidential" and usually with these customers also, if it's something very specific and scenario-based type of confidentiality, we might even sign an NDA specifically with the people that are receiving the information so a non-disclosure agreement. But otherwise, because some of these customers we have had for a long time, we have an NDA that is already in place and it's kind of like a corporate NDA. I mean you can never ever fully control the flow of information between people but ultimately there is an agreement between companies to guard the information and to safeguard it when it comes to confidentiality. I think that people work in a very professional way for most parts so if I send pricing information to my customer I should be able to trust that they would not send that information to my key competitors and they won't. That's the way it works because there is a professional agreement between companies. Should that type of

document come out into the wrong hands, and it has in the past I've seen things like that in the past at other jobs, then of course it can happen. But at the end of the day something as sensitive as pricing for example, it's all scenario-based. So it's customer specific you know right here, right now. So it has perhaps some value for a certain amount of time, but ultimately not really too much value because it changes constantly. It is very customer specific and case specific. So even though it's extremely important and has value - it doesn't have value for a very long time.

84. **F1: Okay, and that also seems to be the purpose of setting up those policies and sending that type of information - that in time it will lose its value.**

85. **F1: Those were all of the questions that we had, so we are wondering if you have any further comments or something you would like to add.**
86. I: No I think I've said basically I told you more or less how I work and how we work and the types of specific scenarios that I have. Naturally people in other roles have more particular, especially those who create certain type of information and documentation they have to classify certain way. I mean everyone has a code of conduct training that they have to take every year. So it's an update to refresh on it. We just had now a compliance training on Thursday which I also participated in. So regarding all kinds of legalities that we need to be aware of and then there is of course security, information security, and constituting offers and promises to customers. Things that we're allowed to do and things we're definitely not allowed to do and even in an e-mail perhaps if somebody writes something in a certain way. An e-mail is a legal document which can be used in the future and in a court should one have to end up in a certain sort of unpleasant situation. I think that we have all the right training and right information to know what's right and what's not. And if we're unsure we also know where we can go to ask questions. But if we break these rules and potentially do things without intending to but do things that can result in commercial and business disruption, or legal suits, then literally people understand that they can be fired because that is the type of severity that is transgressed and it's a consequence. And that happens also on a yearly basis - some things will happen around the world where people will actually be asked to leave their position because they have made such a big mistake that its cost the company not only problems but also cost and financially to settle.

87. **F1: Maybe also customer relationships.**

88. I: Absolutely, absolutely. And that's why it's very important for me and my role, I cannot over promise, I cannot say things that are not true or correct, I cannot give an impression that we're doing things and will deliver in a few months. Somebody has not signed off that that can actually be communicated to the customer and especially when you are developing new software, even new products and software. Things that are in development it's only product management that can sign off what can be told to the customers and promised to customers - nobody else can. So for me it would be a great mistake if I was to promise things to customers and they would buy for example certain products today because other products - they would assume are coming in the next few months. That is totally illegal and irresponsible and that's the type of behaviour that could cause employment termination.

Appendix 3: Företag A, Individuell intervju, I2

F1 = Författare 1
I = Informant

*Informanten identifieras som **Maintenance Sales Manager, 52.***

1. **F1: I'll begin by asking you what your age is and what language is used within the organisation?**
2. I: My age is 52 and I use English 99% of the time in the company.

3. **F1: Alright, super.**

4. **F1: Could you describe what your department's role is within the company?**
5. I: We look after the maintenance revenue in the Nordics and the Baltics or within the company. And what we try to do is obviously we try to grow that revenue stream and we try to protect it as well. We do this obviously by looking at the demands from the customer and where they actually want to go in the future. So we get closer to the customer, see where they want to go and try and help them get there. And by doing that, hopefully by protecting - grows the revenue stream as well.

6. **F1: Okay. Could you explain a little bit what your role is within the department - what do you work with?**
7. I: Sure. For me, I look after that revenue stream within the Nordics and the Baltic. I look at anything that affects that revenue whether it's up or whether it's down. I obviously just sort of try to grow this by sort of meeting with the customers or sort of taking on various cases that would affect the revenue. So it's also coordinating for all of the regions, basically sort of represent this revenue stream and if there's any kind of problems or escalations they will come to me. If there's any deals on the table that affect this revenue stream, which most of them do actually, most deals do, they will also sort of come to me so I can decide whether or not they should go ahead or it should be change in any way.

8. **F1: How long have you worked with this role?**

9. I: 3 years. I've been working at Företag A for 3 years now.

10. **F1: What would you say your role is called? What is the title?**

11. I: It is the Maintenance Sales Manager.

12. **F1: Alright, super**.

13. **F1: How does the company work on a security level? Do you guys receive any training, or are there any policies?**
14. I: Yeah, there are a few different trainings that take place and that's usually at least once a year. So they will do some sort of certification and it depends on the different kind of security training whether it's compliance security or whether it's a common

sense security. These usually happen, I say it's mandatory and a lot of the times you do have to do tests for this. They are not also totally straight forward so you have to use your brain a bit and really pay attention to what you say "yes" or "no" to. That happens you know like a couple of times a year but then of course the security that you have and what you're asked to do is different depending on what kind of job you have, what kind of classified information you have access to, what type of customers for instance that we have. So that all depends if it's a lot within the organisation, depending on what you have access to.

15. **F1: Would you say that you receive new information for every new training that you have or is it the same information?**

16. I: Some of it is new so they do try to change it a bit and bring new kind of elements into it or a new stance. A lot of it is pretty much the same I would say actually and a lot of that has to do with compliance law security on that and security on information.

17. **F1: Okay super. We are going to define what we feel information security is.**

18. **F1: We define information security as: "The protection of information from being stolen or used wrongly or illegal." What does information security mean to you?**
19. I: I think that is an excellent way of actually putting it, to be perfectly honest because it sort of like widespread, in a sense. It's the information that can be taken, misused or even used without permission as well. I think you summed that up really well. I will stick to your meaning of it.

20. **F1: This question is a little bit repetitive, but has the company given you any training within IT-security?**
21. Yeah, it has. They have to, and we have various certifications at different times of the year. So yeah, of course, if something actually happens or something big hits the news or something then maybe you get additional sort of information that you may be aware of and have to make sure that it doesn't happen.

22. **F1: Okay so the company is pretty good on giving you recent updates as well.**

23. I: Yeah, for sure.

24. **F1: Alright, that's really good.**

25. **F1: From a personal view, how do you perceive the IT-department? What do you think is the role of the IT-department?**
26. I: I think it's huge, do you know what I mean, especially at Företag A. It encompasses obviously everything. So whether you're talking about IT from a very practical level you know sort of the tools you use like laptops, computers or iPads sort of from that angle to the people who have got the infrastructure. To manage the networks and then you've got all of these sort of programs that's within it as well. So the IT-department expands over everything. I'm sorry, I don't think I'm doing a very good job at explaining this at all…

27. **F1: No, no don't worry. You're doing a really good job. Don't worry about it.**

28. I: So I'm not really sure to be honest because what was the question again? Can you repeat that please?

29. **F1: How would you perceive the IT-department? What do you think their role is within an organisation?**
30. I: Yeah so then again it is back to that it could be everything. Being involved to make sure that we have equipment that works, that's compatible and that we can develop on it and that it's not ready for now but that it's ready for the future. And the same for the programs, that our infrastructure is secure and that we also have the training as well to be aware of things that could affect the way that we do business. So it's on a very broad basis the department and it should be touching upon everything.

31. **F1: That's a really good answer. We're going to ask the last question on the general overview of information security etc.**

32. **F1: How does the distribution of resources between strategic and technical security look like at Företag A?**
33. I: I remember when I – I know that when I read this question from the sheet when you sent everything, you know that at Företag A we're pretty good at security in the fact that a lot of it is in the need to know. So we don't broadcast a lot of things, even internally. So if you look at somebody who really know that information I could ask for it at Företag A there are probably a few people that could tell you that we've got this many in strategic and this many in the everyday works and everything. I really don't know what that would be, as I say I think this is solid ethics that they don't tell anybody this. Because you know it obviously weaken our position and if everyone kind of knew where the break of it was, the resources and stuff.

34. **F1: Yeah that's a reasonable answer as well. It's definitely okay if you don't know so we understand that.**

35. I: I don't think many people know as I say. I don't think many people know at all because I know that some our customers that I actually have got have high security and it's very rare that even the checks that you do when you get to that level is just phenomenal. Hardly anybody in the company know, it's just a handful of people to need to know certain things.

36. **F1: Yeah but that's understandable. We're going to go onwards with the three components within the - it's called the CIA-triad - and the first component is confidentiality. So we are going to ask a few questions about that one.**

Confidentiality

Technical questions:

37. **F1: The first questions is what security equipment, from a technical perspective, does the company use towards information? Do you know if the company uses firewalls or VPN tunnels?**

38. I: Yeah they do. They use the firewalls and various sort of tunnels and things and I think anything at all that's there for security - we use.

39. **F1: Okay.**
40. I: So whatever you can think of and obviously for us being an IT company you know, we've got access to everything so everything is checked and any kind of security we get put on something do.

41. **F1: Alright that's really good. It's good that the company is also aware that they want to increase their security by getting the latest and the best there is.**

42. **F1: What sort of information do you have access to and with what technical resources?**
43. I: Well I've got access to most information to be perfectly honest and how to get into this technically - a lot of the time you have to ask for permissions of course. So you would fill in various forms and ask for permission and say why you actually would need certain things. And depending on how much security information that you actually get access to, obviously it depends who needs to verify this information and who needs to approve or disapprove it. I don't know if that answers your question or not? I feel as if I'm being very vague but I'm not actually.

44. **F1: No, no, no. I understand also if there are a few things that you can't say but whatever you feel is good enough then we'll take that.**

45. I: Great.

Strategic questions:

46. **F1: What policies do the company have towards information sharing?**
47. I: I don't know if they've got any policies, it's a good question so they probably have got policies for everything but I'm trying to think of what that is - I'm not quite sure on. I know that some of the times that obviously if you mark something that is confidential then you have to really really make sure that it doesn't go anywhere. Whether it's just internal-only information or whether it's even confidential within the internal bracket. I think there is a set of rules that kind of dictate what you can and you can't do with that and that would also involve where you store these things. You know whether you store it on a kind of drive that everyone has got access to or just a few people, things like that.

48. **F1: Yeah. Do you think it could also depend on the customer that you have?**

49. I: For sure, absolutely. There are certain customers that are very limited and are very security sensitive and that's a totally different ball game, that really is.

50. **F1: That's really smart.**

51. **F1: Within the confidential policies, are you aware of the current policies? What are you allowed to share with external parties (such as family and friends) and where does the limit go?**

52. I: Mm, good question. I'll think about this. Obviously the inside of trading part of things for myself and a few other people who have got access to you know information that is really going to affect the stocks and shares. For us there is a set of rules where you can't actually talk about certain things. And then of course we can't actually tell friends or family to go on on the stock market at a certain blackout time for instance.

53. **F1: No.**

54. I: I think that some of it is just pure common sense you know. There is the odd thing that is isn't really sort of set to anybody about anything when it's a very high security. But other than that it's just common sense about what you say and what you don't say.

55. **F1: That's good. We'll be moving onwards then with the second component which is integrity. And the first question is as followed:**

Integrity

Technical questions:

56. **F1: How do you work with information backup?**
57. I: Well there is a backup that's run every night, that's one thing. So that's quite good so obviously if something sort of crashes, there is something there. And obviously service backups as well. You can't do it much quicker than that. So you do it every few hours or whenever you actually want to do it. But other than that I think that's about it. You don't obviously for instance put anything on a carded memory stick you know, just in case you lose it or something. There is some sort of backups that's there and backed up and that's also with passwords and everything. So it really depending on what you've got and where you're going to store it, and how you're going to store it really.

58. **F1: So the company, they automatically update most of their information that you guys have?**

59. I: I would say so yeah.

60. **F1: Alright.**

61. I: Or at least for mine, yeah every night and everything.

62. **F1: That's good.**

Strategic questions:

63. **F1: To which degree can you alter information that you have access to? If you can, how would you do it?**
64. I: A lot of it yes. A lot of it you can actually sort of alter and change, and some of it no. Some of it that they've said "Right this is the standard for whichever reason" you

know you can't actually alter it and you just wouldn't. If you desperately, desperately wanted to alter it you would have to go and ask for permission to do so.

65. **F1: Okay.**

66. I: So they treat that really quite seriously if there is something that's not supposed to be altered and you try to use it in another way without permission you know it's not a good thing.

67. **F1: Alright.**

68. **F1: If you were allowed to alter information, how do you assure the accuracy of information? If people have the same rights towards a document knowing that they can also alter information, how would you assure the accuracy of information?**
69. I: I think that obviously other than asking for a review before anything gets sent out you know, that would happen. And is does actually have happened that when there is a certain, say presentation or a document that is going to go out, you always have in the end "Can we do a review before it goes to whoever it's supposed to go to? ". But obviously this depends on what the information is and who it's going to like if it's going to the broader market or going to a public site for instance and then there is a hell of a lot of checks that's done before it usually hits there. If it doesn't then something must have fell through the hoops by now basically but most of the time it's all supposed to be checked and double checked before it hits the public.

70. **F1: Yeah okay. That's smart and a good way to know that the customer doesn't always get random documents - that everybody actually has reviewed them.**
71. I: Well the thing is that obviously it depends like where it is, if you're doing an e-mail do you know what I mean, where it's to correspondence and it's "Okay we'll hand it this week". All of that is kind of an everyday thing but if it's something of significance then we've got this "4 eyes" policy and it's sort of better to have a few people looking at this rather than just one.

72. **F1: Yeah, no that would make sense. We'll go on to the last component which is availability so there are just a few more questions.**

Availability

Technical questions:

73. **F1: Based on the technical systems you have access to in order to do your job, have you ever experienced that you cannot access information that you need?**
74. I: Oh god yes. I was really laughing when I saw that, so yes absolutely, it was like "Absolutely, oh god". Yeah the thing is for my job - it's so wide on what I need to access and you know you can do some wonderful things and there are so many different system that you've got. I think sort of for my job it's a bit different to most other people's jobs. There's only like in each region there's probably about 2 jobs that are you know what I do, in each region. So it's quite unique, so you do need to access loads of different types of information and as I mentioned before is that you have to apply for permission yeah. So apply for permission and then you have to send this off and you

have to say why you are asking for this permission and everything like this. A lot of the time, especially sort of when you, I know people showing me different things, different systems, when I first started, things like how does this kind of work and what does it do. And then when you would write it on the format for permission, you never heard back or it was rejected. You think "God what was that permission for again?" because it means nothing to you because you never used it before. So yes, unfortunately the negative part of this thing is that even today, even today I am still saying that if I has access to everything you know, it would be really nice. I would be able to do some nice things much quicker and more efficiently.

75. **F1: How long would it maybe take to get your permissions?**
76. I: Hahah I think I'll sooner retire. No honestly I wouldn't go back there. The thing is that it is just so difficult so that some of these things, I just said that I can't even remember now "What the hell do I forward" so it's just like live without it you know, It's like somebody says "Guess what, this is really good for you." so I simply wouldn't bother unfortunately. I've got too many other things I need to do without going back there. I have a very big stress in my life without putting that on it.

77. **F1: We are also wondering what security programs do you use.**
78. I: God, no idea in an easy answer. Sorry, no idea. I haven't got a clue of what they use.

79. **F1: Yeah, do you have on your own computer, do you know if you have any own security anti-virus programs?**

80. I: Probably, I'm sure that we we've got everything that runs but I'm just trying to see. I haven't really like McAfee and everything like that, that just sort of come up, I've got nothing that really just comes up and that's a security program. So we've probably got things there but we just don't see them, they'd be behind the scenes I think.

81. **F1: That's alright.**

82. **F1: What is the company's view on security towards external parties? It can be physical security by having access cards and gates and codes.**
83. I: It's pretty good but to be perfectly honest I think that these things can always be better than what they are. Years ago I used to work for a security company, IT-security company, that's called X and they were red hot on like encryption and also you know these cards to get into buildings and everything like that. And I think that here of course we've got cards and codes and we've got cameras and we've got things, these basic things - certain doors that have got different codes in. I still think on the whole that we're way behind on what we should be on the physical security, on the cameras and access and things like that. I think it's a shame really to be perfectly honest and we're not the only ones. You see it everywhere, you see it absolutely everywhere. You know so we should have you know cards that have got a hell of a lot more information on them, you know so there is actually nothing to stop - of course it costs money, but fingerprint technology of going in and things like that. It really should be better than it is, definitely.

84. **F1: Maybe sometime in the future they will be able to.**

85. I: Yeah but it is crazy when you think of it, when you think of how long this technology has been available you know. Very few places is still adapting to it, it's just craziness you know.

86. **F1: It's understandable yes. We have one last question to finish off.**

Strategic questions:

87. **F1: We have one last question to finish off and that is what policies does your department have when it comes to sending information to the right receiver?**

88. **F1: It's a little bit how you know that the information you are sending to a customer, how do you know what hasn't been altered on its way but also that the receiver is the right person?**
89. I: Well there isn't, I don't think there is any policy you know on that. I've never seen it put it that way. I think you have the common sense prevail and you know sort of people realise that "Okay, this should go to this person and everything else" and that "This is the correct person to receive the information". But I don't think there is a policy that you know says that "Okay certain people shouldn't have this kind of information". I don't think so any way.

90. **F1: Okay. You've had really good answers and we appreciate your time both for the interview and taking your time for looking at the questions.**

91. I: No problem at all.

92. **F1: Thank you so much. We're just wondering if you have any final comments or anything you would like to add that you felt like you didn't have time to say?**

93. I: No I think everything was fine. I just want to wish you good luck with your thesis.

Appendix 4: Företag A, Individuell intervju, I3

F1 = Författare 1
F2 = Författare 2
I = Informant

*Informanten identifieras som **Local legal counsel, 35.***

1. **F1: So I will first and foremost ask how old you are.**
2. I: 35.
3. **F1: You are 35?**
4. I: Yes.
5. **F1: Super okay.**

6. **F1: Could you describe a little bit your department's role within the company?**
7. I: I am working for the legal department and we are providing legal support to business, sales and other departments within the company.

8. **F1: Okay, alright and could you describe what your role is and what it includes?**
9. I: I'm a local legal counsel so basically I'm negotiating the contracts related to the deals that we have, contract review and drafting, corporate issues, compliance issues and other legal tasks.

10. **F1: Alright and what's the role called?**
11. I: Local legal counsel.
12. **F1: Okay, alright and how long have you had it?**
13. I: I think for 8 months.

14. **F1: Okay. Could you describe a little bit how the company works on a security level?**
15. I: Actually you know, I only have access to a part of this information which is mostly generally available to the employees. But I think that Företag A is taking this extremely, extremely seriously so there are a lot of security programs implemented at Företag A:s, policies that have to be followed by everyone and there if a high focus on a continuous training and information as to the different disclosure rules depending on the type of information. The training is mandatory for all employees and it is continuously improved and followed-up..

16. **F1: Alright, super.**

17. **F1: Could you give your personal view of what information security means to you?**
18. I: Okay this a pretty tough question. I think that it is just a way to enable you know safe ways doing business and being compliant with the applicable laws, but also protecting the confidentiality of the information that is specific to us and also just making sure that we are compliant overall I think, yeah.
19. **F1: Alright.**

20. **F1: Has the company given you any training within IT-security?**
21. I: Yeah I think it is part of the main security training you know- how to handle your password and access rules. We also have online trainings that are mandatory to be passed and followed up and the training attendance information is visible for the responsible managers. So it's a very transparent and well-managed system.

22. **F1: Yeah, that's good.**

23. **F1: How would you perceive the IT-department? What do you think is the role of the IT-department?**
24. I: Because you know we are working for sales organizations in Sweden so I think that the IT-department here basically support the roll-out of the IT initiative undertaken at a company level. The IT policies are run within the entire company.. The local team within IT department main act as a support department for the local entity. I think that my opinion is not really representative for the complex set-up and role of the IT department throughout the company, as I use the internal IT services in my position of an employee. So it depends. For myself as an employee it's just a support because I don't really directly need them otherwise.

25. **F1: Yeah, no but that's fine. We're more interested in what you think their role is.**

26. **F1: How does the distribution of resources between strategic and technical security look like at the company?**
27. I: Actually I don't know.

28. **F1: Okay that's fine.**
29. I: I don't know.
30. **F1: Okay so we are going to go onto the three different components within this triad and the first component is confidentiality. And the first question is:**

Confidentiality

Technical questions:

31. **F1: What security equipment does the company use towards information?**
32. I: Infrastructure wise?

33. **F1: Yes. If you have an idea.**
34. I: No, not really. I mean I'm not really sure how this is done technically but we are using separate folders with passwords and different layers of security measures are implemented. And we also have a very well-managed access to information, which is on a strict need-to-know basis and by a very well-controlled group of people. So I think that the control over who is using and accessing and has different rights in relation to the information is very, very strict.
35. **F1: Okay.**
36. **F1: What sort of information do you have access to and with what technical resources?**

37. I: You know I normally have access to all the deals-related information so the information that is relevant to my scope of work. Everything related to project which is legally relevant and then the way to do it is that we follow processes and use systems for contract management purposes.

38. **F1: Do you use your computer or an iPad?**
39. I: Yeah, yeah, just like everyone else. Nothing special basically.
40. **F1: Alright.**

Strategic questions:

41. **F1: What policies does the company have towards information sharing?**
42. I: Very complex policies and you know information sharing, again depending purpose and the way of processing, it is well-managed. Because of course we always have to be compliant with the security measures related to the data packages we log as well and it's not just a matter of confidentiality, but of overall legal and contractual compliance.

43. **F1: Mm. Yeah.**
44. I: So a lot of relevant policies.
45. **F1: Okay that's good.**

46. **F1: Within confidential policies, are you aware of the current policies? What are you allowed to share with external parties?**
47. I: For our department it is different because we are actually more involved in these policies. But anyway, for all the employees I think the best part is that the company is actually following up the training program and ensuring employee's compliance. They frequently improve and renew the training and review the policies so that the knowledge is continuously maintained.

48. **F1: Yeah so they are constantly being updated and changed?**
49. I: Yeah exactly, and just making sure that everybody understands them and has proper training and this is a mandatory type of certification.
50. **F1: Okay that's good. We're going to go onto the second component which is integrity of information.**

Integrity

Technical questions:

51. **F1: How would you work with information backup?**
52. I: I think that normally when we are for example making an agreement we have different editorial rights: there is an owner of the drafts and then you always have to put the proper disclaimers and mark it as a draft and then also mark it as confidential and include it only to the people that actually need to be involved in that discussion. So it's a very controlled process., depending on the actual role of the colleagues that are involved. Some of them can only view and cannot make changes, some others can also edit.

53. **F1: Okay. Does the company automatically backup all of your information?**

54. I: Actually I don't know. I guess so but I really don't know. I mean for sure there's an automatic backup that is limited in time should be but I don't know...

55. **F1: Alright**.
56. I: The technical…
57. **F1: No, no that's fine.**

Strategic questions:

58. **F1: To which degree can you alter information? If you can, how would you do it?**
59. I: The information that I am owning and drafting and processing, definitely I mean I can alter it when I'm writing the contracts. I can alter it based on the policies that we have in place but we have lots of guidelines and so on. But otherwise no. Only if I am directly involved in a certain project otherwise I don't have any kind of rights to change information without prior approvals. It's only the person that is owning the respective task or initiative.

60. **F1: Okay.**

61. **F1: How do you assure the accuracy of information if you yourself and possibly other colleagues can alter information?**
62. I: You know normally, because again most of my work is related to contracts I always save the contract drafts and mark them which one is final and which one is...yeah, the dates are right version, yeah. So that's pretty much it.

63. **F1: Okay that's good. We are going to go onto the last component which is availability.**

Availability

Technical questions:

64. **F1: Based on the technical systems you have access to, have you ever experienced that you cannot access information that you need?**
65. I: No. I think that the support is really good for our systems so no, it has not happened.

66. **F1: Okay, I think you are the first one.**
67. I: Haha yeah, I think that maybe because the systems that I'm using are not maybe so demanding when it comes to that as legal department doesn't work with big data for daily work tasks.
68. **F1: Yeah, no but that's true.**

69. **F1: What security programs do you use?**
70. I: I think the ones that are pre-installed. We have a set that is automatically installed on each computer once we start working here.

71. **F1: Mhm.**
72. I: But I don't know exactly their names. We have a lot security when it comes to accessing internet, I mean there are a lot of filters and everything is controlled via IT,

quite a lot I think when it comes to this internet access, in order to ensure the secure connection.

73. **F1: That's perfect.**

74. **F1: What is the company's view on security towards external parties? What we mean by this is more of the physical security.**
75. I: Physical yeah. I think all the regular measures I mean are official. We all have access cards and sometimes we have certain codes after certain times or in the morning and then we have a very strict visit policy that nobody can get inside the office. There are separated customer areas that are very well separated physically.

76. **F1: Okay, that's good.**
77. I: We are not...you have to lock your computer when you are not at your desk, you cannot leave your badge on your table so a lot of this common sense rules are eventually followed up.
78. **F1: Mhm. That's perfect. We are going to finish off with one more question.**

Strategic questions:

79. **F1: What policies does your department have when it comes to sending information to the right receiver?**
80. I: I think that...you mean externally or?

81. **F1: It could be a customer or you know just making sure that the information, like if you have to send information to yeah, specifically a customer, what are you allowed to include in the e-mails and make sure that it's the right person that gets them?**
82. I: I mean obviously we are always using disclaimers that are related to confidentiality for example and also when it comes to the actual receiver, everybody is responsible for understanding who they are sending e-mails to. We are immediately the counter party so yeah, normally we send e-mails to the person that is interested in that e-mail.

83. **F1: Okay. So you still have a check on who it is and everything?**
84. I: Yeah, yeah. And we have personal responsibility for understanding how to do that.

85. **F1: Yeah, that's perfect. We don't have anything more for the interview so we're wondering if you have something you want to add or do you have any further comments?**
86. I: Nope, I mean I hope I was useful in any way considering that I'm not very technical. I think it could have been better for you to talk to someone from IT as well but I hope you could get some ideas.

Appendix 5: Företag B, Individuell intervju, I4

F1 = Författare 1
F2 = Författare 2
I = Informant

*Informanten identifieras som **Kundansvarig, 58**.*

1. **F1: Beskriv din avdelnings uppgift inom företaget.**
2. I: Min avdelnings uppgift är att serva kunder med ekonomisk placering och ekonomisk rådgivning och redovisning.

3. **F1: Berätta om din arbetsroll (vad den omfattar, hur länge har du haft den).**
4. I: Den här rollen har jag nu sedan ett år tillbaka ungefär, och jag är kundansvarig.

5. **F1: Hur skulle du beskriva din titel?**
6. I: Jag är kundansvarig, skulle man kunna säga.

7. **F1: För att identifiera dig i uppsatsen sedan behöver vi också din ålder.**
8. I: Jag är 58 år.

9. **F1: Berätta hur företaget arbetar på säkerhetsnivå (går ni någon utbildning, policys).**
10. I: Vi har massor av policys för säkerhet, det första man gör när man börjar här - det är att skriva under ett sekretessavtal, och, hur kommer ni att referera? Kommer ni säga att det är en bank?
11. **F1: Ja, finansiell sektor och bank.**
12. I: Men då har vi ju banksekretess, och det innebär att vi inte får prata med någon om något egentligen och vi har, man skriver under ett sekretessavtal, och det gäller tills man dör egentligen. När jag har slutat har får jag inte heller säga vad vi hållit på med och vilka kunder vi har och hur det ser ut, och sen är det också så att det gäller internt mellan avdelningar, så man ska vara ganska försiktig med vad man säger till folk och sådär. Sen har vi förstås jättemånga säkerhetslagrer i våra inloggningssystem och sådär. Tidigare hade jag en sån där VPN-tunnel, det vet jag inte riktigt vad det står för, men det vet väl ni, och då kunde man komma åt allt i banken. Och det fick man inte ha längre om det inte var absolut nödvändigt, jag kan tänka mig att liksom på VD-nivå och sådär att dom har det. Men jag var inte heller så road över att mina medarbetare skulle ha den accessen därför att det är ju också en säkerhetsfråga för dom, tycker jag, om man kan sitta ute - då kan man ju få en pistol mot pannan och så kan man börja föra över pengar mellan konton och sådär.

13. **F1: Så det kan kanske vara bättre då att ingen kan och då vet alla det?**
14. I: Ja, exakt. Det var ju ingenting man pratade högt om över huvud taget att man hade den accessen.

15. **F1: Vad innebär informationssäkerhet för dig?**

16. I: Det innebär att ingen annan än dom som är behöriga ska komma åt informationen. Att inga obehöriga kommer åt uppgifter som dom inte ska ha. Och det ska inte bara vara för att någon har ont uppsåt heller - utan det ska inte bara drälla omkring uppgifter som någon råkar få tag i.

17. **F1: Har företaget utbildat dig inom IT-säkerhet?**
18. I: Ja, det har dom på något vis.

19. **F1: Hur ser ni på IT-avdelningen? Vad tycker du är IT-avdelningens roll?**
20. I: Det har inte så särskilt mycket med informationssäkerhet att göra, jag tycker att dom ska utveckla nya programvaror och se till att digitalisera och ligga i framkant när det gäller det - sedan är det såklart så att de har ju en säkerhetsuppgift också. Men jag ser på deras roll som att de - ja roll inom vilket sammanhang? Informationssäkerhet, såklart, eftersom att ni frågar om detta… Ja, men det är klart att de måste se till att de har schyssta brandväggar och att allting funkar, att våra inloggningar… När vi väl är behöriga så ska det verkligen fungera. Då ska det vara hyffsat enkelt att komma åt allt det som man behöver komma åt för att kunna sköta sitt arbete. Men att de också ser till att det finns avgränsade fack där ingen obehörig kommer in. Skulle jag säga.

21. **F1: Hur ser fördelningen av resurserna mellan strategisk och teknisk säkerhet ut?**
22. I: När ni säger, strategisk, menar ni då användarvänlighet, eller mer beteende?
23. **F1: Vi tänker nog mer på beteendet då.**
24. **F2: Om företaget använder utbildningar, hur ni ska tänka kring situationer och ni har policys som ni måste följa, det kan vara mänskliga faktorer som kan påverka.**
25. **F1: Användarvänlighet handlar lite mer om design och så…**
26. I: Jag tror man tänker mycket på både och, men jag tror man är väldigt tung på den tekniska sidan här, därför att det är livsviktigt för vår kärna. Funkar inte den tekniska säkerheten så kan vi ju lägga ner. Och sedan om vi får hacka oss fram, eller allt ska funka smidigt flödesmässigt - ja det tror jag att man tittar en del på för det vinner man ju mycket tid och arbetskraft på såklart. Men jag tror att tyngdpunkten ligger på den tekniska biten, men jag vet inte. Jag bara gissar!
27. **F1: Vi undrar vad du själv tror, så här finns inget rätt eller fel på den frågan…**
28. I: Ja, för när man sitter och hackar i systemen…
29. **F1: … Och med hackar menar du då att man försöker ta sig fram?**
30. I: Ja, man sitter här försöker göra saker och sköta sitt jobb. Jag menar inte hacka sig in!

Confidentiality

Tekniska frågor:

31. **F1: Vilken sorts information har du tillgång till och med vilket tekniskt redskap?**
32. I: Jag har tillgång till information som rör mina kunder, jag har tillgång till intranätet här hos oss, jag har tillgång till SecureMail - att vi kan skicka på särskilt sätt. Via dator och telefon.

33. **F1: Vad använder företaget för säkerhetsutrustning till information?**
34. I: Det kan jag inte svara på, det vet inte jag.

Strategiska frågor:

35. **F1: Vad har företaget för policys angående informationsdelning? Och då tänker vi, vad får du dela för information externt och internt?**
36. I: Det var lite det jag pratade om innan, vi har ju banksekretess, och får absolut inte prata om våra kunder med någon, så är det ju rågångar så. Sitter någon på en annan avdelning så ska jag inte prata om mina kunder med dom. Sen informationsdelning… jag får ju dela med mig till mina kunder, och det måste jag ju göra på ett säkert sätt. Det finns ju vissa saker, rent allmänna, vi håller ju utbildningar och seminarier för våra kunder och då kan vi ju dela med oss av information, men det kanske inte är den informationen ni tänker på.
37. **F1: Jo, men det kan vara sådan information…**
38. I: Ja, för frågar de vad de har på kontot så måste jag ju berätta det för dom.
39. **F1: Vi har en fråga sen som rör lite mer hur man säkert kommunicerar, så det kommer en fråga om det sedan.**
40. I: Okej!

41. **F1: Inom sekretesspolicys, vet du om vilka policys som finns? Vad får du dela med dig till utomstående och var går gränsen - det har vi pratat om lite innan…**
42. I: Jag får i princip inte dela med mig någonting med någon, utom den det rör. Sedan får jag prata med mina arbetskollegor om kunden - för vi samarbetar ju - och där måste man ju vara öppen för att kunna ge kunden bästa service. Vad var det mer?
43. **F1: Vet du vilka policys som finns?**
44. I: Ja det vet jag.
45. **F1: Och vad får du dela med dig och vart går gränsen?**
46. I: Allt som rör kunder.

Integrity

Tekniska frågor:

47. **F1: Hur arbetar ni med backup av information?**
48. I: Vi jobbar mot servrar och jag tror det tas backuper en gång i timmen. Det jag sparar, det sparas ju omedelbart och sedan finns det tekniska lösningar för att hämta upp det där.

Strategiska frågor:

49. **F1: I vilken grad får ni ändra information? Om ni får, hur gör ni det?**
50. I: Det beror ju alldeles på vad det handlar om, alltså de dokument som jag själv har skrivit och som jag själv har gjort - det kan jag ju ändra i. Men det syns, det loggas ju, det ses när det är sparat. Men jag kan ju inte ändra i avtal och sådant där i efterhand, de är ju undertecknade och inskannade och klara liksom. Det går ju inte att fippla med det. Och skulle vi ändra i någon information som vi lämnat till vår kund, då måste vi ju kontakta vår kund och berätta det. Det är rätt mycket dualitet, som det heter då, är det något man gör på kundens begäran, om det handlar om pengar som ska flyttas, då måste vi vara två som skriver på. En som utför och en som attesterar, alltså en som godkänner att det ska göras. Så man får aldrig sitta själva och hålla på med det.

51. **F1: Hur säkerställer ni riktigheten av information?**
52. I: Det beror alldeles på vilken information ni menar. Det finns ju intern information i banken, och allt sådant kommer ju från vår informationsavdelning, och det är inte något vi kommer åt och ändra i eller så. Och säkerställa att den är riktig… Jag har ju ett uppdrag med mina kunder att se till att det jag skriver till dem och det jag säger till dem, att det är rätt. Sen får jag ju korrigera det ibland - ibland blir det fel. Nej, jag kan inte riktigt svara mer än så. Integrity - integritet…

53. **F1: Ja, det handlar ju om att säkerställa att informationen man har är riktig…**
54. I: Men det ligger ju i vårt uppdrag, det bygger ju på förtroende vårt varumärke, så att säga. Om vi inte svarar rätt på frågor, då dör vi ju. Då är det ingen som vill vara kund här hos oss längre. Vi är noggranna i det vi gör, redan från början. Jo, får jag säga en sak till - om det går ut information internt i banken, då går det alltid ut via vårt intranät, vi godtar liksom inte information från vem som helst, utan vi måste ha det bekräftat via rätt kanaler. Ofta så silar det då ner mellan cheferna, och man får information på flera olika sätt. Ingen ska liksom kunna smitta ner vår information på något sätt.

55. **F1: Då kommer vi alltså till det sista benet i CIA-triaden, som vi har översatt till tillgänglighet.**

Availability

Tekniska frågor:

56. **F1: Utifrån de teknologiska systemen du har tillgång till, har du någonsin upplevt att du inte kommer åt information som du behöver?**
57. I: Ja, det har jag. Och det beror antagligen på att det finns någon kodning någonstans som gör så att jag inte har tillåtelse att titta på det. Men då får man lösa det genom att prata med en kollega som har behörighet att ta fram det. Det händer inte så ofta, men någon gång har det hänt.

58. **F1: Vad använder ni för säkerhetsprogram?**
59. Nej.

60. **F1: Hur ser företaget på säkerhet mot utomstående? Och då tänker vi mer fysisk säkerhet, passerkort, murar sådana saker.**
61. I: Ja, våra brandväggar är ju jättetuffa om man tänker på datateknologi.
62. **F1: Nu tänker vi mer på…**
63. I: … Det fysiska?
64. **F1: Ja, precis.**
65. I: Vi har ju passerkort, som loggar var man är. Man kommer inte in någon som helst stans utan att ha passerkort. Tidigare hade jag ett passerkort som gällde på annan ort också, men det har jag inte kvar eftersom jag inte reser till den där orten hela tiden som jag gjorde tidigare. Nu var jag där och hälsade på häromdagen, och då fick jag öppna upp mitt passerkort för en dag. Och det är jättenoga med att man inte kommer åt våningsplan som man inte har anledning att vara på.
66. **F2: Skulle det vara lätt för någon som tar sig in genom entrédörrarna att ta sig in?**

67. I: Nej, de kan inte ta sig in. Man kommer till banksalen, sedan kommer man inte vidare. Och vi får inte ta med oss utomstående in heller.

Strategiska frågor:

68. F1: Vad har er avdelning för policys när det gäller utskick av information till rätt mottagare? Om du ska till exempel skicka till en kund, hur vet du att det kommer rätt?

69. I: Posten måste man ju lita på. Vi skickar väldigt mycket via post fortfarande.

70. F1: Är det för att ni inte tror att det är säkert att skicka…

71. I: Vi vet att det inte är säker att skicka mail. Men vi har en service nu som heter SecureMail, där vi lägger det på en server utanför banken, och så får kunden gå och hämta det via en maillösning. Det vet jag inte hur den tekniska lösningen fungerar… Att skicka mail är som att skicka vykort, har vi blivit upplysta om. Så det får vi absolut inte göra. Och sedan skickar vi mycket på post, det känns ju 1800-tal, men de handlingar som jag hanterar mycket, det är undertecknade avtal, och det finns ingen bra teknisk lösning, utan det kräver en signatur. Och då måste man ha pappret i handen.

72. F1: Har du något som du vill tillägga, någon övrig kommentar eller så?

73. I: Nä, jag tror inte det. Svårigheten får vår bransch är att ha en säker hantering men att ändå vara digitala. Att inte någon hackar vidare.

Appendix 6: Företag B, Individuell intervju, I5

F1 = Författare 1
F2 = Författare 2
I = Informant

*Informanten identifieras som **Assistent, 60**.*

1. **F1: Beskriv din avdelnings uppgift inom företaget.**
2. I: Uppgiften är att ta hand om donatorns vilja, det vill säga den som testamenterat pengar till kunden, samt att följa de regler och önskemål som han skrivit i sitt testamente. Han har ju donerat pengar och de ska förvaltas och gärna förräntas, och ska sedan delas ut till exempel studerande, gamla och sjuka, som behöver lite bidrag.

3. **F1: Berätta om din arbetsroll (vad den omfattar, hur länge har du haft den).**
4. I: Jag har hand om ansökningsförfarandet, det vill säga alla ansökningar som kommer in. Och registrerar dem, och även gör utbetalningar när styrelsen har gått igenom ansökningarna och föreslagit vem som ska ha bidragen.
5. **F1: Hur länge har du haft din arbetsroll?**
6. I: I fem år.

7. **F1: Hur arbetar företaget på en säkerhetsnivå, det vill säga, har du gått någon utbildning, finns det några policys för säkerhet?**
8. I: Ja, när det gäller mailen så har vi SecureMail, till exempel. Sedan har vi vissa bestämmelse, till exempel när kunder skicka in fakturor så ska det attesteras. Vi får inte ta uppdrag på mail hursomhelst, utan då får vi kontakta uppdragsgivaren och fråga om han eller hon har skrivit det här mailet till oss och hon vill att vi ska göra detta för dem.

9. **F1: Vad innebär informationssäkerhet för dig, vad tänker du när vi säger informationssäkerhet?**
10. I: Jag tänker att det är en trygghet mellan uppdragsgivaren och de som ska utföra arbetet, det är det första som dyker upp i huvudet.

11. **F1: Har företaget utbildat dig inom IT-säkerhet?**
12. I: Nej, inte utbildat på det viset.

13. **F1: Hur ser ni på IT-avdelningen? Vad tycker du är IT-avdelningens roll?**
14. I: Det är väldigt viktigt att det finns en IT-avdelning, och att där sitter professionella människor som kan sortera informationen som kommer hit, vi har ju spam-filter och så, så att vi inte blir hackade till exempel. Det är viktiga saker, tycker jag.

15. **F1: Hur ser fördelningen av resurserna mellan strategisk och teknisk säkerhet ut? När vi säger strategisk säkerhet så menar vi hur man beter sig i system, och med teknisk mer saker som brandväggar och likande.**
16. I: Jag tror att man lägger nog mycket resurser på det tekniska, för att data ska vara så säker som möjligt.

Confidentiality

Tekniska frågor:

17. **F1: Vilken sorts information har du tillgång till och med vilket tekniskt redskap?**
18. I: Det är mail vi använder på jobbet. Och sedan har vi våra interna system som vi använder oss av. Det dator och telefon jag använder.

19. **F1: Vad använder företaget för säkerhetsutrustning till information?**
20. I: Nej.

Strategiska frågor:

21. **F1: Vad har företaget för policys angående informationsdelning? Vad får du skicka i mail, vad får du prata om, lite sådana saker.**
22. I: När det gäller mail ska man inte skicka personuppgifter och sådana saker, som eventuellt kan hamna i orätta händer. Det är viktigt.

23. **F1: Inom sekretesspolicys, vet du om vilka policys som finns? Vad får du dela med dig till utomstående om vad du arbetar med, och sådana saker?**
24. I: Man är väl överlag ganska restriktiv när man prata med personer, vad man gör exakt och så, Vi talar till exempel inte om vad vi har för kunder - det är tabu. Det är sekretess. Och där är vi väldigt stränga, att vi inte röjer vad vi har för kunder.

Integrity

Tekniska frågor:

25. **F1: Hur arbetar ni med backup av information?**
26. I: Ja, genom att motringa, om vi får uppdrag utifrån kunder så måste vi motringa och säkerställa att det verkligen är korrekt avsändare.

Strategiska frågor:

27. **F1: I vilken grad får ni ändra information? Om ni får, hur gör ni det?**
28. I: Jag passar på den frågan.

29. **F1: Hur säkerställer ni riktigheten av information?**
30. I: Ja, som jag sa innan, så mail från en kund så motringer vi. Och om det kommer information från arbetsgivaren så hoppas man att den är korrekt och att det skulle stannat om om det är något som kommer utifrån. Att IT-avdelningen har klarat av att stoppa det.

Availability

Tekniska frågor:

31. **F1: Utifrån de tekniska systemen du använder har du någonsin upplevt att du inte kommer åt information som du behöver i ditt arbete?**
32. I: Det kan hända, för vi måste ha behörighet för att kunna komma in i olika system. Sedan kan det vara beroende på vilken avdelning du jobbar, om du ska ha en behörighet till den informationen eller så. Det är väldigt strängt, om man säger så.

33. **F1: Vad använder ni för säkerhetsprogram?**
34. Nej.

35. **F1: Hur ser företaget på säkerhet mot utomstående? Och då tänker vi mer fysisk säkerhet, passerkort, murar sådana saker.**
36. I: Vi anställda har passerkort, och vi har inte access till att komma in överallt i huset, vilket man kunde göra förr, men det kan man inte längre utan då får man ansöka om behörighet att komma in på en speciell avdelning om man har där att göra. Så det är faktiskt rätt så strängt.

Strategiska frågor:

37. **F1: Vad har er avdelning för policys när det gäller utskick av information till rätt mottagare? Om du till exempel ska skicka något till en kund - hur vet du att det hamnar rätt?**
38. I: Det hoppas man ju, att man fått rätt email-adress. Det är det jag kan svara på den frågan.

39. **F1: Har du något som du vill tillägga, någon reflektion du har eller så?**
40. I: Nej.

Appendix 7: Företag B, Individuell intervju, I6

F1 = Författare 1
F2 = Författare 2
I = Informant

*Informanten identifieras som **Avdelningsansvarig, 62**.*

1. **F1: Vill du beskriva din avdelnings uppgift inom företaget?**
2. I: Vi förvaltar våra kunder. Dessa kunder ger bidrag till exempel forskning, eller behövande. Och då har vi destinatörer som ringer hit och vill ha hjälp med att söka dessa pengar från kunderna.

3. **F1: Berätta om din arbetsroll (vad den omfattar, hur länge har du haft den).**
4. I: Jag är avdelningsansvarig, och har den administrativa delen i det hela. Presenterar bokslut och liknande, och ser till att det administrativa för kunden fungerar. Bland annat att fakturor ska betalas, handlingar ska skickas till länsstyrelsen och skatteverket m.m.
5. **F1: Hur länge har du haft din arbetsroll?**
6. I: Sedan 2007.

7. **F1: Berätta hur företaget arbetar på en säkerhetsnivå, det vill säga, har du gått någon utbildning, finns det några policys för hur man arbetar?**
8. I: Vi har inte gått någon utbildning direkt kan man väl säga, men vi har blivit informerade hur vi ska bete oss. Och det är mycket med mail, till exempel. Ingenting får skickas utan SecureMail. Så det är den biten.

9. **F1: Vad innebär informationssäkerhet för dig?**
10. I: Att inte information läcker ut från företaget eller från avdelningen utan att det hålls inom enheten. Utan att det hålls inom. Som bank har vi ju sekretess, så det får inte hända.

11. **F1: Har företaget utbildat dig inom IT-säkerhet?**
12. I: Ja, vi har fått lite information där också. Det är information om vad som kan hända och ske ute.

13. **F1: Hur ser ni på IT-avdelningen? Vad tycker du är IT-avdelningens roll?**
14. I: Ur en säkerhetssynvinkel?
15. **F1: Ja, till exempel.**
16. I: Som säkerhet så bör det vara program som säkrar att det inte läcker ut information. Detta måste ju vara helt säkert.

17. **F1: Hur ser fördelningen av resurserna mellan strategisk och teknisk säkerhet ut? När vi säger strategisk säkerhet så menar vi hur man beter sig i system, och med teknisk mer saker som brandväggar och fysiska apparater. Har du någon uppfattning om hur företaget fokuserar på de här två delarna?**
18. I: Som jag känner det så detta med brandväggar och säkerhetsgrejs, och säkerhet på den nivån, det är ju IT-avdelningen som sköter det. Där ser vi ju ingenting eller hör

någonting om hur det ligger. Sen är det ju hur vi beter oss, för vår säkerhet. Med SecureMail och likadant med våra telefoner som är avlyssnade för att säkerställa den biten. Men just den biten vad gäller brandväggar, det känner inte jag att vi har någon kunskap om.

Confidentiality

Tekniska frågor:

19. **F1: Vilken sorts information har du tillgång till och med vilket tekniskt redskap? Och med tekniskt redskap menar vi till exempel dator, eller telefon och sådana saker.**
20. I: Ja, min information kommer ifrån datorn och de program som vi har. Sen kan jag få information från kollegor, och det är per telefon. Men det jag kan läsa in, det är i datorn som vi har de programmen. Det är mail eller intranätet. Intranätet ger min jättemycket information av säkerhet så har vi bara tillgång till de program som vi behöver för vårt arbete.

21. **F2: Det du jobbar med, får du den mesta informationen ifrån kunderna?**
22. I: Ja, det kan man väl säga. Information om hur kunden vill ha det, det får jag av kunderna. Sedan har vi mycket information som ligger i våra system om kunderna, vilket är vårt arbetsredskap i de fallen.

23. **F1: Vad använder företaget för säkerhetsutrustning till information?**
24. I: Nej.

Strategiska frågor:

25. **F1: Vad har företaget för policys angående informationsdelning? Vad får du skicka i mail, till dina kunder vad får du inte skicka i mail och sådana saker.**
26. I: Allt som har med kund att göra måste vi skicka med SecureMail. Så skickar vi en årsredovisning eller portföljsammanställning så får det skickas med SecureMail.

27. **F1: Och internt - finns det några restriktioner där?**
28. I: Information om kunder. Inte generellt, men specifikt om en kund som kan komma i orätta händer och läcka ut.

29. **F1: Vet du vilka sekretesspolicys som finns? Vad får du dela med dig till utomstående kanske som inte arbetar med just det du arbetar med?**
30. I: Vi har sekretess, total sekretess kan man säga. Jag kan inte dela med mig till utomstående vilka kunder vi har. Jag kan inte diskutera detta med andra avdelningar i banken som inte har med kunden att göra. Utan inom avdelningen skall det vara stopp. Så att vi har totalt sekretess.

31. **F1: Vi går vidare med integrity, som vi översätter till integritet, som då handlar om att säkerställa att information man har är korrekt.**

Integrity

Tekniska frågor:

32. **F1: Hur arbetar ni med backup av information?**

33. I: Det görs backup på våra maskiner varje natt, så det skall väl göras. Så är det sagt.

Strategiska frågor:

34. **F1: I vilken grad får ni ändra information? Om ni får, hur gör ni det?**
35. I: Vad för information?

36. **F2: Information som du behöver för att utföra ditt arbete.**
37. **F1: Till exempel om någon kund, eller sådär.**
38. I: Mm. Visst kan jag ändra på någon information, inom vissa ramar, om jag säger så. Men däremot kan jag aldrig ändra på stadgar vad gäller en kund, om du tänker så, där kan man ju aldrig göra någonting.

39. **F1: Har du något sätt att säkerställa att den informationen du har om någonting är riktig?**
40. I: Jag har experter till hjälp. Om jag har en fråga som man tror man vet svaret på så kan detta ha ändrats under tiden och då är det bra att ha experterna att rådfråga innan man går ut med ett svar.

41. **F1: Vi tänker lite, till exempel, om du får ett mail eller något sådant, eller intranätet, hur vet du att det är rätt - att det kommer från rätt mottagare och sådana saker?**
42. I: Det vet man inte, nej. I det fallen får man ju titta på det och se hur det se ut och ibland känner man ju igen namn och dylikt. Men visst, det finns ju mail som man inte öppnar utan kastar direkt, för man vet att det här är inte rätt.

Availability

Tekniska frågor:

43. **F1: Utifrån de tekniska system du använder har du någonsin upplevt att du inte kommer åt information som du behöver?**
44. I: Av behörighetsskäl? Ja, visst har det hänt.

45. **F1: Vad använder ni för säkerhetsprogram?**
46. Nej.

47. **F1: Hur ser företaget på säkerhet mot utomstående? Passerkort och sådana saker.**
48. I: Vi har passerkort och under vissa tider har vi vissa koder som man ska slå. Det är individuellt vad man kommer åt med sina kort. Vi kommer bara in i de utrymme som vi behöver för vårt arbete och gemensamma utrymme.

Strategiska frågor:

49. **F1: När det gäller utskick av information, till exempel om du ska kontakta en kund via mail, har du några policys för vad du får skicka i mail och sådana saker?**
50. I: Ja, det finns det. Men det är som jag sa innan, det är SecureMail som gäller för det som är känsligt.

51. **F1: Det var alla frågor. Har du något som du någon reflektion eller kommentar som du vill tillägga?**
52. I: Nej.

Appendix 8: Företag C, Individuell intervju, I7

F1 = Författare 1
F2 = Författare 2
I = Informant

*Informanten identifieras som **Konsultchef/Projektledare/Systemutvecklare, 46**.*

1. **F1: Vi börjar med att fråga hur gammal du är?**
2. I: 46 år.

3. **F1: Vilket språk använder ni inom er organisation när ni arbetar?**
4. I: Svenska.

5. **F1: Kan du berätta om din avdelnings uppgift inom företaget.**
6. I: Vi är konsulter så att vi, vi är inget produktbolag även om en del tror det kanske. Men vi samverkar med kunder så vi ska producera någon form av applikationer. I vårt fall är det kanske 90-99% självapplikationer nu mera. Sen har vi en inriktning mot e-handel egentligen, eller jag har det. Avdelningen i sig gör nog egentligen allt som kunden vill om vi känner att vi har kompetensen. Vi får ju oftast någon form av förfrågan när det finns en väldigt svag kravbild på vad applikationen ska göra eller vad syftet är, och då brukar vi göra estimat eller skriva någon tydlig ’kravspec’ och sen så bygger någonting utifrån det. Det är nog så det funkar.

7. **F1: Skulle du kunna beskriva din arbetsroll.**
8. I: Den är kanske lite svårdefinierad. Jag är konsultchef, systemutvecklare, programmerare och systemarkitekt. Konsultchefsrollen har jag egentligen haft det sista 1,5-2 åren och där innefattar det löneförhandlingar och utvecklingssamtal och ganska mycket åt HR-hållet för den konsultgruppen jag är ansvarig för. Och det är viktigt för att, ja, det var lite roligare när man blev lite äldre. Det var lite tyngre att hänga med allt nytt som kommer när man blir äldre tror jag. Och så finns det så många unga hungriga som behöver liksom lite guidning och vägledning och så, så jag kände att jag kunde bidra lite där eftersom jag har programmerat sedan -82. Så jag skulle nog säga att kanske 20% konsultchef, 20% projektledare och 60% systemutvecklare, kanske något sådant.

10. **F1: Hur länge har du arbetat med konsult, programmering…**

10. I: Det har jag egentligen gjort sedan -89, -90.

11. **F1: Så du har ganska många års erfarenhet…**

12. I: Ja ganska många år. Jag jobbade lite som snickare innan jag började på elektroteknik i Lund och då hade jag en egen firma så det gjorde mig mer erfaren då. Och sen körde vi vidare på den firman som jag hade ihop med min bror under ganska många år. Snickare och sådant känns lite mer konstruktivt. Och sen har jag varit här sedan 2007 på Företag C.

13. **F1: Hur skulle du beskriva företagets arbete på en säkerhetsnivå? Går ni någon utbildning eller har ni säkerhetspolicys?**
14. I: Vi borde ju såklart ha det. Nu är det mest i Stockholm men där har dem ju ganska framskjuten ställning när det gäller just säkerhet och har väldigt hög kunskapsnivå när det gäller IT-säkerhet. Företag C är till exempel med och utvecklar Applikation 1. Jag har skrivit en hel del banker, och vi är med och skriver Kund 1s nya sajt här nere. Jag har aldrig blivit 'preppad' med någon sorts säkerhetstänk. Det är nog mer att man lutar sig mot sunt förnuft. Vi har ju, Företag C, utbildar ju andra programmerare i säker programmering. Men vi har inte det som någon obligatorisk guide internt, vi kanske borde ha haft det men vi har inte det.

15. **F1: Känner ni att det skulle behövas?**

16. I: Nej det kan jag inte påstå. Vi har inte så mycket säkerhetsfolk här nere så att vi lutar oss nog mot att när vi känner att "Ja men här vill vi nog vara väldigt säkra på att det här blir bra och korrekt och rätta krypteringsmetoder" då ringer vi till någon i Stockholm som tar ner någon från Stockholm. Men det är någon sorts fingertoppskänsla när det behövs. Det beror ganska mycket på vad det är för sajter. Tyvärr är det fortfarande så att företagen inte gärna vill lägga ner någon extra peng för att få det väldigt säkert.

17. **F: Om man kollar på strategisk säkerhet och hur anställda ska bete sig, att dem inte lägger ner mer pengar på det i jämförelse med teknisk säkerhet…**

18. I: Nej, vi har ju metoder för alla nyanställda och det finns riktlinjer för vad vi skickar i mejl och inte skickar i mejl till exempel. Det som det skulle kunna vara tjafs och de det pratar om i Stockholm, det är om vem du skickar känslig information till i mejl när det ligger någonstans i molnet. Men annars har vi nog inget utöver det.

19. **F1: Vi definierar informationssäkerhet som: skyddandet av information från att stjälas, eller användas felaktigt eller olagligt. Vad innebär informationssäkerhet för dig?**
20. I: Jag skulle nog säga samma. Det var en ganska bra och precis definition. Jag har inget att tillägga.

21. **F1: Har företaget utbildat dig inom IT-säkerhet?**
22. I: Nej företaget har inte utbildat mig inom IT-säkerhet.

23. **F1: Har du haft någon utbildning inom säkerhet om du bortser från företaget?**

24. I: Nej, ingen formell utbildning. Vi, Företag C, har interna grupper och interna mejlgrupper samt många kanaler internt där man förmedlar nyheter inom säkerhet så det är något vi blir matade med ganska kontinuerligt utan att vi ser det som en formell utbildning, fast vi får information om det.

25. **F1: Hur ser ni på IT-avdelningen? Vad tycker du är IT-avdelningens roll?**
26. I: Generellt ser vi nog på IT-avdelningen som någon som ska se till att vi har licenser, mejlen funkar. Om dem gör ett bra jobb så märks dem inte. Men det kanske skulle

ligga på IT-avdelningen egentligen om vi skulle bli ålagda att kryptera del av den informationen. Här nere sitter vi inte på så mycket hemlig information. Om man tar koden för en e-handel så finns det inte så mycket hemligt där egentligen. Så vi sitter inte på den mängden hemlig information som dem gör i Stockholm.

27. **F1: Hur ser fördelningen av resurserna mellan strategisk och teknisk säkerhet ut?**
28. I: Nej jag tror att det är väldigt få som har den uppfattningen på hela Företag C hur fördelningen är. Jag har ingen aning.

Confidentiality

Tekniska frågor:

29. **F1: Vad använder företaget för säkerhetsutrustning till information?**
30. I: Ingen. Jag tror inte att vi krypterar särskilt mycket alls. Brandväggar har vi självklart. Det låter ganska dåligt att vi har en brandvägg, det har jag hemma också. En del har förkrypterat sina diskar i och med att vi har laptops till exempel. När jag hade en laptop krypterade jag disken. Nu har jag en stationär så då låser jag in mina diskar innan jag går hem på kvällen. Det är upp till var och en egentligen, vi kräver inte att någon ska göra det. Så ja, en brandvägg.

31. **F1: Vilken sorts information har du tillgång till och med vilket tekniskt redskap?**
32. I: Vilken information skulle det kunna vara? Jag kan nog nå all information i och för sig. Jag vet inte riktigt vad det syftar till.

33. **F1: Det du arbetar med, finns det någon specifik information du måste få tillgång till för att kunna utföra ditt jobb?**
34. I: Nej det är ju liksom koden. Det är jag som administrerar rättigheterna till kodbanken om man får säga det så. Vi hostar all vår kod själva så den ligger på en server någonstans. Jag kan nå all information jag behöver. Jag kan använda och administrera så att andra når den koden de ska nå. Jag använder en stationär här men har även en laptop som jag kan nå allt på.

Strategiska frågor:

35. **F1: Vad har företaget för policys angående informationsdelning?**
36. I: Jag känner inte till några, det kanske finns men jag vet inte. Man skulle kunna säga att policyn, vi har en policy för att vi hade en debatt om det när vi flyttade upp all mejl i molnet. Då är policyn sunt förnuft och känner du dig tveksam så skicka inte mejl om det. Då blir det lite helgarderat. Vi skickar inte gärna lösenord. Ja, visst har vi någon policy. Alltså, lösenord och annat som man känner krävs för att logga in någonstans, det skickar vi inte i mejl. Men det måste nog vara så. Ja, det kan jag tänka mig göra personligen fast om Företag C står för säkerhet känns det ganska dumt att gå emot det. Det ser dumt ut om vi hjälper banker men så skickar vi runt massa skräp själva.

37. **F1: Inom sekretesspolicys, vet du om vilka policys som finns? Vad får du dela med dig till utomstående och var går gränsen?**

38. I: Det är nog olika från kund till kund. Vi har många kunder som vi får fylla in en ‘form’ angående fullständig tystnadsplikt och då får jag egentligen inte prata med någon. Jag får inte prata med någon om det på kontoret. Om jag sitter i ett projekt där dem har dem kraven, vi har några kunder här nere som har dem kraven, då får jag inte ventilera det till någon mer än dem som är med i projektet. Det är praktiskt ganska svårt eftersom vi har ett öppet landskap men vi har en tystnadsplikt på företaget som alla accepterar när de styr upp varsina anställningsavtal. Så det är nog mycket från kund till kund.

Integrity

Tekniska frågor:

39. **F1: Hur arbetar ni med backup av information?**
40. I: Det som vi har markerat som väsentlig information för oss själva backas varje dygn och åker upp i molnet. Krypterat eller inte vet jag faktiskt inte eftersom det inte är jag som har lagt upp rutinerna men jag skulle gissa på att det är krypterat. Det backas upp automatiskt.

Strategiska frågor:

41. **F1: I vilken grad får ni ändra information? Om ni får, hur gör ni det?**
42. I: Jag får tänka praktiskt vad det skulle vara för information jag skulle kunna tänkas ändra. All information som jag når får jag ändra antar jag. Men jag vet inte riktigt vad det skulle vara för information faktiskt.

43. **F1: Hur säkerställer ni riktigheten av information?**
44. I: Jag har svårt att se vad det skulle kunna vara praktiskt. Jag kan tänka mig att det finns en hel del dokument som ligger på en delad filyta som en begränsad mängd människor här kommer åt. Den är versionshanterad och kanske om jag skulle vara jätteintresserad skulle jag kunna hacka den versionshanteringen, fast det vet jag inte hur man gör. Då skulle man kunna titta i versionen och man kan alltid se vem som har ändrat senast och så vidare. Då är det versionshanterat så det går nog att se.

45. **F1: Så ni har filrättigheter då?**

46. I: Ja.

47. **F1: Okej.**

48. **F1: Vi går vidare till den sista komponenten, vilket är tillgänglighet.**

Availability

Tekniska frågor:

49. **F1: Utifrån de teknologiska systemen du har tillgång till, har du någonsin upplevt att du inte kommer åt information som du måste få tillgång till? Det kan vara filrättigheter, eller att något inte stämmer.**

50. **F2: Nu är ju du administratör…**

51. I: Inte så mycket nu längre utan det var mer förr. Vi satt ihop, förr satt Stockholm, Malmö och Göteborg ihop mätmässigt och då skulle det administreras som simultant med Göteborg så då var det ganska ofta man upplevde att man inte kom åt vissa servrar eller någonting.
52. **F1: Mm.**
53. I: Men det var nog inte för att det var hemliga saker på den, det var nog för att någon inte visste hur man gjorde.

54. **F2: Mm, okej. Det kan hända!**

55. **F1: Ni jobbar med applikationssäkerhet, så vi undrar lite vad ni använder för säkerhetsprogram internt, om du skulle känna till något?**
56. I: Nej, jag kan inte säga på rak arm. Vi har mjukvara där vi har olika projekts IP adresser, lösenord och så vidare som ligger krypterat på en delad filyta men jag kommer inte ihåg vad den heter. Men det är något vi använder i alla fall. Eller, ibland. Det är också mycket beroende på kund liksom. Japp.

57. **F1: Hur ser företaget på säkerhet mot utomstående? Det kan vara tillgångskort till byggnader, det kan vara fysisk säkerhet - murar grindar…**
58. I: Nu har vi precis flyttat hit så här är vi inte så nöjda. Det kommer att komma upp nya lås, ellås, och vi har själva brickor för att komma in, larmkoder och så vidare. Just nu är det fritt blås så det är ganska många som bara kan gå rakt in.

59. **F1: Hur känns det?**

60. I: Nej det går inte.

61. **F1: Nej.**

62. I: Det känns inte bra alls. Det är ganska mycket spring här för det har legat ett annat företag här innan så, och sen så det är vissa som tar chansen. Det var några förra veckan som sa att dom skulle till andra sidan av huset så de gick in här och undrade om de fick gå igenom och ‘Nej det får ni inte’. Så det kommer upp faktiskt mer lås, så [den] dörren kommer vara låst sen. På det gamla stället var det ganska lugnt för då var det dels en ytterdörr där nere och sen så skulle man upp på 7:e våningen och sen skulle man in igenom larmet och sen skulle man ha sin kodbricka. Det blir något liknande här sen.

Strategiska frågor:

63. **F1: Japp, avslutningsvis så undrar vi då när det gäller utskick av information till rätt mottagare, det vill säga till era kunder, har ni några policys för det? Det kan vara att se till att rätt information kommer till rätt kund…**
64. I: Nej det finns nog ingen uttalad policy för det. Vi faller nog tillbaka på använd ditt sunda förnuft liksom och om du tänker dra iväg en massa känslig information så är kanske inte just ett helt vanligt mejl är det rätta sättet att göra det på. Så utöver sunt förnuft så nej - inget uttalat. Är du tveksam så gör inte det.

65. **F1: Har du några övriga kommentarer eller något du vill tillägga?**

66. **F2: Är det något du känner att du vill förmedla, men inte riktigt fick fram?**
67. I: Nej jag tror i så fall bara att det skulle vara, jag kan kanske känna själv att jag kan svara ganska dåligt på flera frågor men det beror nog på att den största säkerheten sitter i Stockholm och att det är som små öar där vi egentligen har olika inriktningar på Företag C. Vi löser våra liksom grejer och det låter som vi har ganska dålig säkerhet men det kan ju bero till en stor del på att det vi har som går att komma åt är inte särskilt stöldbegärligt. Bara en parentes.

Appendix 9: Företag C, Individuell intervju, I8

F1 = Författare 1
F2 = Författare 2
I = Informant

*Informanten identifieras som **Projektledare/Lösningsarkitekt, 28.***

12. **F1: Vilket språk använder ni inom er organisation?**
13. I: Svenska.

14. **F1: Beskriv din avdelnings uppgift inom företaget.**
15. I: Jag skulle inte säga att vi har någon specifik avdelning utan vi jobbar ju i projekt så allting är uppdelat i projekt. Alla är samma och man har ju en viss roll i ett projekt men ingen avdelning som sådan. Så det är mer vilken roll jag har inom ett projekt.

16. **F1: Kan du berätta om din arbetsroll.**
17. I: Jag är en projektledare och lösningsarkitekt.

18. **F1: Hur länge har du arbetet med det?**
19. I: Jag har väl haft den positionen jag har nu i ett halvår kanske.

20. **F1: Vill du beskriva lite om vad du arbetar med inom dem rollerna och givna uppgifter?**
21. I: Jag har den generella kundkontakten och jag tar fram det som ska göras i projektet tillsammans med kunder och fördelar det arbetet med dem andra som jobbar med projektet. Och sen utvecklar jag också.

22. **F1: Hur skulle du beskriva företagets arbete på en säkerhetsnivå? Går ni någon utbildning eller har ni säkerhetspolicys?**
23. I: Nej, här finns det ingen utbildning eller policys. I Stockholm finns det nog lite mer. Vi har ju knappt någon intern IT så det är inte så att vi har kunders grejer här utan dem lägger vi ut till andra. Och sen är det den generella utbildningen i projekten när man gör någonting så då får man läsa på och lära sig. Sen har vi våra kompetensutbildningar på företaget två gånger om året och det är ganska mycket IT-säkerhet men speciella saker så som man går någon certifiering när man börjar finns inte.

24. **F1: Vi definierar informationssäkerhet som: skyddandet av information från att stjälas, eller användas felaktigt eller olagligt. Vad innebär informationssäkerhet för dig?**
25. I: Ja jag tror er definition var ganska bra. Informationssäkerhet är väldigt mycket som ni sa, och som ordet själv säger skyddandet av information så det finns inte mycket att tillägga.

26. **F1: Har företaget utbildat dig inom IT-säkerhet?**
27. I: Nej.

28. **F1: Har du haft någon tidigare utbildning inom IT-säkerhet?**

29. I: Nej inget annat än det man har haft på universitetet.

30. **F1: Hur ser ni på IT-avdelningen? Vad tycker du är IT-avdelningens roll?**
31. I: Vi har ingen IT-avdelning som sådan. Vi har någon en infrastrukturgubbe som har hand om den interna IT vi har. I och med att vi inte driver någon produkt som sådan utan vi har ju kundernas projekt så är det oftast deras IT-avdelning som sköter dem bitarna och infrasturkturbitarna och säkerheten kring det. Vi kanske kommer in och konsultar det men då är det kundernas avdelning. Du ser ju där inne, där finns det ingenting. I Stockholm är det exakt det dem jobbar med: konsulta kundernas IT-säkerhet hos kunden. Där har vi inte heller alltså någon generell IT-säkerhet inhouseat därför vi har inget inhouse. Kunderna kommer till oss och säger att vi behöver hjälp med vår IT-säkerhet och så kommer vi och hjälper dem i deras IT-avdelning och med deras anställda. Det blir lite omvänt. Vi jobbar mycket med IT-säkerhet men inte hos oss själva i och med att vi egentligen inte riktigt har något att skydda och allting är outsourcat. Mejlen har vi inte hand om heller själv till exempel. Vi har lagt ut allting för att ha så lite som möjligt för det tar så mycket tid och resurser.

32. **F1: Hur ser fördelningen av resurserna mellan strategisk och teknisk säkerhet ut?**
33. I: Det blir lite samma sak där i och med att vi inte riktigt har så mycket IT-säkerhet inom företaget. Det blir kanske mer strategiska frågor eftersom vi är ute hos kunder och pratar men där är det också mycket tekniska grejer. Det kan vara allt från att analysera folks brandväggar till att kolla social engineering eller vad som helst. Fördelningen är väl ganska jämn skulle jag säga. Kostnadsvis kan jag inte svara på.

Confidentiality

Tekniska frågor:

34. **F1: Vad använder företaget för säkerhetsutrustning till information?**
35. I: Den lilla informationen som vi har, den ligger bakom brandväggar och skyddat på dem diskarna dem ligger på. Data backas upp. På en teknisk nivå är det väl så. Men sen ligger det mycket i molnet och det kan vi inte själva råda över. Det är nackdelen med att outsourcea olika saker och ting i molnet. Du förlorar lite av kontakten i kedjan i och med att du skriver och kommunicerar härifrån och dit så kan det hända mycket på vägen som du inte kan råda över om det nu är så säker information som du vill skicka.

36. **F1: Ni säger att ni lägger upp information i molnet, innebär det då att alla på kontoret här har tillgång till all information?**
37. I: Vi använder oss av Office 365 för molnet. Nej, bara det man delar ut. Det fungerar precis som Google Drive.

38. **F1: Vilken sorts information har du tillgång till och med vilket tekniskt redskap?**
39. I: Det är det som kunden tillåter mig att se. Jag behöver inte ha tillgång till någonting här. Det blir en svår fråga när du frågar ett konsultföretag därför vi inte har någonting själv. Om vi hade haft en egen produkt till exempel hade vi kunnat säga att Om du jobbar med den här komponenten så får du inte se mer än så. Så har vi det inte. Nu jobbar vi mot kunder och där kan man få tillgång till mycket roliga saker och ting för

att saker oftast ska gå snabbt. Det säger dem nog inte själva. Konsulter är nog ofta den svaga länken när det delas ut behörigheter. Du får nycklarna till slottet. Jag vet inte hur mycket ni har läst om sådana här grejer men det är oftast den bristande källan till informationssäkerhetsförluster. Det är konsulter och annat eftersom de får behörighet och tillgång till en databas och kan se allt. Så är det jätteofta.

40. **F1: Då får de helt enkelt lita på den personen?**

41. I: Ja, men för att någon IT-avdelningsguide är enkelt att… sen är det vissa som har jättebra koll. Men här har vi ingenting själva så vi har ingenting att skydda. Någon kan komma åt anställningskontraktsmallar, här finns ingenting att ta. Om någon skulle hacka oss, så liksom, ja vi har testmiljöer.

42. **F1: Om någon skulle få tag på information som ni har fått från era kunder, då hade det varit problem för era kunder och er att tappa tilliten.**

43. I: Absolut, då hade det varit ett problem. Självklart är det så. Och då får man skydda den informationen bra.

Strategiska frågor:

44. **F1: Vad har företaget för policys angående informationsdelning?**
45. I: Nej, det är lite kundspecifikt. När du blir anställd av kunder, inhyrd, får du skriva på non-disclosure agreement som säger att du får inte ens prata om det här med någon på kontoret. Det är jättevanligt. Alla kunder är inte så men generellt är det så när vi börja jobba. Jag vet inte om ni var tvungna att skriva på ett NDA när ni började här därför en informant pratade om kunder och det är visst känslig information såklart. Det skriver vi på vid anställningsavtalet att det vi pratar om här, det pratar du inte någon annanstans. Sen är det liksom common sense att man pratar om vad man gör på jobbet men man kanske inte ska prata om nu ska den här nya kunden som ingen vill ha, lansera sin nya produkt. Det kanske inte är något man går runt och säger till alla. Det är det du skriver på vid anställningsavtalet att det säger du inte. Jo, det finns en generell NDA för säkerhet.

46. **F1: Inom sekretesspolicys, vet du om vilka policys som finns? Vad får du dela med dig till utomstående och var går gränsen?**
47. I: Det är vissa saker som när man jobbar med offentliga kunder, alltså kunder som har sin produkt på marknaden, så är det oftast det man snackar om. Det finns redan ute så det är inga större problem. Man får tänka lite grann om vad man pratar om men oftast är det inga problem att snacka om vad man gör. Man får vara försiktig för visst pratar man med sin sambo men där kan det också gå snett eller någon annan hör.

Integrity

Tekniska frågor:

48. **F1: Hur arbetar ni med backup av information?**
49. I: Det är i stort sett kod vi arbetar med och den är versionshanterad. Det är den backupen som finns och det är mer än tillräckligt för att allting som är versionshanterad på GitHub, det är backat och kan bara hämtas ner om datorn går sönder.

50. **F1: Hur ofta uppdaterar ni era backups?**

51. I: Vi har inte dem själva. Om jag jobbar med en kund och vi jobbar med GitHut till exempel så checkas koden in dit så det ligger i molnet. Den koden som vi har här, den backas väl upp kontinuerligt men jag vet inte när detta görs.

Strategiska frågor:

52. **F1: I vilken grad får ni ändra information? Om ni får, hur gör ni det?**
53. I: Vi har ingen databas som innehåller företagsinformation. Det enda vi har är vårt AD som ligger någonstans i Göteborg. Om det är någon som byter telefonnummer så ändras det av en databasadministratör. Hos kunder är det de som bestämmer men jag har ju tillgång till mina kunders databas. Om de vill att jag ska ändra någon data där så får jag göra det. Men igen, det är upp till projektet som sådan jobbar du med ett finansiellt system, som till exempel Kund 1, där har vi inte tillgång till dem databaserna överhuvudtaget. Där är det jättenedlåst, du får inte ens lov att se. Där är det så många lager emellan och det är också mycket på grund av massa revision och såna grejer. Du ska inte bara få lov att förvanska data, det är jätteviktigt. Det är ett generellt tänk, absolut. Jag skulle säga att det skulle bero på data:n i sig och kunden. Vi har ingen data här själva så vi har ingenting som skulle kunna förvanskas här. Jag skulle kunna ändra mallen för ett anställningskontrakt men det är allt vi har här.

54. **F1: Hur säkerställer ni riktigheten av information?**
55. I: Det vet man inte. Det mejlas information och du vet inte om någon har varit emellan men någonstans får man lita på att den kedjan är intakt men oftast skickas det inte viktig information på det sättet. Kontrakt och sånt postas ju ofta. Jag vet inte vad det skulle vara som jag skulle verifiera, oftast när man ska in i större kunders miljöer så är det oftast 3-stegs inloggning, sms och ‘hitan och ditan’ och krypterade anslutningar. Jag vet inte om det är så att vi ska skicka information mellan oss så som lösenord och annat, så försöker man oftast använda lösenordstjänster som LastPass för då har man någon koll på att det inte bara händer grejer i mellan. Jag kan inte på rak arm komma på vad det skulle vara men i överlag så skickar man inte grejer av dem karaktären i mejl. Jag gör inte det i alla fall.

Availability

Tekniska frågor:

56. **F1: Utifrån de teknologiska systemen du har tillgång till, har du någonsin upplevt att du inte kommer åt information som du behöver?**
57. I: Absolut. Jag har kunder där jag inte har tillräckliga behörigheter för att göra det jag behöver göra då blir det jättesvårt. Då ska man gå igenom 5 led för att öppna upp eller någon ska sätta igen en checkbox eller såna här grejer. Vi har inga problem här i och med att vi har inte dem grejerna liggandes här men hos kunder är det absolut så. Den ena kunden vi har är det jättenedlåst. ‘Du får tillgång till den här databasen med den här användaren’ men om jag vill göra någonting utöver den behörigheten så går det inte. Med det är jättevanligt.

58. **F1: Vad använder ni för säkerhetsprogram?**

59. I: Vi har inga generella säkerhetsprogram. Folk använder sig väl generellt av LastPass som börjar bli mer vanligt men det är vanligare att vi använder oss av kunders säkerhetsprogram för att komma åt deras system härifrån för att vi inte ska sitta på deras nätverk. Annars är det saker som VPN in hit så man ska kunna jobba hemifrån för att vi inte exponerar databaser utifrån. Så man kan sitta hemma och VPN:a in hit. Det är väl det enda säkerhetsprogram vi har som man skulle kunna komma in utifrån på.

60. **F1: Hur ser företaget på säkerhet mot utomstående?**
61. I: Det är jätteviktigt. Vi har inte haft det här i och med att vi har precis flyttat hit men kommer få sådana här taggar så folk inte bara ska kunna vandra in hit på dagen eftersom man inte ser dörren från där man sitter. På det gamla kontoret var allting inlåst, dörrarna var låsta utifrån och så kommer det att bli här också.

62. **F1: Hur känns det att det inte är så säkert just nu?**

63. I: Jag tänker inte på det men det är inte så att man sitter i en bank där folk ska kunna komma in och råna en. Men det är absolut trevligt att folk inte bara kan öppna dörren och komma in. Det ska bli bra med lås på dörren.

64. **F1: Vet ni när det kommer att fixas?**

65. I: Det kommer väl om några veckor tror jag.

Strategiska frågor:

66. **F1: Vad har er avdelning för policys när det gäller utskick av information till rätt mottagare?**
67. I: Nej, vi har inga policys för det utan det är väldigt mycket att man får tänka själv vad det är man håller på med. Du får tänka lite grann på vad du håller på med. Du skickar inte lösenord eller känslig information bara så där i ett mejl till 10 cc:ade människor. Det är så i överlag att folk har kritiskt tänk. Man får tänka lite grann på vad man håller på med och jag tycker att det fungerar bra. Jag tycker inte att om jag skulle öppna min mejlbox och titta igenom den så ligger det inte någon känslig information.

68. **F1: Känner du att innehållet av information påverkar hur man ska tänka till vem man skickar till?**
69. I: Ja absolut. Det är så sällan… delar vi ingen känslig information… jag kan inte komma på när jag skulle göra det. Om vi skickar lösenord, om det ska göras, delas det upp det på olika källor därför det ingen bra idé att skicka ett lösenord och användarnamn i samma mejl. Man får tänka lite grann med vad man håller på med och det brukar fungera bra. Nu ligger mejlen i Office 365, innan så hade vi det själv men nu ligger det på Office 365 och jag vet inte var dem servrarna står men de går väl igenom NSA på något sätt. Men igen, så känslig information skickar vi inte så det inte skulle kunna gå att skicka i mejl.

70. **F1: Har du några övriga kommentarer eller något du vill tillägga?**
71. I: Nej det tror jag inte.

Appendix 10: Företag C, Individuell intervju, I9

F1 = Författare 1
F2 = Författare 2
I = Informant

*Informanten identifieras som **Utvecklare, 27.***

1. **F1: Vi undrar först hur gammal är du?**
2. I: "Jag är 27 år."

3. **F1: "Jättebra."**

4. **F1: Vi börjar med den första frågan och då undrar vi om du kan beskriva din avdelnings uppgift inom företaget.**
5. I: Min avdelnings uppgift är att utveckla först och främst - ta fram det våra kunder vill ha.

6. **F1: Om du vill utveckla lite på vad du menar med utveckling?**

7. I: Vi skapar tjänster främst och applikationer. Det är väl vårt yttersta ansvar kanske.

8. **F1: Om du går in sen lite på din enskilda arbetsroll.**
9. I: Min egen arbetsroll… alltså jag sitter dagligen och utvecklar, fixar buggar och skapar nya saker - och emellan dessa så är det väl möten och liknanden och så också lite kundkontakt men det är absolut främst utveckling för mig. Sen har jag inte jobbat här så länge, inte ens ett halvår, utan jag är ganska fräsch från plugget själv.

10. **F1: Kan man fråga hur länge har du haft rollen som utvecklare?**

11. I: Utvecklat sen, på detta företag, rollen som utvecklare har jag haft sen jag började, sen har jag utvecklat i många år. Jag pluggade civilingenjörsprogrammet i datateknik på LTH, gjorde mitt ex-jobb och bara det hade ju med alltså utveckling och sen sökte jag hit.

12. **F1: Det låter jättebra.**

13. **F1: Skulle du kunna berätta lite om hur företaget arbetar på säkerhetsnivå. Det vill säga har ni utbildningar, säkerhetspolicys? Om du känner till det.**
14. I: Nej, jag känner inte till så mycket om just det faktiskt. Policys och säkerhetsutbildningar är ingenting som har nämnts för mig direkt. Sen har jag väl kanske känt lite att det är lite det företaget embracear på något sätt, så det kanske låter lite konstigt men man antar väl att folk...

15. **F1: Eftersom du är relativt ny, känner du att det är någonting du skulle vilja ha - någon form av utbildning om säkerhet?**
16. I: Ja, ifall det är relevant, absolut. Företaget ställer ju olika frågor så det är viktigt att alla är på samma nivå och vet vad som gäller såklart.

17. **F1: Mm…**

18. I: Och framför allt ha den kompetensen som behövs för att kunna hålla den nivån som man har satt.

19. **F1: Vi definierar informationssäkerhet som: skyddandet av information från att stjälas, eller användas felaktigt eller olagligt. Vad innebär informationssäkerhet för dig?**
20. I: Nej men det låter som en bra definition. Jag antar att det finns ganska många definitioner…

21. **F1: Mm…**

22. I: Men den lätt vettig.

23. **F1: Ja. Det finns inget du vill tillägga eller känner också är viktigt när det gäller just informationssäkerhet?**
24. I: Nej, att stjäla information var precis det du sa. Det är väl någonting om att säkerställa integriteten av information. Men det låter bra.

25. **F1: Ja, men det låter jättebra**.

26. **F1: Vi har gått igenom lite att du inte riktigt har fått någon utbildning, vi kommer ändå att fråga.**

27. **F2: ... i IT-säkerhet då…**

28. **F1: Ja, men vi kommer ändå att fråga: Har företaget utbildat dig inom IT-säkerhet?**
29. I: Företaget har inte utbildat mig inom säkerhet alls faktiskt. Sen så läste jag väl egentligen kommunikations-/säkerhetsinriktningen på LTH på dataprogrammet. Så jag har väl inte direkt frågat efter någonting heller utan man ju har stött på till exempel om man har utvecklat - hur saker görs och varför det ska vara säkert och så vidare. Så då har jag ju såklart frågat men man kan väl nästan se det som någon form av bieffekt till att sitta och utveckla - att man får lära sig hur det funkar i just det projektet men inte annars, nej.

32. **F1: Skulle du säga att din kunskap om IT-säkerhet är endast från skolan - skolutbildningen?**
33. I: Skola och fritid om man skulle slå ihop dem två.

34. **F1: Mm, ja**.

35. **F1: Hur ser du fördelningen av resurser mellan strategisk och teknisk säkerhet? Vet du skillnaden mellan strategisk och teknisk säkerhet först?**
36. I: Strategisk är väl hur man förebygger antar jag…

37. **F1: Mm, det kan vara liksom utbildning, det kan vara policys, det kan vara själva mänskliga beteende mot säkerhet och teknisk är då mjukvara, program, hårdvara…**

38. I: Ja. Vad var frågan?

39. **F1: Hur ser du fördelningen av resurser mellan strategisk och teknisk säkerhet? Det kan vara anställda, det kan vara kostnader. Om du har någon uppfattning om det. Du får säga att du inte vet om du inte vet.**

40. I: Eftersom jag precis suttit och sagt att jag inte är utbildad här inom säkerhet så kan jag väl säga då ligger resurserna för den tekniska delen. Vad jag vet eller är ganska överrepresenterat. Samtidigt så vet jag inte exakt allting om de tekniska förutsättningarna här heller. Men jag skulle säga att det är där resurserna ligger, majoriteten av dem i alla fall.

41. **F1: Mm, det blir jättebra. Vi kommer att gå vidare till dem tre komponenterna i CIA-triaden. Dem heter Confidentiality, Integrity och Availability. Vi kommer att börja med confidentiality vilket är sekretess.**

Confidentiality

Tekniska frågor:

42. **F1: Vad använder företaget för säkerhetsutrustning till information? Det kan vara brandväggar eller VPN om du vet det.**
43. I: Jag vet inte ifall det finns något generellt där heller…

44. **F1: Okej.**

45. I: ... att svara på. Sen kan jag inte så mycket på de andra projekten i övrigt. Just i den biten är det mycket hur kunden upplever vad säkert ska vara och sen är man ofta flera stycken som är inblandade. I mitt projekt nu har vi ju servrar och SSHR hit och dit och det är ganska mycket. Och sen kan vi inte ge oss in på något kvickt sätt kundens applikationer i produktion så här heller. Så just på den biten känns det ganska genomtänkt.

46. **F1: Använder företaget någon säkerhetsutrustning för intern information? För att skydda från utomstående, människor, att ta sig in till företagets information?**
47. I: För att andra ska ta sig in här? Nej alltså, hur menar du med att ta sig in här?

48. **F1: Har ni brandväggar, använder ni någon sån?**

49. I: Jag har väl bara antagit det egentligen, det är faktiskt ingenting jag kan svara på. Jag har antagit att det ska vara så ifall man skulle vara utsatt från någon form av attack medan jag sitter på vårt nät här. Det är lite knepigt.

50. **F1: Du jobbar med utveckling så vilken sorts information har du tillgång till och med vilket tekniskt redskap?**

51. I: Vilken information.. jag har tillgång till jättemycket information. Man kan specificera lite mer vad för typ av information emellan.

52. **F1: Du får beskriva exakt det du vill - sån information du behöver för att kunna utföra ditt arbete.**

53. I: Om våra kunder eller om oss eller?

54. **F1: Både och.**

55. **F2: Framför allt… det är en liten svår fråga men framförallt liksom internt. Har du tillgång till information generellt eller hur det ser det ut?**

56. I: Jag har tillgång till information som jag behöver. Sen har jag inte letat efter mer information än så. Inte sett någon anledning till det. Jag har ju tillgång till information som angår mig.

57. **F1: Har du tillgång till information som inte angår dig?**
58. I: Det beror på. Jag kan ju säga ja på den frågan men det kan vara information som av dess naturlighet är meningslöst.

59. **F1 & F2: Mm.**

60. I: Och då är det inte så relevant kanske för just det här. Det är klart att jag har tillgång till information som inte angår mig egentligen men inte som är av någon form av…

61. **F1: Vesäntlig information?**

62. I: Nej precis, inte som är känslig.

63. **F2: Nej, okej.**

64. **F1: Vad använder du för tekniskt redskap? Laptop, stationär dator?**

65. I: Laptop och mobil. Den biten.

Strategiska frågor:

66. **F1: Vi undrar lite vad har företaget för policys angående informationsdelning? Känner du till något sådant? Vad får du dela med dig och sådant?**
67. I: Om vårt företag vet jag inte. Jag vet att när jag jobbar med kunder, då är det såklart svart på vitt på papper om vad man får dela med sig och inte. Just angående företaget i sig, nej inte direkt några policys vad jag vet. Sen som sagt har jag inte riktigt fått någon sån utbildning alls eller vad det nu är, utan det är vett och etikett där också kanske som gäller.

68. **F1: Ja. Vi vet ju då att du inte riktigt vet, eller det kanske inte finns några policys inom sekretess men vi undrar:**

69. **F1: Vad du får dela med dig till utomstående och var går gränsen? Om det är familj eller vänner - vad får du dela med dig till folk som inte har med projektet att göra eller inte arbetar inom företaget.**
70. I: Just för projekt så är det väldigt specifikt. Projekt är projekt och om vad man får lov att dela med sig men många vill inte alls att man ger ut någon form av känslig information som kan hjälpa eller stjälpa.

72. **F1: Är det på kundens begäran då, att inte dela med sig information?**

73. I: Ja det är mycket det såklart. Det är inte så konstigt att kunder är lite rädda, för att de vill ju skydda sin egen produkt så att säga.

74. **F1: Mm. Tror du att det finns väldigt mycket tillit i er att inte läcka information?**

75. I: Jag tror att folk litar på att jag inte delar med mig av saker som jag inte får dela med mig men det är ingen som hade kunnat stoppa mig från att gå och bryta kontrakten och avtal och styrelsen pratar ju jättemycket såklart. Men så är ju världen.

76. **F1: Nej precis. Vi kommer att gå vidare till integritet.**

Integrity

Tekniska frågor:

77. **F1: Vi undrar lite om hur företaget arbetar med backup av information?**
78. I: Backup av information, ja…

79. **F1: Det kan gälla kod, det kan gälla intern information eller något sådant.**

80. I: Ja rent generellt när det gäller utveckling har vi GitHub. Vi ju allt möjligt och flera databaser och liknande så där är det aldrig någon panik direkt. Där brukar vi vara ganska på det klara på både de externa databaser och lokala databaser, eller så på allt möjligt.

81. **F1: Mm.**

82. I: Backup av information, det är väl ifall du har information som du känner dig är känslig så får du se till att du har backup på den ifall det inte är någon form av utvecklingsområde. Alltså säg mejlkonversationer och såna saker som har med kunder att göra och så vidare - det är lite upp till var och en tror jag. Se till att inte bli av med dem.

83. **F1: Skulle du säga att ni gör egna backups på er information eller görs det automatiskt via GitHub?**

84. I: Ja alltså jag kan svara för mig i alla fall och i mitt projekt då…

85. **F1: Ja absolut.**

86. I: ... ifall vi pratar utveckling och där har vi GitHub. Där har vi allt.

87. **F1: Och den uppdateras automatiskt då?**

88. I: Ja alltså vi gör ju ”commits” till den och delar med oss information och sen finns det, jag vet inte vad man kallar, hur inne ni är i …

89. **F2: Men det är versionshantering då?**

93. I: Versionshantering då men där kan man ha mängder med olika grenar egentligen av samma sak. Det är ju ett väldigt bra sätt om man kan kalla det backup eller inte. Men man kan gå till vilket skede som helst i ens utveckling när som helst.

90. **F1: Mm det låter ju jättebra**.

Strategiska frågor:

91. **F1: Eftersom du jobbar med utveckling, i vilken grad får ni ändra information och om ni får, hur gör ni det?**
92. I: Ja hur vi gör, det beror ju helt på vilken information det är. Den är svår att fråga på om vi får ändra information. Vi får ju ändra precis vad vi vill göra så länge vi inte gör någonting dumt egentligen. Vad för typ av information är ni intresserade i här? För att ändra information är väldigt…

93. **F1: Det är väldigt generellt men..**

94. I: Väldigt brett.

95. **F1: Men om vi säger informationen du har tillgång till - får du ändra allting? Eller finns det en viss gräns?**

96. I: Nej det får jag absolut inte göra.

97. **F1: Så det finns ändå en viss gräns på saker och ting du får ändra om det skulle behövas.**

98. I: Ja, ja. Jag kan ändra jättemycket saker och sen så finns det mycket - vi har tillgång till alla saker som hade varit jättedumt att göra, både för mig personligen och för hela företaget. Absolut.

99. **F1: Tror du att det finns en stor tillit i dig för företaget?**

100. I: Ja, dels det och att det inte hade gått annars. Jag måste ha tillgång till den här informationen för att kunna göra mitt jobb. Och sen så hade det såklart gått att fixa i efterhand, det är inte så att det hade blivit någon form av katastrof - att ingenting hade funkat därefter, men det kanske hade tagit någon dag att få allt på plats sen. Såklart för det kan ju skada kunden och skada allt möjligt ifall vi ställer till det. Så det är klart att det finns tillit, det måste det ju göra.

101. **F1: Ja, det håller jag med om.**

102. **F1: Eftersom ni kan ändra information, hur säkerställer ni riktigheten av information? Hur vet ni att informationen är så riktigt som den måste vara?**
103. I: Det är också, vill man säkerställa riktigheten av information måste man lägga någon form av antagande på den information som jag vill säkerställa. Då måste den vara väldigt, alltså den ska vara specifik på något sätt, den måste vara känslig information till exempel som på något sätt påverkar någonting som jag faktiskt vill säkerställa att den här informationen är riktigt. Och då finns det jättemycket versioner jag kan ändra som jag kanske inte riktigt bryr mig om ifall den är riktig eller inte. Sen är det ju svårt ändå för jag vet inte ifall jag har någon riktig information jag vill kunna säkerställa. Om jag ska vara helt ärlig så är det jättemycket användare och sådant - det är väl 300 000 användare i något system och så vidare. Men jag är inte så intresserad av ifall det är riktig information - ifall den informationen inte är nödvändig på det sättet för att allting ska fungera utan det är mer för kunderna som använder det senare. Dem har riktiga personer som använder det och inte 300 000 kloner typ.

104. **F1: Mm. Den sista komponenten är tillgänglighet så vi kommer bara ställa några frågor på det också.**

Availability

Tekniska frågor:

105. **F1: Utifrån de teknologiska systemen du har tillgång till, har du någonsin upplevt att du inte kommer åt information som du är i behov av?**

106. **F1: Det kan vara hos en kund, det kan vara internt…**
107. I: Ja såklart alltså det beror ju lite på förutsättningarna man är i situationen men absolut har det ju varit tillfällen där man har velat göra någonting men så kan man inte det för att jag inte kommer åt den här databasen på det här nätet till exempel. Det får jag inte lov att göra, och såna saker har ju hämmat en ibland faktiskt.

108. **F1: Mm, hur gör ni för att fixa det? Måste ni fråga då kunderna eller någonting om…**

109. I: Nej, det är bestämmelser som har legat länge för det här projektet som jag sitter i - det har varit i gång i ganska många år. Det är jag i så fall som får anpassa alltså mig liksom och göra något annat under tiden snarare än att jag ber att få komma åt vissa saker var jag än är, när dom redan har sagt att "så här är det". Absolut. Sen är det ju så att om en server går ner eller whatever som man vill komma åt ibland så blir det ju jobbigt. Då får man vänta.

110. **F1: Okej, det låter bra.**

111. **F1: Vet ni, eftersom du arbetar med utveckling, vad ni använder för säkerhetsprogram?**
112. I: För säkerhetsprogram. Jag specifikt som utvecklare eller?

113. **F1: Ja, det du arbetar med.**

114. I: Det är väl inte räknat som säkerhetsprogram. Du menar - anser du att säkerhetsprogram är anti-virus och sådant här ni pratar om eller menar ni något annat?

115. **F2: Vi tänker generellt. Vi vill liksom veta lite om vad - om vi säger säkerhetsprogram, vad tänker du då?**

116. I: Jag vet inte riktigt vad jag tänker men det är väl snarare anti-virus i så fall som jag kanske…

117. **F1: För att förhindra från att utomstående skulle kunna komma åt liksom er kod som ni arbetar med eller någonting för att komma och förstöra?**

118. I: Ja precis, jag är lite i en situation där vi till exempel använder GitHub för vår versionshantering och jag får då på något sätt, som utvecklare, lita på att dem sköter sin säkerhet där så att ingen annan kan gå in och fixa våra saker medan jag då får lösa min säkerhet här. Dem har ett helt annat arbete här och får se till att dem enskilda som kommer åt är faktiskt dem personerna som dem är medan jag får se till att den som använder mitt konto är jag och ingen annan.

119. **F1: Mm.**

120. I: Det blir lite det ansvaret jag känner att jag har där så man pratar säkerhetsprogram på det sättet så borde det ju nästan vara på min dator då eller liknande. Då är det väl anti-virus program. Så har väl jag en uppfattning om något anti-virus program. Dem är inte så jätteeffektiva längre. Jag använder det som kopplas till Windows 10 och det är ganska bra för att följa med så här… Men det fångar ju bara det lilla och det kända egentligen. Det finns inget anti-virus program idag som kan fånga dem bästa och dem nya - det finns för många virus. Då gäller det snarare att inte klicka på den där konstiga länken i mejlet.

121. **F1: Mm, det här är en liten sidofråga som jag funderar på nu. Vet du om alla anställda på det här kontoret har samma anti-virus program på alla jobbdatorer?**

122. I: Nej det har jag ingen aning om och det skulle inte förvåna mig ifall någon inte har ett anti-virus program i överhuvudtaget. Det är ingenting som jag hade höjt på ögonbrynen för heller, utan det är inte konstigt. Jag vet många som kör bara för att, fast det knappt är lönt längre.

123. **F1: Så företaget ställer inga krav på att alla ska ha säkerhetsprogram?**

124. I: Nej, det har jag inte hört någonting om alls.

125. **F1: Okej, jag tänkte bara på det. Och det var jättebra.**

126. **F1: Hur ser företaget på säkerhet mot utomstående? Liksom med det här kontoret - det kan vara tillgångskort, hur skulle du se deras syn på det?**

127. I: Precis, den är en intressant fråga. Jag har inte jobbat här så länge så på förra, ja jag var på det förra kontoret i en vecka som var i stan, och där kändes det ju säkert, tryggt absolut. Det var högt upp och var kod och allt för att bara komma in igenom entrédörren till byggnaden och sen upp, och sen igen för att komma in i kontoret så att säga. Här är det lite annorlunda - sen har man inte varit här särskilt länge men det är väl på g det här med lås och liknande. Sen här är ju larm och galler och så men det kommer dagligen in folk ”Vet ni var detta är någonstans?” och ”Ah, kan inte vi gå igenom här borta?”. Ibland har det varit ganska mysko situationer faktiskt.

128. **F1: Hur känns det för dig att vem som helst kan komma in när ni sitter bara meter ifrån och jobbar?**

129. I: Det känns inte alls bra, speciellt inte när man har datorer och sådant som ligger här. Man vill på något sätt känna sig helt säker här och kunna vara lite glömsk kanske utan att det ska kunna straffa sig. Sen vet man att det är tanken också. Det är bara att allt sådant tar sån tid.

130. **F1: Nej, det är förståeligt.**

Strategiska frågor:

131. **F1: När det gäller utskick av information till rätt mottagare, det vill säga någon kund, vet du vad ni har för policys när det gäller din arbetsroll? Vad du får skicka ut.**
132. I: Nej, det vet jag inte. Det har jag faktiskt ingen koll på i överhuvudtaget. Jag skickar inte så mycket mejl och så kunder är det väl mest möten och i så fall enstaka mejl och Slack. Jag vet inte ifall ni känner till det, det är en sorts chatt-klient som är ganska välanvänd. Jag står ju inte så mycket för det här bakom, i vår ruta, utan nu är det hands-on och att skapa saker. Jag står inte för den mesta kundkontakten om man säger så.

133. **F1: Mm, det leder lite till avslutningsfrågan.**

136. **F1: Det går lite tillbaka till allmänna frågar och då är det hur du ser på IT-avdelningen? Jag vet att ni inte har någon IT-avdelning men hur skulle du se på en IT-avdelning och vad rollerna på en IT-avdelning är?**
137. I: Vi har väl en IT-person tror jag här i Malmö.

138. **F1: Typ en IT-ansvarig?**

139. I: Ja precis. Det är väl ingenting jag har gått och tänkt på direkt egentligen i överhuvudtaget men det är en person som ska se till att det ska fungera egentligen. Jag tycker, rent säkerhetsmässigt, kanske inte man ska lyfta för mycket ansvar på en, nu är det ingen avdelning såklart, utan en IT-person. Hade man behövt en IT-avdelning så hade man faktiskt kunnat ha som mål att gruppen ska ha vissa egenskaper så man kan sätta förutsättningar på att dem sköter säkerheten för hela kontoret. Och det tycker inte jag är lika rimligt när man har en person som är här ibland. Utan det är mer att se till att saker fungerar, se så att servrar fungerar och allt det här. Jag hade personligen inte

tyckt att en person skulle sköta säkerheten.

140. **F1: Den tekniska säkerheten då?**

141. I: Ja precis.

142. **F1: Det låter jättebra.**

143. **F1: Har du några övriga kommentarer eller något du vill lägga till som du känner att du inte fick igenom?**
143. I: Nej, jag tror inte det.

Referenser

Agarwal, A. & Agarwal, A., 2011. The Security Risks Associated with Cloud Computing. *International Journal of Computer Applications in Engineering Sciences,* Volym 1, pp. 257-259.

Al-Hamdani, W., 2009. Non risk assessment information security assurance model. *Information Security Curriculum Development Conference on - InfoSecCD '09,* pp. 84-90.

Dhillon, G., 2001. *Information Security Management: Global Challenges in the New Millennium.* United States: IDEA Group Publishing.

Dhillon, G. & Backhouse, J., 2000. Information System Security Management in the New Millenium. *Communications of the ACM,* 43(7), pp. 125-128.

Dutta, A. & Roy, R., 2008. Dynamics of organisational information security. *System Dynamics Review,* 24(3), pp. 349-375.

Dynabyte, 2016. *Är säkerhet ett säkerhetsproblem?.* [Online]
Available at: http://www.dynabyte.se/blog/2016/03/02/ar-sakerhet-ett-sakerhetsproblem/
[Använd 4 April 2016].

Gonzalez, J. J. & Sawicka, A., 2002. *A Framework for Human Factors in Information Security.* [Online]
Available at: http://www.wseas.us/e-library/conferences/brazil2002/papers/448-187.pdf
[Använd 10 Maj 2016].

Hedström, K., Kolkowska, E., Karlsson, F. & Allen, J., 2011. Value conflicts for information security management. *Journal of Strategic Information Systems,* Volym 20, pp. 373-384.

Hight, S. D., 2005. *The Importance of a Security Education, Training and Awareness program.* [Online]
Available at: http://www.infosecwriters.com/Papers/SHight_SETA.pdf
[Använd 8 April 2016].

Human Factors and Ergonomics Society, 2016. *Definitions of Human Factors and Ergonomics.* [Online]
Available at: http://www.hfes.org/Web/EducationalResources/HFEdefinitionsmain.html
[Använd 12 Maj 2016].

IsecT Ltd. (2016). *ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls (second edition).* [Online
Available at: http://www.iso27001security.com/html/27002.html
[Använd 26 Maj 2016].

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

Katsikas, S. L. J., Backes, M., Gritzalis, S. & Preneel, B., 2006. *Information Security.* Germany: Springer Science & Business Media.

Layton Sr., T. P., 2005. *Information Security Awareness: The Pshycology Behind the Technology.* Bloomington, Indiana: AuthorHouse.

LeVeque, V., 2006. *Information Security: A Strategic Approach.* New Jersey, United States: John Wiley & Sons, Inc..

Nullbyte, 2014. *Open Curtains In Swish Payments Service.* [Online]
Available at: http://blog.nullbyte.eu/open-curtains-in-swish-payments-service/
[Använd 6 Mars 2016].

Phoenix TS. "CIA Triad (Security Triad) - CISSP Training Series."4 Juni 2012. Online video clip. *Youtube*. Använd 27 April 2016. <https://www.youtube.com/watch?v=SP8cr0fg5Sg>

Siponen, M., 2000. A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8 Januari.pp. 31-41.

Stanton, J., Mastrangelo, P., Stam, K. & Jolton, J., 2004. *Behavioral Information Security: Two End User Survey Studies of Motivation and Security Practices*, New York: Proceedings of the Tenth Americas Conference on Information Systems.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems Eur J Inf Syst, 18*(2), 101-105.

Wilson, K. S., 2013. Conflicts Among the Pillars of Information Assurance. *IEEE Computer Society*, Juli/Augusti, pp. 44-49.

Wylder, J., 2003. *Strategic Information Security.* United States: CRC Press.