LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Medvetenhet om informationssäkerhet

Skillnader mellan anställda och konsulter

Kandidatuppsats 15 hp, kurs SYSK02 i Informationssystem
Framlagd Maj 2015

Författare: Filip Alpteg
Gustav Malm
Martin Sonesson

Handledare: Umberto Fiaccadori

Examinatorer: Bo Andersson
Anders Svensson

Medvetenhet om informationssäkerhet: Skillnader mellan anställda och konsulter

Författare: Filip Alpteg, Gustav Malm, Martin Sonesson

Utgivare: Inst. för informatik, Ekonomihögskolan, Lund universitet

Dokumenttyp: Kandidatuppsats

Antal sidor: 34

Nyckelord: Informationssäkerhet, Medvetenhet, Konsulter, Fast anställda

Sammanfattning:
Informationssäkerhet är idag en stor angelägenhet för organisationer runt om i världen. I takt med att den tekniska utvecklingen går framåt skapas allt fler sätt där känslig information blir utsatt för externa hot. Det finns idag många studier kring informationssäkerhet där granskning sker gällande den mänskliga faktorn, som är en viktig komponent inom detta område. Den mänskliga faktorn innebär även att det skapas interna hot där företag idag ofta brister. På grund av det agila arbetssätt som många organisationer har idag blir det allt vanligare med externt inhyrd arbetskraft. Detta i sin tur ökar problematiken för hur företag ska agera när det kommer till att informera sina anställda om hur informationssäkerhet ska hanteras. I denna uppsats utförs en jämförande studie som granskar skillnaden mellan externa konsulter och fast anställdas medvetenhet kring informationssäkerhet. Resultatet visar på en skillnad där konsulternas medvetenhet överlag är sämre. Avslutningsvis redovisas även exempel på vad företag borde tänka på för att minska denna skillnad.

Innehåll

Figurer

Tabeller

1 Inledning

Informationsteknologin har utvecklats enormt under de senaste åren, och är idag en väsentlig del av de flesta organisationers verksamhet. På samma sätt har även de som använder sig av teknologi utvecklats. Förr såg användare annorlunda ut, då de som jobbade inom IT-branschen ofta var experter på datorer och informationsteknologier. Eftersom det endast fanns ett begränsat antal människor som jobbade inom denna bransch, krävdes det också att de var insatta i hur teknologin fungerade. Intresset för IT drev också de involverade att söka sig till denna bransch. I takt med att teknologin har utvecklats och automatisering skett gällande de flesta verksamheter, har antalet IT-användare ökat dramatiskt. Dagens användare når dock inte upp till samma standard rent kunskapsmässigt, då användandet av dagens teknologi kräver mindre förståelse gällande de processer som utförs i praktiken. Detta leder ofta till att brister uppstår inom de branscher som är helt beroende av IT. En stor angelägenhet som innefattas i dessa brister gäller hanteringen och säkerheten kring den känsliga information som är kopplad till organisationers verksamhet. Eftersom det idag även finns mer information kopplad till företag ökar också kraven på företagen och dess anställda gällande medvetenheten kring informationssäkerhet (Tomson &Von Solms 1998).

"Empirical and anecdotal evidence indicates that the number of incidents related to information security is increasing (AIRC 2008; Symantec 2009) even as organizations invest more in technology-based solutions. Success in information security can be achieved when organizations invest in both technical and socio-organizational resources." (Bulgurcu, 2010, 524).

1.1 Bakgrund

Informationssäkerhet är idag en stor fråga bland företag då information är en av de mer värdefulla resurser som ett företag kan ha. Ett problem som ofta uppstår är svårigheten att uppskatta vilken effekt som den specifika informationen kommer att ha på företaget. Detta leder i sin tur till att informationsvärdet är svårt att specificera (Cavusoglu, 2004). Det går däremot att uppskatta om informationen kan vara värdefull. Det är till exempel skillnad på information som berör produkter som redan finns på marknaden, och information om produkter som ännu inte har nått marknaden. Uppskattningen av värdet på informationen avgör hur mycket säkerhet som krävs för att skydda den. Ett företag kommer inte att lägga onödiga resurser på att skydda information som inte har något reellt värde (Peltier, 2005).

Att skydda informationen på företaget med tekniker som t ex brandväggar och antivirus är väldigt vanligt. Enligt en undersökning gjord av D'Arcy et al. (2009) uppger 70 % av de till-

frågade företagen att de använder teknik för att skydda sin information. Till exempel virusskydd och brandväggar. Men endast 28 % uppger att de har ett Security education technology awareness (SETA) program för att öka de anställdas medvetenhet (D'Arcy et al., 2009). Endast 13 % av företagen uppger att anställdas medvetenhet är ett av deras topp tre informationssäkerhetsområden som de lägger resurser på enligt undersökningen av Ernst & Young (2003). Det framgår i en annan undersökning som utförts av D'Arcy et al. (2009) att bara ca 25-50% av alla säkerhetsbrister uppstår från utomstående aktörer, medan 50-75% kommer inifrån själva företagen. I ytterligare en undersökning som genomförts av Bulgurcu (2010) ligger den interna hotbilden på 64 %. Ofta är det alltså anställda på företaget som gör misstag som leder till att utomstående aktörer kan komma åt hemlig information. Detta innebär att företagen hade kunnat få bättre säkerhet om de hade omfördelat hanteringen av sina resurser. Om de istället hade lagt mer resurser på att utbilda sina anställa att bli mer säkerhetsmedvetna hade det skett mindre misstag som leder till säkerheten brister inom företaget (D'Arcy et al., 2009).

Företag har ofta en informationssäkerhetspolicy (ISP). Men vet de anställda vad företagets policy säger? Om de anställda inte vet vad företagets policy säger blir policyn helt verkningslös, även om den tar upp varenda detalj gällande säkerheten. Om policyn tar upp hur mail ska skickas externt genom kryptering och vad för slags information som inte får skickas, men den anställda inte vet om regleringen, så uppfyller inte policyn sitt syfte. Företagen kan skapa ett Information Security Awareness program (ISA) eller ett Security education technology awareness program (SETA), där de utbildar de anställda i säkerhetsfrågor samt informerar de anställda om vad företagets policy säger (D'Arcy et al., 2009).

Konsulter utgör en stor del av dagens teknikföretag, då det är enklare att justera hur mycket personal som behövs i de olika konjunkturerna. Antalet datakonsulter ökar med varje år som går och det blir allt vanligare att företagen använder flera konsultbolag, som de hyr in konsulter ifrån (IT-statistik, 2015). Men är dessa konsulter som egentligen tillhör ett annat företag, lika säkerhetsmedvetna som den personal som är fast anställda av företaget? Eller har de ett sämre säkerhetstänk då de inte på samma sätt tillhör det specifika företaget?

1.2 Problemformulering och frågeställning

IT-företag hyr in allt fler konsulter från bemanningsföretag. Interna säkerhetsbrister utgör en större del av de säkerhetsbrister som uppstår i företag. Eftersom informationssäkerheten är en kritisk faktor är det av stor vikt att ta reda på hur IT-företag hanterar inhyrd arbetskrafts Information Security Awareness (ISA) gentemot den egna anställda personalens. Då interna risker relaterade till informationssäkerhet kan bli förödande för företagen, blir det essentiellt för företagen att hålla en jämn nivå hos samtliga anställda gällande deras medvetenhet.

Vår forskningsfråga blir därför hur Information Security Awareness (ISA) skiljer sig mellan fast anställda och externa/inhyrda konsulter inom företag i IT-branschen?

Syftet är att få fram en bild av hur medvetenheten inom informationssäkerhet skiljer sig mellan inhyrda konsulter som jobbar på företag och de som är fast anställda av företaget. Eftersom säkerhetsrisker ofta finns inom organisationer vill vi genomföra en studie som tar reda på om det finns någon väsentlig skillnad mellan personal med varierande anställningssituationer. Då det blir allt vanligare med inhyrd arbetskraft i form av konsulter vill vi fokusera på hur ISA skiljer sig på detta plan.

1.3 Avgränsningar

Eftersom vi tror att anställda på IT-företag har bättre medvetenhet kring säkerhet hade det gett en felaktig bild att jämföra IT-företag med andra sorters företag. Då det är skillnaden mellan konsulter och fast anställda vi vill undersöka och inte skillnaden mellan olika företag, begränsar vi studien till denna bransch. Vi kommer också endast att granska de anställda och exkludera ledningen samt de informationssäkerhetsansvariga på företagen.

2 Teoretisk referensram

2.1 Interna vs externa hot för organisationer

Det finns många debatter gällande var de största säkerhetsriskerna finns gällande informationshantering. Idag finns många externa hot som organisationer måste hantera och skydda sig emot. Då externa hot alltid är en risk att stöta på lägger många företag ner stora resurser för att skydda sina system från dessa hot som kan inkludera hackare, bedragare och de som är inblandade i industriellt spionage. Då fokus ofta lagts på externa hot har företag ofta haft stora brister med att följa upp de interna brister som lett till att de externa hoten uppstod i första taget (Wall, 2013).

När man tar upp interna hot som borde hanteras för en organisation finns det två typer av primära problemområden som är viktiga att analysera. Det första är avsiktliga interna hot som utförs av de egna anställda som vill skada företaget medvetet. Detta kan bestå av parter där anställda jobbar för egen vinning eller åt en tredje part. Det andra problemområdet är där oavsiktliga misstag begås av de anställda som beroende på olika anledningar inte följer de policies som är uppsatta för den gällande organisationen. Det kan utöver detta finnas flera orsaker till att säkerhetsbrister uppstår omedvetet bland personalen som hanterar känslig data. Exempel på detta kan vara bristande policies eller dålig kommunicering inom ett företag gällande vilka policies som gäller (Wall, 2013).

När det kommer till att identifiera säkerhetsrisken och var den i grund och botten har uppstått är det av intresse att se över hur de specifika användarna har agerat. När det gäller oavsiktliga misstag som begåtts av anställda finns det i sin tur två typer där risker för bristande informationshantering uppstår (Wall, 2013).

2.1.1 *Den välmenande anställde*

Som det låter har den välmenande anställde inget uppsåt med sitt agerande. Denna typ hanterar ärende som de ska utföras, men kan tack vare antingen bristande förståelse för de policies som finns tillgängliga eller undermålig hantering av känslig data, bidra till stora läckor inom organisationen *(*Wall, 2013*).* Exempel på misstag som den välmenade anställda kan vara att välja dåliga lösenord som till exempel *"password"* (Stanton et al., 2004). Det kan även handla om delning av lösenord till kollegor, som är ett vanligt säkerhetsproblem. Då personen ifråga endast vill hjälpa en kollega genom att dela med sig av sitt lösenord, men i själva verket delar med sig av sin identitet. Ifall den som lånat identiteten begår ett brott eller misstag kommer ägaren av identiteten få skulden. Delning av lösenord är ofta förbjudet i policies (Ferreira et al., 2013). Dessa typer av misstag som begås kan vara svåra för ett företag att hantera, då det är svårt att kontrollera varje utförande som sker från de anställda. Misstag är alltid något som kan ske, men genom att lägga resurser på utbildning inom informationssäkerhet minimeras denna typ av anställd inom företaget *(*Wall, 2013*).*

2.1.2 *Den försumlige anställde*

Denna typ består av anställda, medarbetare eller samarbetspartners med legitim tillgång till känslig data, och som kanske inte lägger så stor vikt vid att hantera sina ärenden inom ramen av de uppsatta reglerna gällande säkerheten på företaget. Orsaken till försummandet av säkerhetstänk kan vara varierande men grundar sig ofta i att de vill göra livet enklare för sig själva.(Wall, 2013). Ett exempel på detta kan vara att bristfälligt konfigurera företagets WIFI så att det blir lättare att personligen ha åtkomst, vilket kan leda till att obehöriga personer som står utanför lokalen kan koppla upp sig till samma WIFI och ta del av känslig information (Stanton et al., 2004). Genom att ta genvägar för att nå sina mål negligeras ofta de policies som ledningen skapat. Även om den försumlige anställde inte agerar för att skada företaget, kan denna typ av risktagande ge företaget omfattande problem. Det kan även vara svårt för företaget att förebygga då det finns situationer då vederbörande varit medveten om de "misstag" som begåtts (Wall, 2013).

2.1.3 *Exempel på bristande informationssäkerhetsmedvetande*

Då företag ständigt kan vara utsatta från hot utifrån, är det extra viktigt att hela tiden jobba för att minimera de brister som finns inom organisationens säkerhetshantering. Det är därför av stort intresse att genom noggrann studie, se över vilken typ potentiella läckor som kan leda till att känslig information hamnar i fel händer. Det finns både vanliga och ovanliga sätt för data att exponeras för yttre hot, men med god medvetenhet om några av de vanligaste felen som utförs är det ofta lättare att förebygga internt risktagande. Några av de vanligaste sätten där information utsätts för extern exponering kan vara exempelvis att de anställda (Wall, 2013):

1. Oavsiktligt avslöjar information
2. Gör data osäker genom att ta genvägar
3. Lämnar känsliga uppgifter på hårddiskar i kasserade maskiner
4. Inadekvat hanterar data som delas med tredje part
5. Skickar osäkra uppgifter via offentliga post- och leveranstjänster
6. Inte uppdaterar e-post och distributionsinformationslistor
7. Inte granskar användarnas åtkomsträttigheter

Samtliga av dessa risker som är vanliga beror ofta på att anställda inte utför sitt arbete på korrekt sätt (Wall, 2013). Riskerna räknas som naiva misstag som inte kräver någon speciell teknisk kunskap att utföra, samt inte är menade att skada företaget (Stanton et al., 2004).

2.2 Aspekter inom informationssäkerhet

Informationssäkerhet är en kritisk faktor för företag i dagens samhälle. Då känslig information kommuniceras ut i större utsträckning än någonsin tidigare inom företag, har fler risker skapats för att denna information ska hamna i fel händer och missbrukas av obehöriga. Det finns

fem viktiga aspekter som behöver beaktas för ett företag gällande informationssäkerhet. (Bishop, 2003)

Säkerhetskrav (Security requirements)
Det är stor skillnad på hur olika organisationers säkerhetskrav ser ut gällande informationshantering. För att få en klar bild över vilka hot och risker som ett företag utsätts för är det väsentligt att skapa tydliga krav för vad det potentiella säkerhetssystemet ska innehålla. För att få fram en tydlig kravspecifikation är det viktigt att ställa enkla frågor till sig själva inom företaget. Exempel på dessa frågor kan vara: Vilken information är känslig? Hur känslig är den? Hur hanteras den känsliga informationen? Osv. (Pfleeger, 2003),(Bishop, 2003).

Säkerhetspolicy (Security policy)
Ur den kravspecifikation som skapats framställs en policy som företaget ska följa gällande hantering av information. En policy består ofta av villkor som ställs på de anställda inom företaget (Whitman, 2003). Exempelvis vad som är tillåtet och vad som inte är tillåtet inom det potentiella systemet. Här skapas även riktlinjer som de anställda ska följa och beroende på företagets agerande anpassas policyn efter hur den känsliga informationen ska hanteras. Om den policy som skapats för företaget inte efterföljs av dess anställda, blir denna verkningslös och dess existens onödig (Bishop, 2003).

Säkerhetsmekanismer (Security mechanisms)
Säkerhetsmekanismerna är de som tvingar fram eller utför åtgärder inom säkerhets policyn. Mekanismernas ansvar är att inte låta företaget hamna i ett ofunktionellt säkerhetstillstånd. Exempel på dessa kan vara restriktioner inom ett system där användare med icke behörighet inte har åtkomst till speciell information. Dessa är mer av en teknisk art och används som en kontroll för att främja anställda att följa de policies som är skapade för organisationen. De ger ledningen verktyg att hantera och kontrollera att säkerhetspolicies efterlevs (Whitman, 2003),(Bishop, 2003).

Säkerhetsgarantier (Security assurances)
Det finns inga garantier för att en organisations säkerhetssystem är heltäckande och ogenomträngligt. Men för att bedöma hur anpassningsbart och funktionellt ett företag hanterar sin informationssäkerhet finns det olika metoder som kan användas. Dessa metoder kan kallas och användas som security assurances (säkerhetsgarantier). I dessa inkluderas både den tekniska aspekten och den mänskliga faktorn för företaget. Det primära syftet med dessa metoder är att säkerställa att hanteringen kring säkerhets policies inom ett företag efterlevs. Det sekundära syftet är att fastställa hur företaget agerar för att informera de anställda om de krav som ställs av den gällande policyn (Bishop, 2003).

Säkerhetskomponenter(Security components)
De finns många perspektiv att beakta när det kommer till informationssystem. De huvudkomponenter som är viktiga att inkludera i ett företags säkerhetssituation är: de krav som ställs på säkerheten, de policies som skapas utefter kraven samt de metoder och verktyg som används

för att främja en hållbar säkerhetsmiljö för organisationen. För att skapa någorlunda säkerhetsgarantier måste samtliga av dessa komponenter ses över och kontrolleras. Då det på förhand är omöjligt att säkerställa att ett företag är helt skyddat från hot, är det av stor vikt att det specifika företagets metoder kring säkerhetshantering granskas (Bishop, 2003).

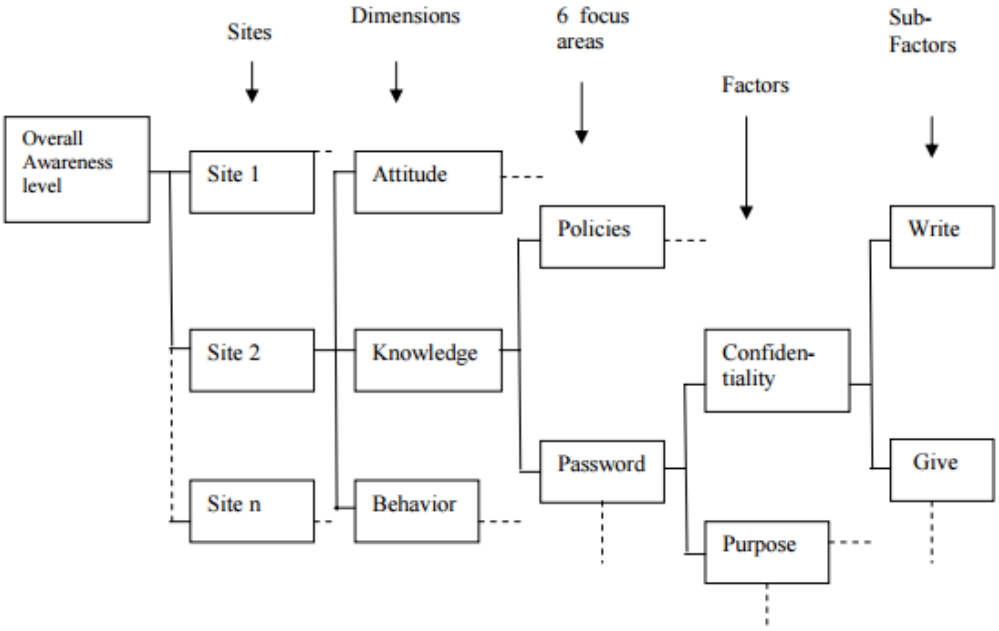
2.3 Mäta informationssäkerhetsmedvetenhet

För att möta hur säkerhetsmedvetna anställda är går det att fokusera på områden som är kritiska för företagets säkerhet. Det kan vara saker som att hålla sina lösenord hemliga eller att använda e-mail och Internet på ett ansvarsfullt sätt. Genom att fokusera på dessa områden får man fram relevanta saker att mäta. Utöver detta kan företaget även göra en mätning som inte mäter säkerhetsmedvetenheten på de områden som är relevanta för företaget. Mätningen kan göras på enskilda avdelningar eller på hela regioner för att se var det behövs sättas in resurser för att öka ISA (Kruger & Kearney, 2005).

Det går att dela upp säkerhetsmedveten i tre olika vyer (Kruger & Kearney, 2005):

1. Kunskap (Vad vet du?)
2. Attityd (Vad tror du?)
3. Beteende (Hur agerar du?)

Dessa tre vyer delas sedan in ytterligare en gång i de områden som företaget har valt att fokusera på. Företaget kan sedan bryta ner områdena som valts och fokusera på mindre delar, för att få en bättre överblick av området. Det bidrar även till att göra det lättare att se var i området problemen faktiskt ligger. Genom att använda ett trädstruktur diagram blir det enklare att dela in problem en strukturerad hierarki, se figur 2.1 (Kruger & Kearney, 2005).



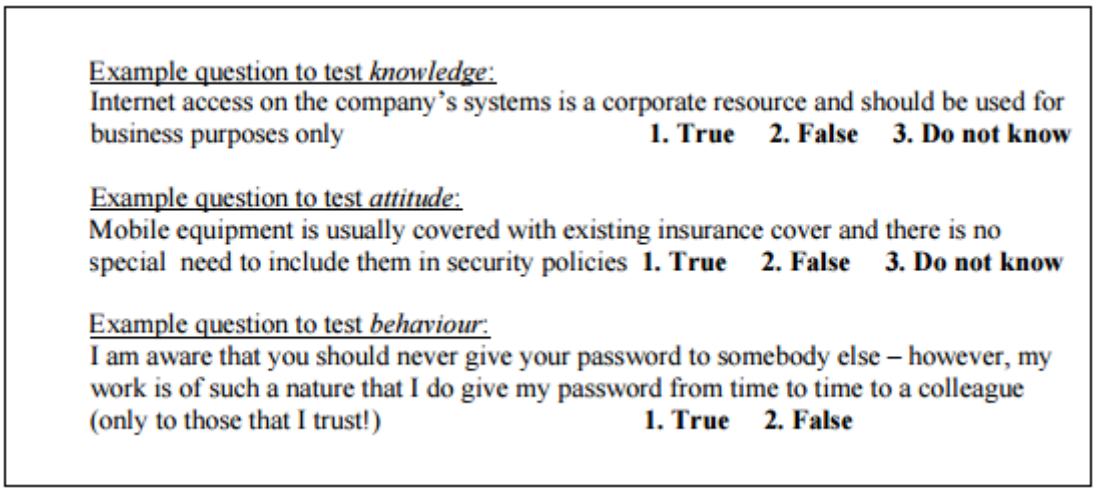
Figur 2.1: Tree structure of problem

För att fastställa vilka områden som mätningarna ska utföras på kan företaget använda sig av en värdebaserad beslutsmetod. En sådan metod består av fyra stycken olika delar:

1. Intervjuer
2. Resultat av intervjuerna görs om till mål
3. Skilja på slutmål och delmål,
4. Sammanställa slutmål och delmål i ett diagram.

Intervjuerna är främst för att fastställa intressenternas mål samt att se vad de har för önskemål, angelägenheter och problem. Resultaten av intervjuerna består av enskilda intressenters syfte och värderingar. Dessa sammanställs till en lista med gemensamma milstolpar. Med hjälp av listan med milstolpar delas de sedan upp i slutmål och delmål. Om ett mål leder fram till ett annat mål klassificeras det som ett delmål. När mål och delmål är fastställda sammanställs de i ett överskådligt diagram. Diagrammet underlättar när relationer mellan olika mål ska tas fram samt kommer att ligga som grund vid beslutsfattanden (Drevin et al., 2007).

Efter fastställandet av områden och delområden ställs ett visst antal frågor till de anställda. Frågorna berör tre olika vyer: kunskap, attityd och beteende. Exempel på frågor inom de olika vyerna kan ses i figur 2.2.



Figur 2.2: Example questions

För att avgöra hur säkerhetsmedvetna de anställda är ges de olika vyerna olika värden beroende på hur företaget värderar vyerna. Till exempel med en skala på 100 så kan företaget värdera kunskap till 20, attityd till 30 och beteende till 50. Sedan ges även värden till de olika områdena. Genom att göra detta kan företaget få fram ett procentuellt värde på hur informationssäkerhetsmedvetna de anställda är. De kan även få en bra bild på var i informationssäkerhetsmedvetenheten det brister och kan då sätta in resurser för att öka ISA (Kruger & Kearney, 2005).

Mätningarna bör upprepas vid flera tillfällen med ett mellanrum på ett antal månader. Upprepade mätningar ger en uppfattning om vilket håll ISA går åt, samt ifall de åtgärder som vidtagits har gett någon nämnvärd effekt. Om de inte har haft någon effekt måste en omvärdering ske om vilka åtgärder som ska vidtas (Kruger & Kearney, 2005).

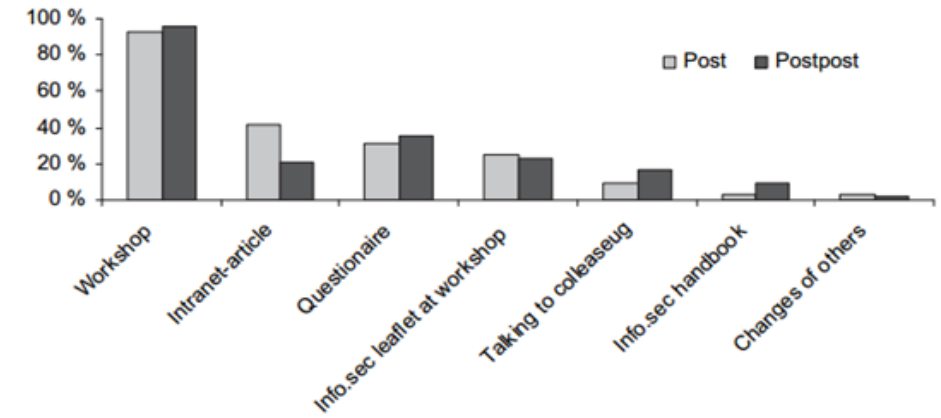
2.4 Öka informationssäkerhetsmedvetenhet

Då ca 50-75% av säkerhetsbristerna i ett företag uppstår inne i organisationen bör företag försöka att öka medvetenhet hos de anställda (D'Arcy et al., 2009). För att öka medvetenheten kan företagen skapa egna ISA eller SETA program där de själva informerar de anställda om de risker de kan stöta på. Det är då viktigt att företaget identifierar de risker som just deras verksamhet kan riskera att råka ut för, och har med risker i sin policy (Hubbard, 2002).

Det finns många sätt att öka medvetenheten hos de anställda. Det kan vara saker som att skicka ut mail med olika risker var vecka, att ha informationen på sitt intranät, sätta upp posters eller ha skärmsläckare med information (Albrechtsen & Hovden 2009). *" Informal methods might include brief newsletter articles, quick notes, lunch meetings, discussion groups, screen savers, posters, and physical reminders like mouse pads, pens, or those neat little tension squeeze balls."* (Hubbard, 2002). De sätt som är mer effektiva är när användarna själva är tvingade att delta. Det kan vara saker som att ha möten med de IT-ansvariga där de får

ställa frågor om säkerheten. Diskussionsgrupper kan även anordnas där de anställda får diskutera informationssäkerhet och bolla idéer med varandra samt lösa några case. Genom att göra användarna delaktiga i informationen kan de inte strunta i den (Albrechtsen & Hovden 2009). Andra informella sätt att öka säkerhetsmedvetenheten är att använda sig av mail och intranätet, där kan personalen själv gå in och kontrollera när de är osäkra (Hubbard, 2002).

Enligt Albrechtsen studie var workshops det mest effektiva sättet att påverka de anställdas medvetenhet då det kräver interaktion av användarna och de måste att tänka efter och diskutera riskerna som finns, se figur 2.3 (Albrechtsen & Hovden 2009).



Figur 2.3: Causes of changes awareness and behaviour employees

Trots att företagen har ett fungerande SETA program samt har hög medvetenhet hos sina anställda hindrar det inte anställda som har för avsikt att begå ett brott och stjäla, förstöra eller modifiera data.

Genom att öka bevakningen av informationsflödet med exempelvis datorövervakning på arbetsplatsen, kan företaget göra de anställda mindre riskbenägna. Detta eftersom att de anställda då vet att fel och misstag de gör kommer att bli upptäckta. Vilket i sin tur minskar risken att en anställd struntar i säkerhetsreglerna. På detta sätt minskar även risken för brott. De gör även att de anställda tänker efter mer när jobbar med viktig och känslig information (D'Arcy et al., 2009).

Det går också att göra straffen för brister i säkerheten mer konsekventa och strängare. Om en anställd vet att det är stränga straff då den bryter mot säkerhetsregler, kommer den att vara mindre benägna att göra detta, även om det är en enkel sak som att låsa datorn då den lämnar rummet. Genom att kombinera stränga straff med datorövervakning kommer det att minska antalet säkerhetsbrister som uppstår inne i företaget (D'Arcy et al., 2009).

Moralen hos de anställda påverkar vilket av antingen ökad datorövervakning eller strängare straff som ger bäst effekt. Hos anställda med hög moral räcker det med vetskapen av att de kan bli upptäckta för att de inte ska bryta mot regler. Däremot hos en anställd med låg moral

är det bättre att förtaget har stränga straff. Det bästa är att kombinera de båda då företaget når båda grupperna (D'Arcy et al., 2009).

2.5 Principal-agent teorin

Principal-agent problem uppstår när en person eller entitet (agenten) har möjlighet att fatta beslut åt, eller beslut som påverkar en annan person eller entitet (ägare). Problemet i sig uppstår när en agent har incitament att agera i sitt eget bästa intresse istället för ägarens (Garber et al., 2011). Till exempel kan en agent ha en tidsram att utföra ett arbete, om han vet att han ligger efter enligt tidsramen kan han ta en genväg, eller inte göra något till 100 % för att ta ikapp tid. Kortsiktigt hjälper det agenten då han har tagit ikapp tid, men det kan senare orsaka stora problem för hur slutprodukten blir och därmed skada ägaren (Holmstrom & Milgrom, 1991).

För att förstå och förebygga detta måste ägaren veta om sina policies och hur de påverkar agenten (Garber et al., 2011, Holmstrom & Milgrom, 1991). Om agenten har möjlighet att fatta beslut utan att ägaren godkänner det, kan det leda till att agenten tar beslut som innefattar en hög säkerhetsrisk för systemet. Alternativt kan agenten ta beslut som endast gynnar honom själv och inte ägaren.

Den största anledningen till att agenter tar genvägar för att uppnå snabbare resultat är för att de är under tidspress. Det är vanligt att ett projekt har en tidsplan, och om projektet inte lyckas hålla planen uppstår extra kostnader för ägaren, ägaren kan då straffa agenten för att han inte har uppnått sina milstolpar i tid. Det är då agenten väljer att ta en genväg, för att visa att han har uppnått milstolpen och därmed slipper sitt straff. Beroende på vilka policies som finns kan dessa genvägar vara mer eller mindre allvarliga. Om agenten har fullmakt för projektet kan vederbörande ta stora säkerhetsrisker för att uppnå målet. Men om policies säger att ägaren måste godkänna sådana handlingar innan de träder i kraft, minskas risken för att dessa säkerhetsrisker uppstår (Garber et al., 2011).

Hur stor risk en agent är villig att ta kan bero på flera olika saker. Garber et al. (2011) tar upp fem olika scenarion som kan påverka agenten: Betalning till agenten för ett uppdrag som blivit utfört enligt tidsplan, hur mycket pengar som ska läggas på att inspektera agentens arbete samt tre straff. De olika straffbara situationerna är: Försening, att bli påkommen med att ta genvägar och för att orsaka ett systemfel som har uppkommit för att agenten har tagit genvägar.

Agenten har nu två val att göra. Han måste välja hur mycket tid och pengar som ska läggas för att kunna hålla deadline eller om han ska ta genvägar för att komma ikapp om han hamnar efter. Agenten håller oftast fast vid de här besluten under hela projektets gång (Garber et al., 2011).

Anledningen till att ägaren skapar ett straff för en missad deadline etc. är för att skapa ett incitament till agenten att hinna i tid. Om inte agenten har något incitament att hålla deadline är

det större risk att han inte håller den. Dock måste tidsplanen vara rimlig, annars ökar risken att agenten använder sig just av genvägar för att hålla den (Garber et al., 2011).

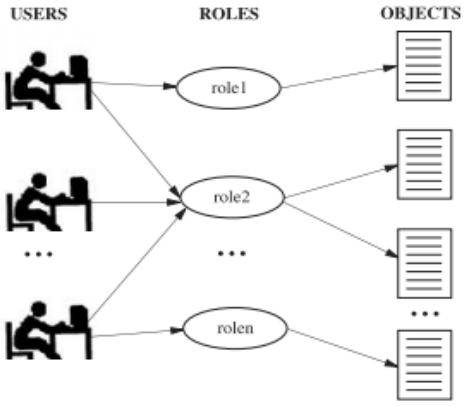
2.6 Rollbaserad behörighetskontroll

För att kunna bestämma vilka användare som ska ha tillgång till specifik data används behörighetskontroller. För att detta ska fungera används olika roller, dvs. de anställda delas in i olika roller beroende på exempelvis vad för arbetsuppgifter de har och sedan får de olika behörighetsnivåer (Samarati, Capitani de Vimercati, 2001). Hur dessa roller delas in kan skilja sig från företag till företag, beroende på hur företagens policies ser ut.

Den mest övergripande metoden att dela in roller är efter titel (Sandhu, R.S., Samarati, P, 1994, Samarati, Capitani de Vimercati, 2001), till exempel alla löneadministratörer måste ha tillgång till viss specifik data för att kunna göra sitt jobb. Det går dock att specificera rollerna ytterligare, exempelvis kan varje löneadministratör endast ha tillgång till en viss avdelning. Allt det här bestäms av företagets policies.

Rollbaserade policies förenklar tilldelningen av behörigheter genom att dela upp uppgiften i två delar: tilldelningen av roller till användare, samt tilldelning av behörighet till objekt åt olika roller. Detta underlättar arbetet att följa policyns, då en administratör endast behöver ge behörighet till användare utefter vilken roll de har (Samarati, Capitani de Vimercati, 2001). D

Ännu en fördel med rollbaserade behörigheter är om till exempel en person blir befordrad. Då är det lätt att ta bort alla behörigheter för den gamla rollen och ersätta dem med behörigheterna för den nya rollen. Om behörigheterna hade varit direkt mellan personer och objekt hade det varit en mycket mer tidskrävande process att ändra alla behörigheter. Det hade även utgjort en större säkerhetsrisk om personen som utför detta arbetet gör något fel och behörigheter ges till fel person (Sandhu, Samarati, 1994), se figur 2.4.



Figur 2.4: Role-based access control

Vi har använt oss av källor som främst berör ämnet informatik. Dessa källor är oftast i form av vetenskapliga artiklar, som har citerats många gånger. I ramverket nedan delas vår teori in i olika områden för att ge en klarare bild över vad som behandlas. Ramverket tar även upp vilka författare som berör de olika områdena.

Tabell 2.1: Teoretiskt ramverk

Område	Beskrivning	Referens
Interna vs externa hot för organisationer	Hur olika hot uppstår inom organisationer och vanliga sätt där känslig data exponeras.	(Wall, 2013) (Stanton et al., 2004) (FERREIRA, et al., 2013)
Aspekter inom informationssäkerheten	Genomgripande om informationssäkerhetens grunder	(Matt Bishop, 2003) (Whitman, 2003) (Pfleeger, 2003)
etMäta informationssäkerhets- medvetenhet	Olika sätt att mäta säkerhetsmedvetenhet. Samt vad som är relevant att mäta.	(Kruger & Kearney, 2005) (Drevin et al., 2007)
Öka informationssäkerhets- medvetenhet	Olika sätt att öka säkerhetsmedvetenheten. T.ex workshops och SETA.	(D'Arcy et al., 2009) (Albrechtsen & Hovden, 2009) (Hubbard, 2002)
Principal-agent teorin	Varför viss personal väljer att använda sig av genvägar för att hinna till deadline, även om det kan innebära en säkerhetsrisk.	(Garber et al., 2011) (Holmstrom & Milgrom, 1991)
Rollbaserad behörighetskontroll	Hur hanteringen av tillgång till viss information sköts genom användning av roller.	(Samarati, Capitani de Vimercati, 2001) (Sandhu, R.S., Samarati, P, 1994)

3 Metod

Hur vi har gått tillväga för att samla in vår empiri. Samt motiveringar för de olika val vi har gjort.

3.1 Kvantitativa och kvalitativa metoder

För att samla in empiriska data kan kvalitativa eller kvantitativa metoder användas.

Kvalitativ metod är en metod som är till för att göra en mer djupgående analys där syftet är att få en förståelse för hur personerna i undersökningen resonerar och tänker om olika ting. Detta görs oftast genom lite längre intervjuer (Jacobsen, 2002).

Kvantitativ metod är en metod där siffror och storlekar står i centrum. En kvantitativ undersökning görs oftast genom ett frågeformulär med fasta alternativ. Detta gör att data blir väldigt enkel att sammanställa. I en sammanställning går det att se skillnaderna och likheterna tydligt och därmed går det att dra slutsatser om varje specifik fråga (Jacobsen, 2002).

För att samla in våra empiriska data har vi valt att utgå från Jacobsen(2002) och använt oss av en blandad uppläggning som lutar åt det kvantitativa hållet. Vi anser att en enkät ger oss tillräckligt med information för att besvara vår frågeställning och vårt syfte då vi inte behöver gå in på djupet. Dock har vi öppna svar på de flesta frågorna för att få ytterligare feedback om inte svarsalternativen stämde in för enkätdeltagaren. Vi vill få en generell överblick för att senare kunna göra en jämförelse.

3.2 Utformning av enkätfrågor

Frågorna till enkäten har vi försökt att använda oss av Kruger och Kearneys metod. Som beskrivs i kapitlet Mäta informationssäkerhetsmedvetenhet. Vi testar de anställdas kunskap och beteende, genom våra enkätfrågor. Exempel på en kunskapsfråga är fråga 1 och 7. Exempel är beteendefrågor är fråga 3 och 5. Vi valde att bortse från attitydfrågor då vi anser att beteendefrågorna även besvarar de anställdas attityd.

Frågorna består mesta dels av scenarier som de anställda får ta ställning till. Genom att ge de anställda fasta alternativ riskerar vi att vi påverkar deras åsikt. Vi valde därför att ha med fasta alternativ för att göra enkäten mer lättsam. Den främsta orsaken till detta är att underlätta för deltagarna och därigenom öka antalet medverkande. För att få ut den information som eftersträvas har frågorna utformats efter den teoretiska referensram som vi skapat i vår litteraturstudie. Nedan går vi igenom syftet med våra empiriska frågor och hur vi tänkt vi utformning av varje specifik fråga.

Indelning*:* **Vad arbetar du som?**

Hjälptext: **Om du är fast anställd på ett företag men är uthyrd som konsult till ett annat företag räknas du som konsult.**

Vi delar upp enkätdeltagarnas olika arbetsroller, där vi specifikt koncentrerar oss på huruvida de jobbar i en extern konsultroll eller är fast anställda med arbetsuppgifter inom den egna organisationen Detta är en nyckelfråga för vår undersökning då den tydligt avgränsar våra olika intervjugrupper.

1. **Har företaget du jobbar för en säkerhetspolicy?**

Frågan fastställer hur medvetna de anställda är kring den säkerhetskontroll som är instiftad i organisationen. Detta är även en viktig fråga för att ta säkerställa att företagen där den anställde jobbar har uppsatta regler för hur personalen ska agera gällande situationer kopplade till säkerheten på sin arbetsplats (Hubbard, 2002). Då vi i teorin har tagit upp syftet med en tydlig säkerhetspolicy är denna fråga essentiell för vår undersökning.

2. **På vilket sätt gör företaget dig mer säkerhetsmedveten?**

Frågan tar reda på vad företagen gör för att göra sina anställda mer säkerhetsmedvetna. Samt ifall företagen har bra vägar att nå ut med information, mer än att få dem att skriva på ett avtal/policy vid anställning. För att jämföra med de informationssätt vi tar upp i stycket *"öka informationssäkerhetsmedvetenhet"*(D'arcy, 2009) som tas upp i teoriavsnitt 2.4.

3. **Du är ledig från jobbet. En kollega ringer och ber om ditt lösenord eftersom de måste ha tillgång till data på ditt konto. Ger du din kollega ditt lösenord?**

Syftet är att se i vilken grad de anställda är benägna att ge ut sitt lösenord till medarbetare. Denna fråga kopplas till *fråga 7* om tillvägagångssätt när man bli ombedd att byta lösenord. Ifall anställda endast ändrar en del av sitt lösenord och lösenordet har fångats upp av obehöriga, har de en enkel väg in i systemet även ifall den anställda byter lösenord.

4. **Du behöver skicka ett mail med information till en extern part. Krypterar du mailets innehåll?**

Frågan kontrollerar hur noggranna de anställda är när det kommer till extern kommunikation. Om de skickar information till externa parter utan att kryptera data finns det risk att informationen avlyssnas och kapas. Denna fråga kopplas till teorin om att oavsiktligt avslöja information genom bristande säkerhetsansvar gällande olika former av informationsutbyte(Wall, 2013).

5. **Du sitter och arbetar och behöver gå ifrån datorn lite snabbt och hämta något. Låser du alternativt loggar ut från datorn?**

Frågan tar reda på ifall de anställda utgör en säkerhetsrisk då de lämnar datorn en kort stund. Ifall de lämnar datorn utan att låsa den riskerar de att någon annan på företaget får tillgång till deras data. Kan även kopplas till *Fråga 8,* som tar upp den fysiska säkerheten på kontoret gällande risker relaterade till huruvida personer utan passerkort kan få tillträde.

6. **Du blir ombedd att byta lösenord av systemet, hur går du tillväga?**

Frågan samlar information om hur anställda gör när de ska byta sina lösenord. Ifall de byter hela eller ifall de väljer det enkla men osäkra alternativet att endast byta en siffra eller bokstav. Fråga 6 kopplas framförallt till teorin om "den välmenande anställde"(Stanton et al., 2004).

7. **Finns det tydligt uppsatta regler för arbete med data utanför företaget?**

Det är inte ovanligt att anställda tar med sig arbete hem från jobbet. Syftet med frågan är att se om det finns regler för hur detta ska ske samt få en uppfattning om hur medvetna enkätdeltagarna är om dessa regler.

8. **Du är på väg in genom dörren. En kollega stannar dig och säger att han har glömt sitt passerkort. Hur agerar du?**

Att kontrollera hur noga de anställda är angående den fysiska säkerheten på kontoret. Denna fråga kan kopplas till *fråga 5,* som ger svar på ifall anställda väljer att inte låsa sina datorer. Risken ökar ifall obehöriga släpps in och datorer är tillgängliga.

9. **Du får tillgång till data som är utanför dina behörigheter. Hur går du tillväga?**

Genom denna fråga vill vi få reda på hur behörigheter hanteras av de anställda. Det vitala med frågan är att få reda på vilket ansvar personalen tar vid uppstående säkerhetsrisker. Det är även av intresse att kontrollera om konsulterna på denna fråga är mer villiga att ta genvägar och gå igenom materialet, vilket kopplas till principle agent teorin som tas upp i teoriavsnitt 2.5.

10. **Du arbetar med en uppgift och behöver hjälp. Du har en kollega som slutat på din arbetsplats men som kan precis det du behöver hjälp med. Den data som du måste lämna ut är någorlunda känsligt men du litar på din gamla kollega. Hur skulle du gå tillväga?**

Ifall de anställda delar med sig av information till anställda som har slutat på företaget riskerar de att data läcker ut till allmänheten. Även om det är en gammal kollega går det inte att vara säker på att han/hon inte vidarebefordrar data för egen vinning. Data som skickas kan heller inte garanteras samma säkerhet runt sig som den har inom företaget. Särskilt inte om företaget utgår från tydligt strukturerade säkerhets policies. Frågan förknippas med punkten " Inadekvat hantera data som delas med tredje part" som tas upp i teoriavsnitt 2.1.

11. Du jobbar med en arbetsuppgift som ska vara klar samma dag, detta kräver att du tar med känslig data hem för att färdigställa uppgiften och därmed nå din deadline. Hur agerar du?

Frågans syfte är att ta reda på hur benägna de anställda är att utföra arbetssysslor i hemmet där hantering av känslig data ingår. Detta är en intressant fråga med koppling till *fråga 7* som efterfrågar information kring de anställdas vetskap gällande företagets reglering av arbete i hemmet.

12. Är du villig att ta genvägar för att nå en deadline?

I principal-agent stycket går vi igenom hur en agent(konsult) kan känna sig tvingad att ta genvägar för att uppnå en deadline. Det finns flera olika orsaker till detta och huruvida en agent är villig att ta genvägar beror både på hur personen i fråga har för inställning samt hur organisationen hanterar en missad deadline. Den här frågans syfte är att se i vilken utsträckning det finns agenter(konsulter) som är villiga att ta genvägar även om det innebär en säkerhetsrisk (Garber et al., 2011).

13. Om någon medvetet utför handlingar som bryter mot säkerheten. Finns det några åtgärder för att förhindra/stoppa det? Om ja, specificera gärna vad i övrigt.

Denna fråga fokuserar på vilka typer av åtgärder som företagen använder för att kontrollera sina anställdas säkerhetshantering. Med frågan vill vi framförallt ta reda på om de anställda har fått redovisat (av sin arbetsgivare) vilken uppföljning som ett bristande säkerhetsagerande kan leda till. Dessa åtgärder är intressanta att ta del av för att utvärdera företagens användande av säkerhetsmekanismer som beskrivs i teoriavsnitt 2.2.

3.3 Val av företag och kontaktsätt

Vi har valt företag som arbetar inom IT. Företagen i undersökningen är större IT-företag och har både konsulter och fast anställda. Företagens kontor är placerade mestadels i Skåne men vi har även inkluderat något företag på annan ort.

Vi försökte att kontakta säkerhetsansvariga på respektive företag. Vi kontaktade 26 företag via mail men endast en bråkdel svarade. Vissa svarade och visade intresse men sedan svarade de aldrig på själva enkäten. Det visade sig även att det var svårt att få de säkerhetsansvariga att vidarebefordra vår enkätundersökning. Vi valde därför att komplettera med personliga kontakter. De personliga kontakterna är personer som vi känner inom de företag som vi i första skedet gett ut enkäten till. Dessa kontakter vidarebefordrade sedan enkäten till kollegor. Vi gick även ut till några av företagen och delade ut fysiska enkäter.

3.4 Utformning av enkätformulär

Vårt enkätformulär innehåller både kryssfrågor och öppna svarsalternativ. Det finns även möjlighet att på varje fråga skriva ett alternativt svar, ifall valmöjligheterna inte tillräckligt beskriver enkätdeltagarens åsikt. Att använda sig av både kvantitativa frågor och kvalitativa frågor kallas för blandad form. Detta är ett bra alternativ då de kvantitativa och kvalitativa frågorna kompletterar varandra. Ett sådant upplägg kallas blandad metod enligt Jacobsen (2002).

Vi har valt att majoriteten av frågorna ska vara mestadels kvantitativa då de är lättare att förstå och det går snabbare för deltagarna att besvara. Antalet frågor valde vi att begränsa till 14 stycken då ett för stort antal frågor kan avskräcka deltagarna att genomföra hela undersökningen.

Vår enkät kommer att vara en webbaserad enkät genom Google Forms. Vi kommer även att dela ut den i pappersform och sedan sammanställa svaren med vår webbaserade enkät. Enkäten finns tillgänglig som bilaga.

3.5 Presentation av empiri

I analysen har vi valt att dela in de olika frågorna i grupper som behandlar samma område. Detta har vi gjort för att underlätta analysen, då frågorna är kopplade till varandra. Vi anser att detta ger bättre förutsättningar för en mer djupgående analys gällande de olika säkerhetsområdena inom informationssäkerhet.

För att underlätta analysen av data har vi använt oss av Excel och skapat cirkeldiagram för de olika frågorna. Vi har även delat upp så att vi fick ett diagram för konsulter och ett diagram för de fast anställda. Det underlättade när vi jämförde resultatet mellan dessa två grupper. På detta sätt ges även läsaren en tydligare överblick över vår statistik som presenteras.

Vi har valt cirkeldiagram som ger en tydlig bild som visar de olika procentsatserna vilket är det underlag som vi kommer att jämföra mellan de två olika grupperna.

Totalt har vi fått in svar från 20 fast anställda och 20 konsulter som samtliga jobbar inom företag som beskrivs ovan i rapporten.

3.6 Etik

Att ha anonymitet i en undersökning med många deltagare är inte svårt. Då det blir svårt att koppla ett specifikt svar till en specifik person. Det går att anonymisera undersökningsdeltagarna genom att inte samla in data som underlättar för identifikation (Jacobsen, 2002). Vi valde därför att inte samla in någon personlig data som till exempel kön, ålder och arbetsgivare.

Det är viktigt att deltagarna frivilligt deltar i undersökningen, samt att de är införstådda med var syftet med undersökningen är (Jacobsen, 2002). Vi informerade därför om syftet med vår uppsats samt vad insamlad data ska användas till i våra presentationsbrev. Dock är det inte säkert att personerna som har vidarebefordrat enkäten till sina kollegor har vidarebefordrat presentationsbrevet.

Informationen vi samlar in är inte känslig för deltagarnas privatliv. Den kan dock uppfattas som känslig ifall deltagarna vet att de agerar på ett sätt som strider mot företagets policy. Därför var det viktigt med anonymitet så att deltagarna inte känner att deras svar på undersökningen kan påverka deras arbete negativt, exempelvis genom att svaren identifieras av en chef.

3.7 Validitet och Reliabilitet

Vår undersökning är mestadels kvantitativ med möjlighet att ge öppna svar. I och med att den är kvantitativ är den även deduktiv och därför begränsas vilken information som samlas in eftersom vi har gett fasta svarsalternativ (Jacobsen, 2002). Det finns dock en fördel vilket är att all data som samlas in är relevant. Att vi begränsat vilken data vi samlar in kan medföra att vi råkar bortse från relevant data för vår undersökning (Jacobsen, 2002). Vi försökte att minska detta genom att även ge möjlighet att svara öppet på alla frågor i undersökningen.

För att säkerställa att vårt resultat från undersökningen är korrekt ställer vi två krav på empirin. Det första är att empirin ska vara tillförlitlig och trovärdig och det andra är att den ska vara giltig och relevant (Jacobsen 2002).

Genom att använda oss av vårt teoretiska ramverk säkerställer vi att den information vi samlar in är giltig. Alla frågor i vår undersökning är grundade i den teori som finns i ramverket. Vi har även använt oss av samma metod för all datainsamling för att öka tillförlitligheten (Jacobsen, 2002). För att minska feltolkningar i frågorna använde vi oss av hjälptexter som gav exempel på vad vi menar med frågan.

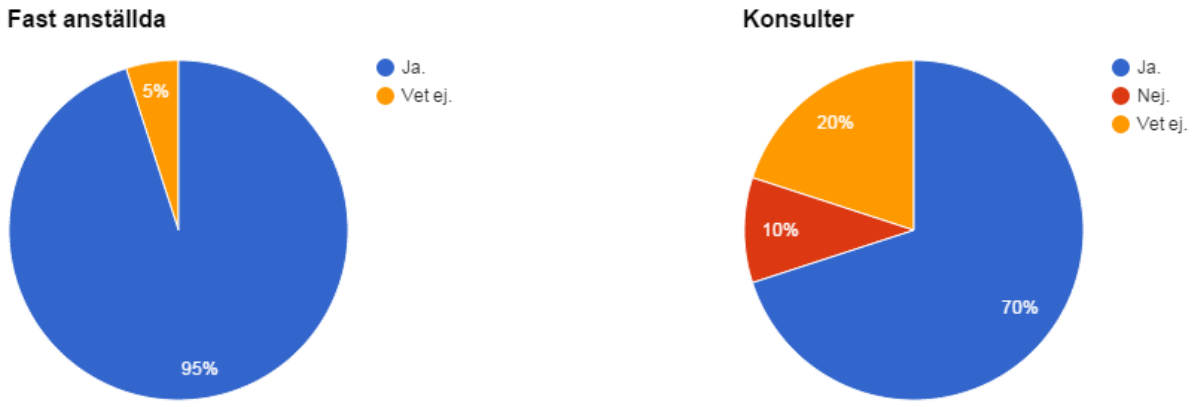
Vi har använt oss av presentationsbrev när vi skickade ut enkäterna till de personer som skulle vidarebefordra den till andra i företaget. Genom att göra detta har vi förklarat syftet med undersökningen för deltagarna. Vi informerade även deltagarna att undersökningen var helt anonym för både deltagare och företaget. Detta gjorde vi för att minska antalet som svarar vad de tror är rätt istället för hur de i själva verket agerar.

4 Resultat av empiri

Nedan redovisas vårt empiriska resultat, med korta kommentarer som främst tar upp skillnaden mellan konsulter och fast anställdas svar:

Fråga 1: Har företaget du jobbar för en säkerhetspolicy?

Hjälptext: Om du är uthyrd till ett företag är det företaget du är uthyrd till som vi syftar på.

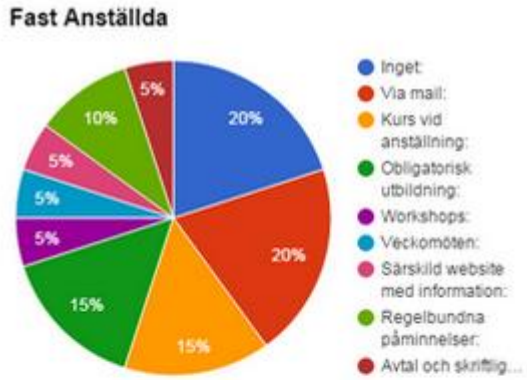


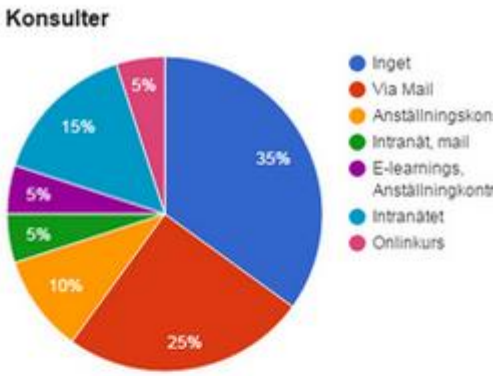
Figur 4.1: Cirkeldiagram fråga 1

Resultatet av frågan visar på att konsulterna är lägre medvetna om deras företag har en säkerhetspolicy. Det visade sig även att fler uppgav att deras företag inte hade en säkerhetspolicy överhuvudtaget.

Fråga 2: På vilket sätt gör företaget dig mer säkerhetsmedveten?

Resultaten på denna fråga väljer vi att presentera med förtydligade svar, då svarsalternativen var öppna för enkätdeltagarna.





Fast anställda

Inget:	4
Information via mail:	4
Kurs vid anställning:	3
Obligatorisk utbildning:	3
Workshops:	1
Veckomöten:	1
Särskild website med information:	1
Regelbundna påminnelser:	2
Avtal och skriftliga policies:	1

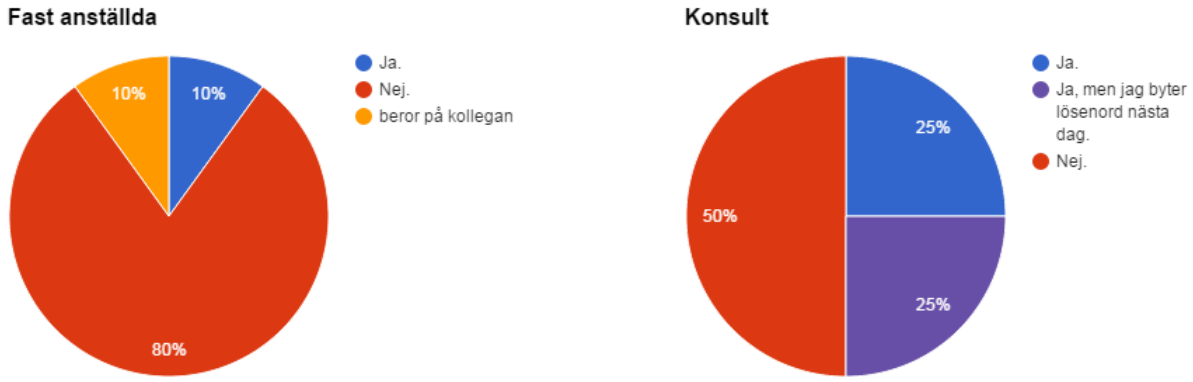
Konsulter

Inget	7
Via Mail	5
Anställningskontrakt intranät	2
Intranät, mail	1
E-learnings, Anställningkontrakt	1
Intranätet	3
Onlinkurs	1

Figur 4.2: Cirkeldiagram fråga 2

Resulten varierade en del mellan anställda och konsulterna. 20 % av de anställda uppgav att företaget inte gjort någon för att göra dom mer säkerhetsmedvetna, medan konsulterna uppgav 35 % samma sak. Vanligaste sättet att informera personalen var via mail, intranät och genom anställningskontrakt.

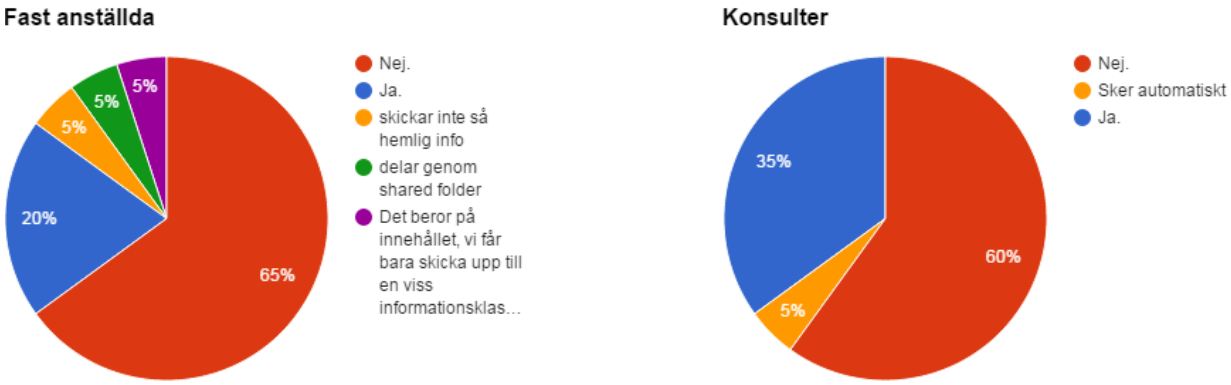
Fråga 3: Du är ledig från jobbet. En kollega ringer och ber om ditt lösenord eftersom de måste ha tillgång till data på ditt konto. Ger du din kollega ditt lösenord?



Figur 4.3: Cirkeldiagram fråga 3

Konsulterna var mer benägna att ge ut sitt lösenord till en kollega, där endast 50 % uppgav att de inte skulle ge ut sitt lösenord under några omständigheter. Hos de anställda var siffran 80 %.

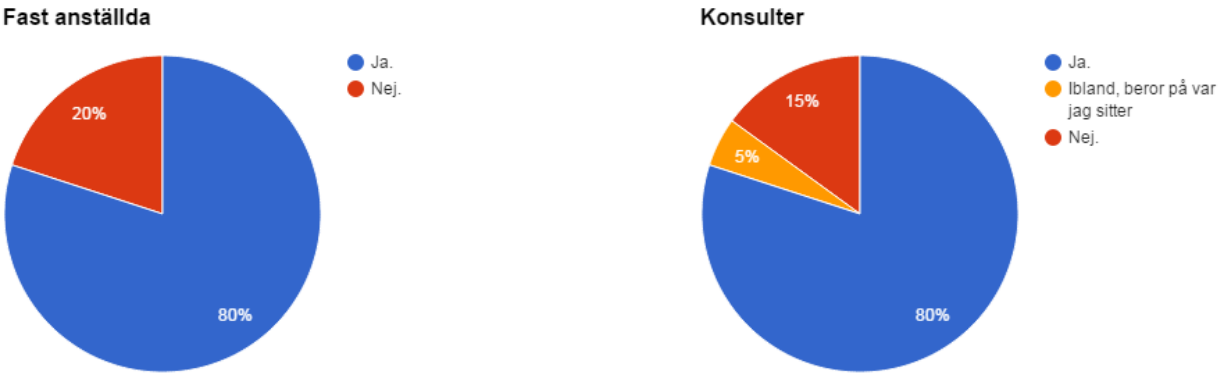
Fråga 4: Du behöver skicka ett mail med information till en extern part. Krypterar du mailets innehåll?



Figur 4.4: Cirkeldiagram fråga 4

Svaren på fråga 4 var relativt lika. 65 % av de fast anställda krypterade inte informationen, medan konsulternas siffra låg på 60 %. 35 % av konsulterna krypterade dock den externt utskickade informationen, men endast 20 % av de fast anställda. De fast anställda hade mer varierande svar med olika typer av tillägg i svaren, som visar på ett motsvarande säkerhetstänk i frågan.

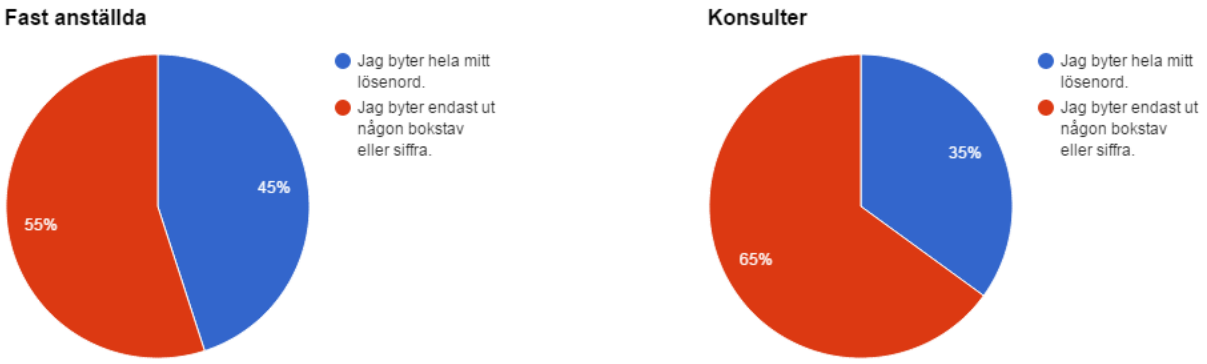
Fråga 5: Du sitter och arbetar och behöver gå ifrån datorn lite snabbt och hämta något. Låser du eller alternativt loggar ut från datorn?



Figur 4.5: Cirkeldiagram fråga 5

På denna punkt var svaren nästan identiska för konsulter och fast anställda. 80 % var noga med att låsa alternativt logga ut från datorn gällande båda grupperna.

Fråga 6: Du blir ombedd att byta lösenord av systemet, hur går du tillväga?



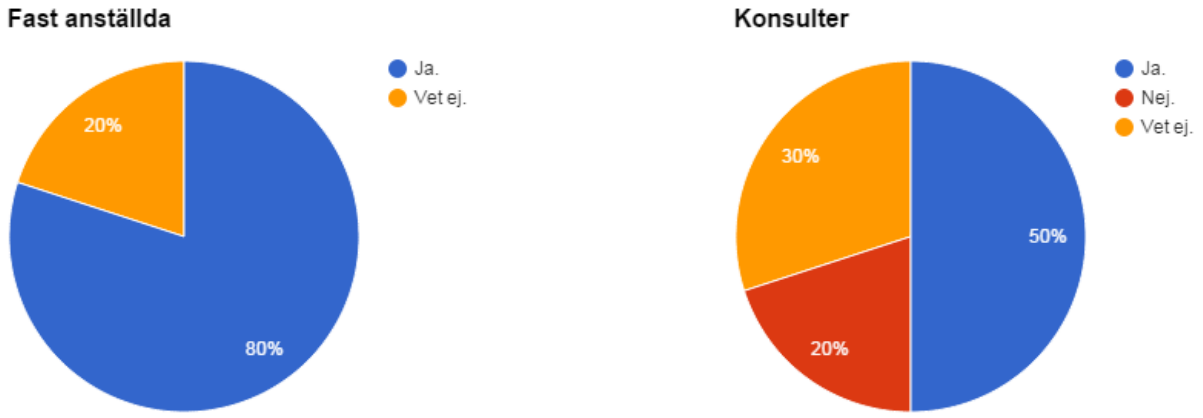
Figur 4.6: Cirkeldiagram fråga 6

Även på denna punkt visade det sig att konsulter och fast anställda agerar snarlikt. De fast anställda har en uppdelning på 55 % respektive 45 % huruvida de byter någon bokstav eller siffra eller om de byter hela lösenordet. Konsulternas uppdelning är 65 % respektive 35 %, vilket endast är marginellt sämre.

Fråga 7: Finns det tydligt uppsatta regler för arbete med data utanför företaget?

Exempelvis om du arbetar hemifrån.

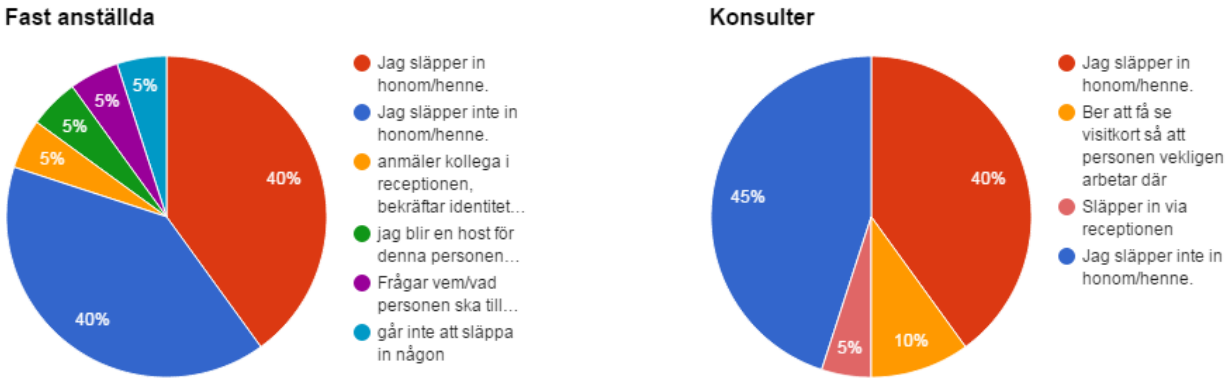
Figur 4.7: Cirkeldiagram fråga 7



Här var det en tydlig skillnad. Av de som var fast anställda visste 80 % att det fanns uppsatta regler för hur man får jobba med data utanför företaget jämfört med konsulternas 50 %. Värt att notera är även att 20 % av konsulterna har svarat nej på frågan och av de som är fast anställda har ingen svarat nej.

Fråga 8: Du är på väg in genom dörren. En kollega stannar dig och säger att han har glömt sitt passerkort. Hur agerar du?

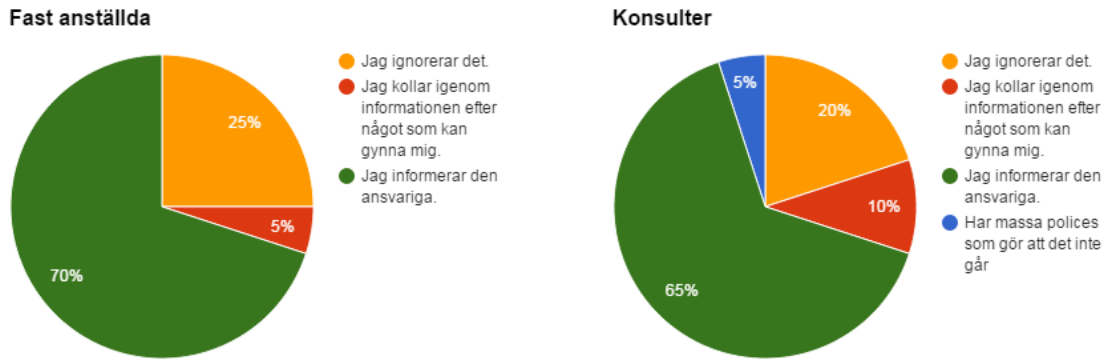
Du känner inte kollegan alternativt har du sett honom/henne någon gång innan.



Figur 4.8: Cirkeldiagram fråga 8

Under fråga 8 agerade konsulter och fast anställda i linje med varandra. 40 % för vardera grupp angav att de släppte in personen utan passerkort.

Fråga 9: Du får tillgång till data som är utanför dina behörigheter. Hur går du tillväga?

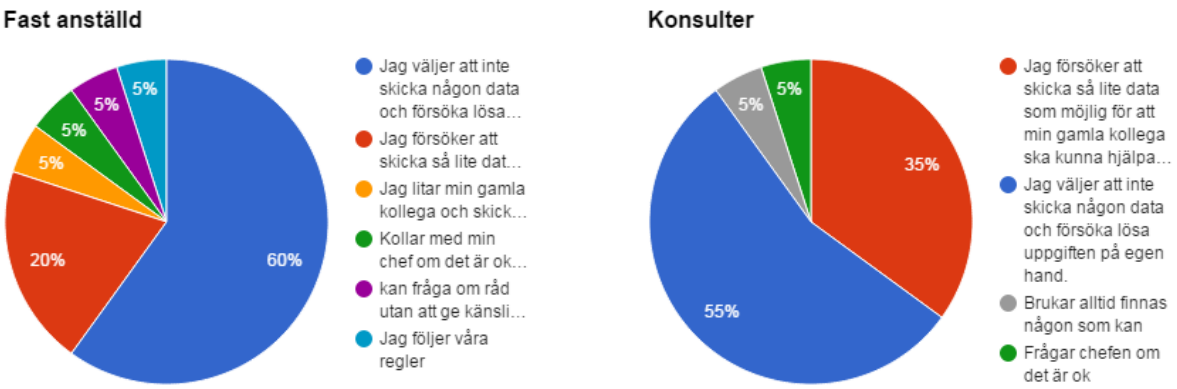


Figur 4.9: Cirkeldiagram fråga 9

Konsulter var någorlunda mer benägna att inte rapportera eller att utnyttja data som de egentligen inte skulle ha behörighet till. 20 % valde att ignorera informationen och inte vidta några åtgärder medan 10 % valde att genomsöka informationen efter något som kunde gynna dem. Endast 5 % av de anställda valde att kolla igenom innehållet.

Fråga 10: Du arbetar med en uppgift och behöver hjälp. Du har en kollega som slutat på din arbetsplats men som kan precis det du behöver hjälp med. Den data som du måste lämna ut är någorlunda känslig. Men du litar på din gamla kollega. Hur skulle du gå tillväga?

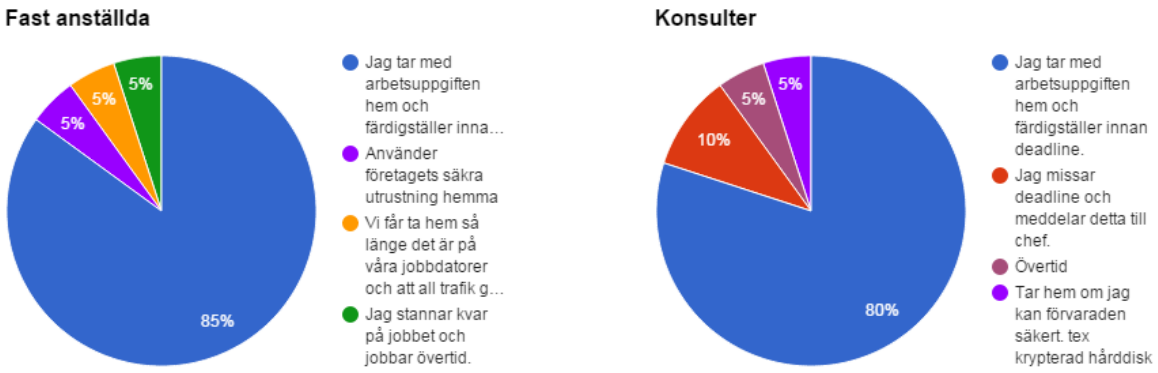
Du kommer inte att kunna göra ett lika bra jobb utan din kollegas hjälp. Och uppgiften ska visas upp för några chefer.



Figur 4.10: Cirkeldiagram fråga 10

Fråga 10 visade på likartade svar från de två intervjugrupperna. Här visade båda grupper att de var någorlunda noggranna med den känsliga data som de hanterade då 60 % av de fast anställda, respektive 55 % hos konsulterna valde att ej skicka information externt. De övriga svaren tyder också på att väldigt få av de tillfrågade var villiga att ge ut känslig information till extern part.

Fråga 11: Du jobbar med en arbetsuppgift som ska vara klar samma dag, detta kräver att du tar med känslig data hem för färdigställa uppgiften och därmed nå din deadline. Hur agerar du?

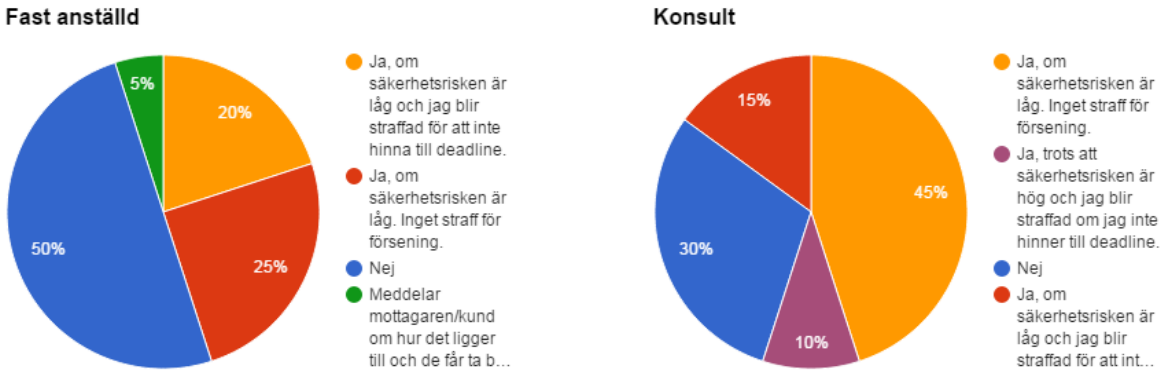


Figur 4.11: Cirkeldiagram fråga 11

Nästan lika många anställda som konsulter uppgav att de tog hem arbetet och färdigställde det. En del uppgav att de tog hem det ifall de kunde arbeta säkert. Det som skiljde sig var att några procent fler konsulter uppgav att de skulle missa deadline istället.

Fråga 12: Är du villig att ta genvägar för att nå en deadline?

Till exempel inte utföra tillräckligt med testning av produkten för att på så sätt hinna färdigt



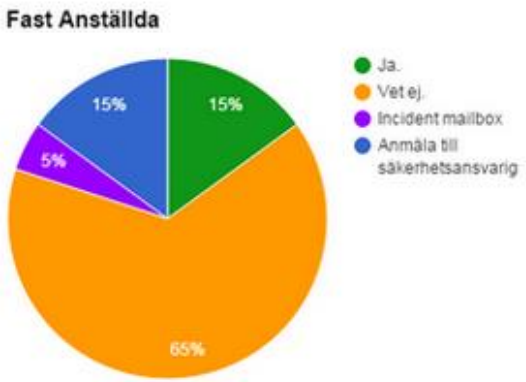
till deadline.

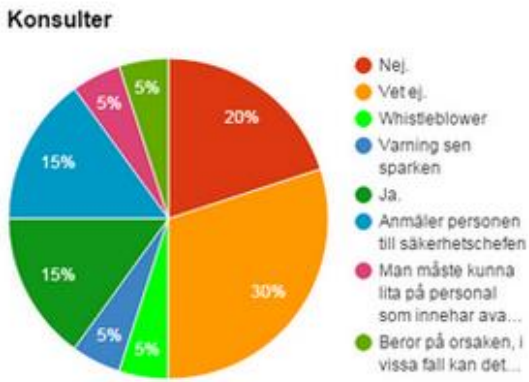
Figur 4.12: Cirkeldiagram fråga 12

Här var det ganska jämt fördelat men de fast anställda var mindre benägna att ta genvägar, 50 % kontra 30 %. 10 % av konsulterna svarade att de kunde ta genvägar trots att säkerhetsrisken var hög, det gjorde ingen av de fast anställda.

Fråga 13: Om någon medvetet utför handlingar som bryter mot säkerheten. Finns det några åtgärder för att förhindra/stoppa det? Om ja, specificera gärna vad i övrigt.

Kan vara vad för sorts tillrättavisning/staff man kan få.





Ja.	3
Nej.	0
Vet ej.	13
Incident mailbox	1
Anmäla till säkerhetsansvarig	3

Nej.	4
Vet ej.	6
Whistleblower	1
Varning sen sparken	1
Ja.	3
Anmäler personen till säkerhetschefen	3
Man måste kunna lita på personal som innehar avancerade tjänster, vilket gör rekrytering avgörande.	1
Beror på orsaken, i vissa fall kan det bero på att man inte inser vilka konsekvenser det kan få. Sådan kan avhjälpas med information. För den som gör det av likgiltighet, oaktsamhet eller för egen vinning finns ingen annan åtgärd än avsked.	1

Figur 4.13: Cirkeldiagram fråga 13

Resultatet från undersökningen pekar på att konsulterna hade bättre kunskap om vad det fanns för åtgärder för att stoppa någon som bryter mot säkerheten. 65 % av de fast anställda visste inte vad det fanns för åtgärder medan motsvarande siffra var 30 % hos konsulterna. Dock svarade även 20 % av konsulter att det inte fanns några åtgärder alls. De åtgärder som uppgavs var att det gick att anmäla den som bröt mot säkerheten till säkerhetsansvarig, eller att personen i fråga först fick en varning och sedan sparkades.

5 Analys och diskussion

Sammanställning av frågor:

5.1 Översikt av medvetenhet och policies

Frågor som är inkluderade under den här rubriken:

- Fråga 1: Har företaget du jobbar för en säkerhetspolicy?
- Fråga 2: På vilket sätt gör företaget dig mer säkerhetsmedveten?

Enligt Principal agent teorin (Garber et al., 2011) påverkar policies hur allvarliga genvägar en agent kan ta. Resultatet i undersökningen indikerar att konsulterna har mindre vetskap gällande huruvida företaget de jobbade för hade en säkerhetspolicy. Detta kan leda till att konsulternas agerande gör mer skada när det kommer till det dagliga arbetet, då exempelvis genvägar som tas kan öka risken för att känslig information äventyras.

I undersökningen av Ernst & Young (Ernst & Young, 2003) frågar de företag att ranka de tre områden som de lägger mest resurser på för att öka informationssäkerheten. Konsulter hamnar på plats fyra medan de anställda hamnar på plats fem. De svaren vi fick i vår undersökning påvisar en lägre medvetenhet hos konsulterna, samt att fler konsulter uppgav att företaget inte gör något för att öka deras säkerhetsmedvetenhet. Vilket indikerar att företagen lägger mindre resurser på konsulter än på de fast anställda.

När det kommer till hur ett företag på bästa sätt kan öka medvetenheten kring informationssäkerhet tar Albrechtsen & Hovden (2009) upp att interaktioner på arbetsplatsen med till exempel workshops är ett av de sätt att som ökar kunskapsnivån för de anställda bäst. Våra resultat visar att endast en av de totalt tillfrågade angett detta som alternativ. Detta kan tolkas som att det finns mycket att göra för samtliga inkluderade företag när det kommer till interaktiv utbildningen för sina anställda. Den utbildning och information som ges ut är ofta genom mail och intranätet, vilket kan vara bra då personalen alltid har tillgång till informationen (Hubbbard, 2002). Men vår teori och undersökning indikerar samtidigt att företagen borde har mer utbildning där konsulter och fast anställda interagerar med varandra. Detta för att få igång en diskussion där personalen måste tänka efter och fatta egna beslut. Genom att diskutera säkerheten och sitt eget agerande, kommer personalen att begrunda hur de själva handlar i dessa frågor. Sätten som företagen informerar sina anställda på är för ensidiga och simpla, och kommer kanske inte ge samma effekt som till exempel workshops eller diskussionsgrupper som även tas upp av Albrechtsen & Hovden (2009).

5.2 Lösenordskontroll

Frågor som är inkluderade under den här rubriken:

- Fråga 3: Du är ledig från jobbet. En kollega ringer och ber om ditt lösenord eftersom de måste ha tillgång till data på ditt konto. Ger du din kollega ditt lösenord?
- Fråga 6: Du blir ombedd att byta lösenord av systemet, hur går du tillväga?

Att ge ut sitt lösenord till en kollega kan vara en stor säkerhetsrisk då det ger kollegan tillgång till all ens data även om lösenordet byts nästa dag. Samt att de handlingar som begås blir svåra att koppla till rätt person, då företaget inte kan bevisa vem det var som använde kontot (Ferreira et al., 2013). Om lösenordet skickas genom mail, sms eller sociala medier finns det en risk att lösenordet fångas upp av någon obehörig som tas upp i punkt fem av de vanligaste säkerhetsriskerna (Wall, 2005). Enligt resultatet i vår undersökning var konsulterna mer benägna att dela med sig av sina lösenord till sina kollegor.

I vår undersökning var både de anställda och konsulterna ungefär lika dåliga på att byta sina lösenord. Enligt Hubbard (2002) kan de bero på att personalen inte har kunskapen om hur ett bra lösenord ska vara uppbyggt samt vikten att de ändrar till ett helt nytt lösenord. Om en anställds lösenord blir äventyrat och han endast ändrar en del av sitt lösenord, blir det betydligt enklare för obehöriga att lista ut det nya lösenordet. Om man dessutom gett ut sitt lösenord till en kollega som vi undersöker i *fråga 3* finns risken att denne får tillgång till kontot på obestämd tid. Även ifall personen ändrar lösenordet och endast byter en siffra eller bokstav som många av konsulterna gjort enligt *fråga 6*, blir det enklare att lista ut det nya lösenordet. Detta bidrar till att behörighetskontroller inom företagen kan äventyras då personal kan få information som är utanför deras behörighet, vilket tas upp som en säkerhetsrisk av Sandhu & Samarati (1994).

Enligt svaren utgör konsulterna en större risk än vad de fast anställda gör. Trots att båda grupperna är lika dåliga på att byta lösenord så anger en större del av konsulterna att de delar med sig av sina lösenord. Att fler konsulter delar med sig av sina lösenord borde åtgärdas med mer utbildningar som tar upp riskerna gällande delning av lösenord vilket tas upp i vår teori om interna hot (Stanton et al., 2004).

5.3 Säkerhet kring arbete i hemmet

Frågor som är inkluderade under den här rubriken:

- Fråga 7: Finns det tydligt uppsatta regler för arbete med data utanför företaget?
- Fråga 11: Du jobbar med en arbetsuppgift som ska vara klar samma dag, detta kräver att du tar med känslig data hem för att färdigställa uppgiften och därmed nå din deadline.

Fler konsulter än fast anställda uppgav att företaget inte hade tydligt uppsatta regler, eller att de inte visste ifall det fanns några regler. På *fråga 11* uppgav majoriteten att de tar med och färdigställer sina uppgifter hemma ifall de har problem med att nå en deadline. Att ta hem och arbeta med data utan att veta vad det finns för regelverk kring detta kan äventyra informationens säkerhet. Endast en person svarade att han/hon använde sig att VPN (Virtual Private Network) när han jobbade hemifrån. De anställda hade bättre vetskap angående reglerna men även hos dem tog majoriteten hem och färdigställde uppgiften. Det var dock färre av de fast anställda som uppgav att de inte visste om det fanns några regler överhuvudtaget. Enligt vår statistik har konsulterna sämre kunskap om vilka regler som gäller när det kommer till säkerheten i hemmet, och eftersom företagen inte lägger ner lika mycket resurser på utbildning kring säkerhetsmedvetenhet enligt svaren på *fråga 2***,** leder detta till att konsulterna överlag utgör en större säkerhetsrisk än de fast anställda.

Att konsulterna är villiga att ta hem data utan att det finns regler för hur det ska gå till, går att koppla till Principal agent teorin (Garber et al., 2011), som tar upp att agenter(konsulter) har större benägenhet att ta genvägar för att uppnå milstolpar. Vår statistik styrker detta resonemanget.

Företagen bör alltså vara tydligare med arbete med data utanför företagets lokaler, då många av konsulterna uppgav att de inte visste om det fanns några tydligt uppsatta regler för arbete med data i hemmet, men ändå tog hem data och arbetade med den.

5.4 Fysisk säkerhet

Frågor som är inkluderade under den här rubriken:

- Fråga 5: Du sitter och arbetar och behöver gå ifrån datorn lite snabbt och hämta något. Låser du alternativt loggar ut från datorn?
- Fråga 8: Du är på väg in genom dörren. En kollega stannar dig och säger att han har glömt sitt passerkort. Hur agerar du?

Både anställda och konsulter var bra på att låsa datorn ifall de skulle lämna den en kort stund. Att så stor del låser sin dator när de lämnar den kan bero på att det är en väldig enkel säkerhetsåtgärd. Det kräver ofta endast tre stycken knapptryck på tangentbordet så det är inte någon större ansträngning för personalen. Ifall fler av de tillfrågade inte hade låst sin dator kunde detta utgjort en stor säkerhetsrisk, då kollegor kunde fått tag i data från ens konto. Om många släpper in personer som uppger sig att vara deras kollega i *fråga 8* kan även obehöriga få tillgång till känslig data.

Resultatet på *fråga 8* gav inte ett helt övertygande svar, men de visar att skillnaden inte är stor mellan konsulter och de fast anställda. Då denna fråga kopplas till *Fråga 5* som gav svar på ifall man låser sin dator, visade våra resultat på att den typen av fysiska säkerhet upprätthölls

på ett tillfredsställande sätt av de flesta enkätdeltagarna. Samtidigt så är det 40 % av båda enkätgrupper som väljer alternativet att släppa in den obehöriga personen. Denna siffra är lite för hög och det krävs förbättring för båda grupperna gällande den fysiska säkerheten. Det finns en klar anledning till varför man ska använda sig av passerkort och på detta sätt inte låta utomstående få tillgång till kontoret. Om reglerna inte efterlevs av de anställda bidrar detta till att företagets policy blir onödig och verkningslös (Bishop, 2003).

5.5 Behörighetskontroll kopplad till Principal agent

Frågor som är inkluderade under den här rubriken:

- Fråga 9: Du får tillgång till data som är utanför dina behörigheter. Hur går du tillväga?
- Fråga 12: Är du villig att ta genvägar för att nå en deadline?

Svaren på *fråga 9* gav inte några större variationer från de två grupperna. Intervjugrupperna svarade väldigt lika vilket påvisar en mindre skillnad i detta avseende. Det mest intressanta som kan granskas kring detta resultat var att lite fler konsulter valde alternativet: "leta igenom informationen efter något som kunde gynna dem". Här var siffran lägre hos de fast anställda. Vi tror dock inte det har något att göra med huruvida en person jobbar som konsult eller fast anställd, utan hur personen i fråga har för värderingar. Majoriteten av enkätdeltagarna svarade att de skulle informera den ansvarige vilket tyder på en bra moral och lojalitet mot företaget. Den här frågan kan kopplas till rollbaserad säkerhetskontroll(Samarati, Capitani de Vimercati, 2001)(Sandhu, R.S., Samarati, P, 1994).

I *fråga 12* var svaren ganska jämna, men fast anställda var mindre benägna att ta genvägar för att uppnå resultat. Av de fast anställda svarade 50 % nej jämfört med konsulternas 40 %. I båda grupperna svarade 20 % att de skulle ta en genväg om säkerhetsrisken var låg och de blev straffade om de inte hann till deadline. Mest anmärkningsvärt att notera är att 10 % av konsulterna kunde tänka sig att ta en genväg trots att säkerhetsrisken är hög. Hur dessa skiljer sig beror troligtvis på vilka företag de har arbetat på och vilken kultur dessa företag har. Ett företag kan sätta stor press på sina konsulter/anställda att hinna deadline och det ökar risken att de tar genvägar. Den här frågan kan kopplas till principal agent teorin (Garber et al., 2011)

5.6 Delning av information till 3:e part och extern kommunikation

Frågor som är inkluderade under den här rubriken:

- Fråga 4: Du behöver skicka ett mail med information till en extern part. Krypterar du mailets innehåll?
- Fråga 10: Du arbetar med en uppgift och behöver hjälp. Du har en kollega som slutat på din arbetsplats men som kan precis det du behöver hjälp med. Det data som du

måste lämna ut är någorlunda känslig. Men du litar på din gamla kollega. Hur skulle du gå tillväga?

Att fler än hälften av både de anställda och konsulter inte krypterar data som skickas externt, innebär att obehöriga kan få tag i data genom att gå igenom andra företag/privat personer, som kanske inte har lika hög säkerhet som det egna företaget. I vilket fall blir informationen mindre säker då den skickas utan kryptering. Denna typ av risk tas upp i teorin om vanligt förekommande säkerhetsrisker (Wall, 2013). Några få uppgav att det sker automatisk och vissa uppgav att de inte skickar så viktig information att det behövs. Det kan även vara så att de anställda inte tycker att den data de skickar är av större värde. Eftersom det även kan vara svårt att värdera den information som skickas ut (Cavusoglu, 2004), bidrar detta till en större oaktsamhet inför den externa kommunikationen.

När det kommer till jämförelsen mellan de fast anställda och konsulterna var skillnaden inte stor i svaren. Det går därför inte att dra någon slutsats att konsulterna skulle vara sämre inom detta område.

För fråga 10 var enkätdeltagarnas svar tillfredställande gällande säkerheten. Både konsulterna och de fast anställda var noga med att kontrollera att de inte ger ut känslig information.

5.7 Åtgärder för kontroll av säkerhet

Frågor som är inkluderade under den här rubriken:

- Fråga 13: Om någon medvetet utför handlingar som bryter mot säkerheten. Finns det några åtgärder för att förhindra/stoppa det? Om ja, specificera gärna vad i övrigt.

Det är viktigt att de anställda vet vad det finns för åtgärder för att stoppa samt förhindra att någon bryter mot säkerheten. Detta för att de ska veta vad de själva kan göra åt det ifall de vet att någon anställd bryter mot säkerheten och vilka åtgärder som finns för säkerhetsbrott. Men om personalen inte vet vad som står i policyn spelar det ingen roll hur bra åtgärder det finns (Hubbard, 2002). Att motverka säkerhetsbrott går att göra genom dataövervakning. Det är viktigt att de anställda vet om att de blir övervakade så att de är medvetna att de säkerhetsbrott de begår kommer att bli upptäckta. Samt att de vet vilka straff som gäller för de olika brotten (D'Arcy et al., 2009).

Företagen i vår undersökning bör utbilda sina anställda bättre när det kommer till åtgärder de kan ta ifall personalen bryter mot säkerheten. I vår undersökning var resultatet överraskande då konsulterna hade bättre kännedom än vad de fast anställda hade i *fråga 13.* Konsulternas kunskap var heller inte övertygande, detta är därför en punkt där företagen har misslyckats med att informera sin personal tydligt om vad som gäller.

5.8 Utbildning av personal

Många i vår undersökning uppger att företagen inte gör någon för att öka deras säkerhetsmedvetenhet. Sätten som företagen väljer att informera sin personal på verkar även mestadels ske genom informationsutskick via intranät eller mail, alternativt skriva under ett avtal vid anställning. Det var få svar som visade på att företagen hade ett informationssätt som var interaktivt inom personalen och där de var tvingade att delta i undervisningen. För att minska de klyftor som finns mellan konsulter och anställda anser vi företagen bör öka resurser för utbildning. Vi anser även att företagen bör utbilda sin personal mer genom interaktiva metoder som tvingar personalen att interagera med varandra till exempel diskussionsgrupper och workshops. Workshops är det sättet som har störst effekt på personalen (Albrechtsen, 2009). Företagen väljer att lägga mer resurser på teknik istället för att utbilda personalen (D'Arcy et al., 2009),(ERNST & YOUNG, 2003). De brister vi har tagit fram i vår undersökning är inget som teknik kommer att hjälpa emot, det krävs utbildning i form av ett SETA eller ISA program. Det hjälper inte att skydda informationen mot utomstående när bristerna uppstår inne i företaget av den egna personalen (Wall, 2013).

5.9 Allmänt

Vår undersökning pekar på att det finns en poäng i principal-agent teorin. Konsulterna var mer benägna att ta genvägar för att nå sina mål. De var även mer benägna att ta högre risker för att nå dem. Vi tolkar siffrorna i undersökningen som att benägenheten att ta genvägar kan bero på att konsulterna inte vet vad som står i policyns och vilka regler som finns. Då de inte är medvetna om vilka konsekvenser deras handlingar innebär för företaget. De är heller inte medvetna vad för konsekvenser det innebär för dom själva eftersom detta ofta är information som finns i policyn och andra uppsatta regler.

För att minska risktagandet i företaget kan företagen införa klart definierade åtgärder för olika regelbrott samt öka dataövervakningen i företaget som beskrivs i kapitlet ”Öka informationssäkerhetsmedvetenhet”. Genom att personalen är medveten om att deras handlingar bevakas och att regelbrott troligen upptäcks, samt att de är medvetna om vilka åtgärder som kommer ske ifall de blir uppräcka, minskar deras benägenhet att ta risker.

6 Slutsats

Vår studie påvisar skillnader mellan konsulter och fast anställda när det kommer till Information Security Awareness. Resultaten visar även att finns mycket att göra gällande ISA för båda grupperna inom IT-branschen. På en del frågor har konsulternas svar visat sig vara i linje med de fast anställdas, medan de i andra svar visat på en betydligt sämre medvetenhet. Totalt sätt har konsulternas svar gett en bild av en lägre uppfattning om hur säkerhetskontrollen ska fungera inom sitt företag.

De punkter som skiljer sig mest i konsulter och fast anställdas säkerhetsmedvetenhet är att konsulter har sämre kunskap om policies och regler. Att konsulter inte vet vilka policies som gäller kan skapa stora problem i säkerheten. När de inte vet vad som gäller i olika säkerhetsfrågor kan de inte vara säkra på att de agerar rätt.

Det var även stor skillnad kring kännedomen angående regler för arbete med data i hemmet. Konsulterna hade sämre uppfattning gällande detta, vilket indikerar att företagen har informerat undermåligt om vilka regler som gäller. Det är återigen utbildningen av konsulterna som brister.

Hälften av konsulterna uppgav att företagen inte gör något för att öka deras säkerhetsmedvetenhet. Den andra hälften uppgav att företagen mestadels ökade deras säkerhetsmedvetenhet genom att skicka ut mail, lägga upp information på intranät eller att skriva under avtal vid anställningstillfället. Ingen av konsulterna uppgav att företagen använde sig av interaktiva utbildningssätt som till exempel workshops, och endast en av de fast anställda angav detta som svar. Eftersom detta tas upp som en av de mest effektiva utbildningssätt enligt Albrechtsen & Hovden (2009), är detta en angelägenhet som samtliga inkluderade företag bör beakta när det kommer till att förbättra sina anställdas medvetenhet kring informationssäkerhet.

B1. Presentationsbrev

Hej!

Vi är tre studenter som läser Systemvetenskapligt kandidatprogram på Lunds universitet. Vår C-uppsats handlar om konsulter kontra anställda på företag och hur deras information security awareness skiljer sig. Vi vill gärna få kontakt med någon som har hand om informationssäkerhet på ert företag.

Vi undrar om vi skulle få ställa några frågor till er i form av en enkät. Enkäten tar inte mer än ett par minuter och är helt anonym. Vi gör en kvantitativ undersökning och det skulle vara mycket uppskattat om du kunde skicka vidare enkäten till personer på din avdelning. Nedan är länken till undersökningen:

https://docs.google.com/forms/d/1MGQni1yU2ANG4E9OF-MTP7ZbTOxmHpvqQrEloMCs881g/viewform

Mvh Filip Alpteg, Martin Sonesson och Gustav Malm

B2. Enkätformulär

Undersökning av säkerhetsmedvetenhet

Vad arbetar du som?

Om du är fast anställd på ett företag men är uthyrd som konsult till ett annat företag räknas du som konsult.

- Konsult.
- Fast anställd.
- Övrigt:

Har företaget du jobbar för en säkerhetspolicy?

Om du är uthyrd till ett företag är det företaget du är uthyrd till som vi syftar på.

- Ja.
- Nej.
- Vet ej.
- Övrigt:

På vilket sätt gör företaget dig mer säkerhetsmedveten?

Ett exempel på detta kan vara workshops om informationssäkerhet.

Du är ledig från jobbet. En kollega ringer och ber om ditt lösenord eftersom de måste ha tillgång till data på ditt konto. Ger du din kollega ditt lösenord?

- Ja.
- Nej.
- Ja, men jag byter lösenord nästa dag.
- Övrigt:

Du behöver skicka ett mail med information till en extern part. Krypterar du mailets innehåll?

- Ja.
- Nej.
- Övrigt:

Du sitter och arbetar och behöver gå ifrån datorn lite snabbt och hämta något. Låser du alternativt loggar ut från datorn?

Du kommer max vara borta från datorn i 1-2 minuter

- Ja.
- Nej.
- Övrigt:

Du blir ombedd att byta lösenord av systemet, hur går du tillväga?

- Jag byter hela mitt lösenord.
- Jag byter endast ut någon bokstav eller siffra.
- Jag använder något av mina gamla lösenord.
- Övrigt:

Finns det tydligt uppsatta regler för arbete med data utanför företaget?

Exempel om du arbetar hemifrån.

- Ja.
- Nej.
- Vet ej.
- Övrigt:

Du är på väg in genom dörren. En kollega stannar dig och säger att han har glömt sitt passerkort. Hur agerar du?

Du känner inte kollegan alternativt har du sett honom/henne någon gång innan.

- Jag släpper inte in honom/henne.
- Jag släpper in honom/henne.
- Övrigt:

Du får tillgång till data som är utanför dina behörigheter. Hur går du tillväga?

- Jag informerar den ansvariga.
- Jag ignorerar det.
- Jag kollar igenom informationen efter något som kan gynna mig.
- Övrigt:

Du arbetar med en uppgift och behöver hjälp. Du har en kollega som slutat på din arbetsplats men som kan precis det du behöver hjälp med. Den data som du måste lämna ut är någorlunda känslig. Men du litar på din gamla kollega. Hur skulle du gå tillväga?

Du kommer inte att kunna göra ett lika bra jobb utan din kollegas hjälp. Och uppgiften ska visas upp för några chefer.

- Jag litar min gamla kollega och skickar datan för att kunna slutföra min uppgift.
- Jag väljer att inte skicka någon data och försöka lösa uppgiften på egen hand.
- Jag försöker att skicka så lite data som möjlig för att min gamla kollega ska kunna hjälpa mig.
- Övrigt:

Du jobbar med en arbetsuppgift som ska vara klar samma dag, detta kräver att du tar med känslig data hem för färdigställa uppgiften och därmed nå din deadline. Hur agerar du?

- Jag tar med arbetsuppgiften hem och färdigställer innan deadline.
- Jag missar deadline och meddelar detta till chef.
- Övrigt:

Är du villig att ta genvägar för att nå en deadline?

Till exempel inte utföra tillräckligt med testning av produkten för att på så sätt hinna färdigt till deadline.

- Ja, om säkerhetsrisken är låg och jag blir straffad för att inte hinna till deadline.
- Ja, trots att säkerhetsrisken är hög och jag blir straffad om jag inte hinner till deadline.
- Ja, om säkerhetsrisken är låg. Inget straff för försening.
- Ja, trots att säkerhetsrisken är hög. Inget straff för försening.
- Nej
- Övrigt:

Om någon medvetet utför handlingar som bryter mot säkerheten. Finns det några åtgärder för att förhindra/stoppa det? Om ja, specificera gärna vad i övrigt. Kan vara vad för sorts tillrättavisning/straff man kan få.

- Ja.
- Nej.
- Vet ej.
- Övrigt:

Referenser

Albrechtsen, E., & Hovden, J. (2009). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. [Elektronisk version]. *Computer and security*, 29, 432–445.

Bishop, M. (2003). What is computer security?. [Elektronisk version]. Security & Privacy, *IEEE*, 1(1), 67-69.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. [Elektronisk version]. *MIS Quarterly*, 34, 523-548.

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2004). Economics of ITSecurity Management: Four Improvements to Current Security Practices. [Elektronisk version]. *The Communications of the Association for Information Systems*, 14, 65-68.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. [Elektronisk version]. *Information Systems Research*, 20, 79-81.

Ernst & Young. (2003). *Global Information Security Survey, 1-6.* [Elektronisk]. Tillgänglig: *http://www2.eycom.ch/publications/_catalog/de.aspx?xp=%7Bhttp%3A%2F%2Fwww2.eycom.ch%2Flibrary%7D%3Aarticle%5B%7Bhttp%3A%2F%2Fwww2.eycom.ch%2Flibrary%7D%3Aperiodical%3D%27giss%27%5D&hr=Periodikum+Global+Information+Security+Survey* [2015-04-15]

Ferreira, A., Correia, R., Chadwick, D., Santos, H. M., Gomes, R., Reis, D., & Antunes, L. (2013). Password sharing and how to reduce it. [Elektronisk version]. *IT Policy and Ethics: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications*, 22, 22-32

Garber, R., & Paté-Cornell, E. (2012). Shortcuts in Complex Engineering Systems: A Principal-Agent Approach to Risk Management. *Risk Analysis*, 32(5), 836-854.

Holmstrom, B., & Milgrom, P. (1991). Multitask principal-agent analyses: Incentive contracts, asset ownership, and job design. [Elektronisk version]. *Journal of Law, Economics, & Organization*, 24-52.

Hubbard W. (2002). Methods and Techniques of Implementing a Security Awareness Program. [Elektronisk version]. *SANS Institute InfoSec Reading Room, 1-3*

Jacobsen, D. I. (2002). *Vad hur och Varför?*

Kruger, H. A., Drevin, L., & Steyn, T. (2006). A Framework for Evaluating ICT Security Awareness. [Elektronisk version]. *ISSA*, 1-11.

Kruger, H. A., & Kearney, *W. D.* (2005). Measuring information security awareness. [Elektronisk version]. *ISSA*, 1-10

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. [Elektronisk version]. *Computers & Security*, 24(2), 125-132.

Peltier, T. R. (2005). *Information security risk analysis 2nd ed*. [Elektronisk version]. CRC press, 24-30

Pfleeger, C. P., & Pfleeger, S. L. (2002). *Security in computing*. [Elektronisk version] Prentice Hall Professional Technical Reference. 498-520

Samarati, P., & de Vimercati, S. C. (2001). Access control: Policies, models, and mechanisms. In *Foundations of Security Analysis and Design*. [Elektronisk version]. Springer Berlin Heidelberg, 37-196

Sandhu, R. S., & Samarati, P. (1994). Access control: principle and practice. Communications Magazine. [Elektronisk version] *IEEE,* 32(9), 40-48.

Thomson, M. E., & von Solms, R. (1998). Information security awareness: educating your users effectively. [Elektronisk version]. *Information management & computer security*, 6, 167-173.

Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. [Elektronisk version]. *Security Journal*, 26(2), 107-116.

Whitman, M. E. (2003). Enemy at the gate: threats to information security. [Elektronisk version]. *Communications of the ACM*, *46*(8), 91-95.

IT-statistik (2015). *IT-branschens anställda.* [Elektronisk]. Tillgänglig: http://www.itstatistik.se/jamfor/anstallda/ [2015-05-18]