
LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

# Hackning utan knackning

## En studie om medvetenhet kring Social Engineering

Kandidatuppsats 15 hp, kurs SYSK02 i informationssystem

Författare: Jesper Brumark
Ludvig Ohlsson

Handledare: Mirella Muhic

Examinatorer: Anders Svensson
Umberto Fiaccadori

# Hackning utan knackning: En studie om medvetandet kring Social Engineering

Författare: Jesper Brumark och Ludvig Ohlsson

Utgivare: Inst. för informatik, Ekonomihögskolan, Lund universitet

Dokumenttyp: Kandidatuppsats

Antal sidor: 159

Nyckelord: Social Engineering (SE), Interpersonal Deception Theory (IDT), Medvetenhet, Theory of Planned Behaviour (TPB), Information Security Policy Awareness (ISPA)

Sammanfattning (Max. 200 ord):

Social Engineering (SE) ses som ett stort hot mot organisationers IT-säkerhet. SE är en typ av icke-teknisk hackning som används för att manipulera individer att avslöja konfidentiell information eller utföra handlingar som äventyrar person- eller organisationssäkerhet. En organisation kan således inte skydda sig mot SE med enbart fysiska och tekniska skydd eftersom det är användaren som redan är inne bakom fysiska lås och brandväggar som lättast kan orsaka skada. Denna uppsats undersöker IT-säkerhetsmedvetenheten, med fokus på SE, hos anställda inom IT-avdelningar respektive övriga avdelningar. Uppsatsen använder en kvalitativ metodansats med semi-strukturerade intervjuer för insamling av empiriska data. Den teori som tagits fram bygger främst på Interpersonal Deception Theory och Theory of Planned Behaviour och kopplas till anställdas medvetenhet. Resultaten visar på att anställda inom IT-avdelningarna har en högre grad av medvetenhet jämfört med anställda inom övriga avdelningar. Utifrån litteraturstudien diskuteras varför medvetenheten ser ut som den gör baserat på faktorer som deception, attityd, upplevd kontroll och subjektiv norm och vad organisationerna bör göra för att förbättra den. Slutligen ges förslag på vidare forskning denna studie kan leda till.

.

# Innehåll

# Figurer

# Tabeller

## Förkortningar

Social Engineering (SE)

Interpersonal Deception Theory (IDT)

Information Security Policy (ISP)

Information Security Awareness (ISA)

Information Security Policy Awareness (ISPA)

Theory of Planned Behaviour (TPB)

## Begrepp och dess användning i denna uppsats

**Access** - *Tillgång till system eller områden (Ivaturi & Janczewski, 2011).*

**Cyberattack** - *Ett kriminellt försök att skada, förstöra eller infiltrera ett datorsystem eller datorn i sig (Symantec, 2016).*

**Deception** - *En samlingsterm för att manipulera, missleda, bedra och ljuga för egen vinning (Hauser, 2016; Moffitt, 2009)*

**Face-to-Face** - *En intervjuform där intervjun sker ansikte mot ansikte.*

**Malware** - *Skadlig programvara (Flores & Ekstedt, 2013).*

**Medvetenhet –** *Medvetenhet för denna uppsats är definierat som en persons samlade erfarenheter, kunskaper och uppfattning om IT och informationssäkerhet* (Bulgurcu et al. 2010).

**Spoofad** - *Att dölja eller manipulera IP-adress, mailadress eller telefonnummer (Ivaturi & Janczewski, 2011).*

**Spear-Phishing** - En attack där meddelandet, ofta ett epostmeddelande, anpassas och konstrueras efter mottagaren (Ivaturi & Janczewski, 2011).

# 1 Introduktion

*I introduktionskapitlet ges bakgrunden till uppsatsens ämne. Vidare ges en problemformulering som mynnar ut i en frågeställning. Slutligen presenteras uppsatsen syfte och avgränsningar.*

## 1.1 Bakgrund

Alla organisationer är idag beroende av informationssystem. Det är i informationssystemen organisationen lagrar information och driver sitt arbete. Eftersom organisationer är så beroende av informationssystem är det viktigt hålla system och dess information skyddad. (Bulgurcu et al. 2010). Dock är IT-säkerhet ett kritiskt problemområde för organisationer över hela världen. Under år 2015 stals eller förlorades över en halv miljard personregister och Spear-Phishing attacker riktade mot anställda ökade med 55%. (Symantec, 2016). Cyberbrott kostar världsekonomin upp till 575 miljarder dollar årligen enligt BofA Merrill Lynch Global Research (Nahal et al., 2015), som vidare säger att i värsta fall står vi inför en '*Cybergeddon*' år 2020, vilket innebär att cyberbrott skulle ta upp en femtedel av allt värde som genereras online. En del av denna kostnad utgörs av rent tekniska cyberattacker och systemfalleringar, men den största orsaken till att informationssäkerhetsincidenter sker är på grund av den mänskliga faktorn. (Kranz & Haeussinger, 2014; Hauser, 2016; Bulgurcu et al. 2010; Ivaturi et al. 2014; Workman, 2008; Algarni et al. 2015).

Social engineering (SE) är den typ av icke-teknisk hackning som används för att manipulera individer att avslöja konfidentiell information eller utföra handlingar som äventyrar organisationssäkerhet (Hauser, 2016; Ivaturi & Janczewski, 2012; Algarni et al. 2015). Förövare inom SE kombinerar inflytande, övertalningsteknik och lögner för att övertyga en anställd att ge ut information (Hauser, 2016). Att manipulera människor är oftast det lättaste, billigaste och mest effektiva sättet för att infiltrera organisationer och dess informationssystem (Hauser, 2016). Organisationer kan således inte enbart förlita sig på tekniska lösningar, såsom brandväggar och antivirusprogram eftersom SE kringgår sådana skydd.

Människan har alltid använt sig av SE-tekniker för att manipulera andra människor, långt innan det fanns datorer och brandväggar. SE är således inget nytt fenomen utan är något som ligger i människans natur (Algarni et al. 2014). Det kanske mest välkända och äldsta exemplet är myten om det trojanska kriget som utspelade sig mellan grekerna och trojanerna. Efter nio års belägring hade grekerna inte lyckats slå sig igenom Trojas murar. Grekerna bytte därför taktik och byggde en stor, ihålig trähäst som de ställde fram framför Trojas port innan de gömde flottan en bit därifrån. En grekisk spion, som låtsades vara en kvarlämnad slav, talade om för trojanerna att hästen byggts som en gåva åt gudarna och lämnats kvar i hopp om att trojanerna skulle ådra deras ilska. Trojanerna drog in "gåvan" innanför murarna och under natten hoppade de gömda krigarna ut ur hästen och öppnade stadsportarna. Grekerna lyckades ta sig igenom trojas murar utan större ansträngning, allt tack vare SE. Det talar för att människor sedan länge förstått att människor är den svagaste länken i ett försvar och vilken stor effekt SE kan få.

Ett modernare exempel, som visar på hur sårbara dagens organisationer är mot SE, är TV4:s granskning av nio statliga myndigheter. Samtliga myndigheter behandlar viktig, känslig och ofta hemlig information om svenska medborgare. Under granskningen besökte en reporter myndigheterna och bad om att få skriva ut sitt CV som låg på ett medtaget USB-minne. USB-minnet var ofarligt men hade kunnat innehålla malware som resulterat i dataintrång. Utav nio myndigheter stoppade Ekobrottsmyndigheten, Inspektionen för vård och omsorg samt Datainspektionen in USB-minnet i organisationens datorer för att hjälpa reportern. (TV4, 2016) Det är alarmerande att datainspektionen, som bland annat ansvarar för att skydda medborgarnas digitala integritet, utan större ansträngning blev infiltrerade av en SE-attack. Om inte datainspektionen har ett fullt skydd finns det risk att andra organisationer inte heller har det.

## 1.2 Problemområde

Människan är det säkerhetshål som är svårast för organisationer att täppa igen, vilket utövare av SE utnyttjar (Ivaturi & Janczewski, 2011). En organisation kan inte skydda sig mot SE med enbart fysiska och tekniska skydd eftersom det är användaren som redan är inne bakom fysiska lås och brandväggar som lättast kan orsaka skada. Trots att SE är det vanligaste och lättaste sättet att hacka en organisation läggs störst resurser på tekniska säkerhetslösningar (Warkentin & Willison, 2009).

En annan anledning till att organisationer är så pass sårbara mot SE-attacker kan vara att IT-relaterade frågor enbart hanteras av IT-avdelningen. I dagens digitaliserade samhälle genomsyrar IT hela organisationen från toppen till botten (Gilbert, 2009) vilket också tyder på att IT-frågor inte endast ska vara centraliserade till en avdelning. Istället borde alla avdelningar ta del av IT-utbildning för att få en bredare förståelse för IT och dess risker. Då SE-förövare angriper den svagaste länken in i systemet sker attacken inte genom IT-avdelningen, utan riktar in sig på övriga avdelningar med lägre medvetenhet (Hauser, 2016; Bulgurcu et al. 2010;)

Organisationer utformar riktlinjer, eller policys, som ämnar ändra anställdas arbetssätt för att arbeta i linje med organisationens värderingar, mål och kultur (Gollmann, 2011). Dessa riktlinjer kan även utformas för att delvis skydda sig mot SE men då är det också vitalt att dessa policys efterföljs av de anställda och att organisationer lägger resurser på uppföljning och utbildning (Durgin, 2007). Dock kan en organisation aldrig vara helt skyddad mot den mänskliga faktorn, men utbildning och medvetenhet ger de främsta förutsättningarna för att identifiera och skydda sig mot SE och andra IT-relaterade hot (Bulgurcu et al. 2010).

Sammanfattningsvis finns det mycket som tyder på att organisationer saknar tillräckligt med skydd mot SE och att det inte investeras tillräckligt med resurser i att informera och utbilda anställda. Trots den klara hotbilden som finns verkar organisationer inte ha förstått hur sårbara de egentligen är, vilket skulle kunna vara en konsekvens av låg medvetenhet inom IT och SE. Medvetenhet hos anställda tycks således vara en vital del i organisationers skydd emot SE och bör vara lika hög inom alla avdelningar.

## 1.3 Frågeställning

Hur ser IT-säkerhetsmedvetenheten, med fokus på social engineering, ut på IT-avdelningar respektive övriga avdelningar inom medelstora / stora organisationer?

## 1.4 Syfte

Syftet för denna uppsats är att identifiera skillnader och likheter mellan avdelningars medvetenhet om IT-säkerhet ur ett SE-perspektiv. Detta sker med fokus på IT-avdelningar och övriga avdelningar. Vi ämnar även att beröra socialpsykologiska aspekter som kan påverka anställdas agerande i IT-säkerhetsfrågor.

## 1.5 Avgränsningar

Uppsatsen berör enbart policys och medvetenhet med koppling till de SE-attacker som berörs under kapitel 2.1. Uppsatsen tar således inte upp policys eller medvetenhet som berör andra typer av SE-tekniker eller IT-säkerhet.

Vi undersöker organisationer med fler än 60 anställda eftersom större organisationer ofta har större omsättning och således en större hotbild.

Vi undersöker inte alla avdelningar utan intervjuar enbart personal inom IT, HR, Ekonomi, Kommunikation och Logistik. Samtliga respondenter har ansvarsområden som innebär att de har behörighet att orsaka stor skada för organisationen. Vi har därmed ej fokuserat på anställda lägst ner i organisationshierarkin.

Vi granskar inte respondenternas individuella faktorer som kulturell bakgrund, kön, ålder eller liknande, utan fokuserar på vilken avdelning hen tillhör.

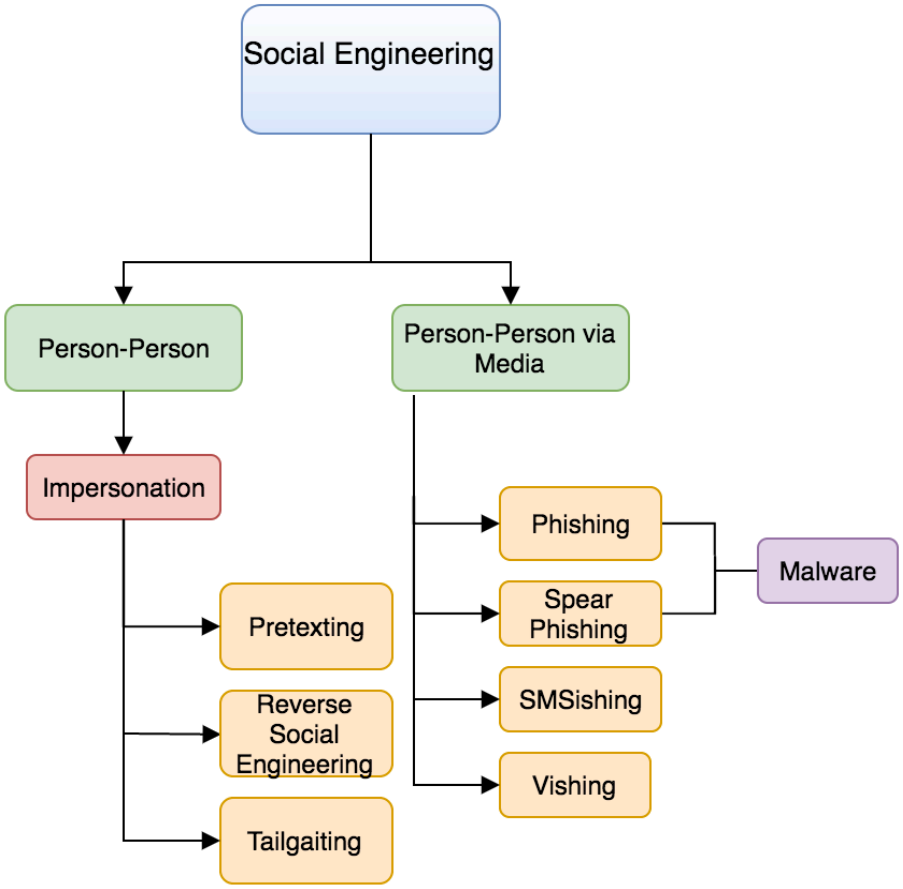
# 2 Litteraturstudie

*I litteraturstudien presenteras litteratur som är relevant för den här uppsatsens syfte och frågeställning.*

## 2.1 Social Engineering (SE)

SE är en typ av icke-teknisk hackning som används för att manipulera individer att avslöja konfidentiell information eller utföra handlingar som äventyrar person- eller organisationssäkerhet (Algarni et al. 2015). Förövaren utnyttjar det hål som finns i alla organisationers säkerhetsarkitektur - människan (Ivaturi & Janczewski, 2011; Hauser, 2016). Denna studie använder en reviderad version av Ivaturi & Janczewski's (2011) modell '*Taxonomy for Social Engineering Attacks*' för att kategorisera SE-tekniker (se figur 1). Modellen sammanställer och beskriver SE-tekniker på ett tydligt och omfattande sätt.

Vår modell skiljer sig ifrån Ivaturi & Janczewski's (2011) i det att vi valt att ta bort två kategorier samt slå ihop två kategorier, vi har även valt att lägga till en kategori. I den här uppsatsens kategoriseringsmodell är kategorierna *Real Person Impersonation* och *Fake Person Impersonation* sammanslagna och kategoriseras som *Impersonation*. Kategorierna *Search Engine poisoning (SEP)* och *Video* är borttagna eftersom vi anser att de är för ovanliga och för svåra att genomföra och är därför inget som ämnas att gå in djupare på. Video-attacker kräver att offret självmant letar upp en video och utför flera självdestruktiva tekniska steg som vi inte anser vanligt förekommande i den målgrupp vi undersöker. SEP är beroende av signifikanta globala händelser för att utföras vilket av oss inte anses tillräckligt vanligt för att tas hänsyn till. (Ivaturi & Janczewski, 2011). Kategorin *Spear Phishing* är tillagd eftersom vi anser att den saknas i ursprungsmodellen. Spear Phishing är en vanligt förekommande SE-attack som många organisationer råkar ut för där meddelandet konstrueras och anpassas utifrån mottagaren (Wright et al. 2014). Den här uppsatsens kategoriseringsmodell är således smalare och mer i linje med uppsatsen syfte, se figur 1.




**Figur 1. Kategorisering av SE-tekniker**

### *2.1.1 Person-Person*

Person-Person är den typen av tekniker som utförs ansikte mot ansikte. Förövaren utnyttjar offrets ignorans eller spelar på offrets känslor för att genomföra en attack (Ivaturi & Janczewski, 2011). Förövaren kan exempelvis lura offret på information eller få offret att stoppa in ett skadligt USB-minne i sin organisationsdator. *Impersonation* är det samlingsnamn för de SE-tekniker där förövaren utger sig vara någon annan för att manipulera sina offer (Ivaturi & Janczewski, 2011).

**Pretexting** utförs i två steg. Först lägger förövaren ner tid och energi på att samla in information om offret för att etablera en kontextuell lögn. Det kan exempelvis vara information om offrets arbetsplats eller känslomässiga tillstånd. Med hjälp av informationen skapar förövaren en trovärdig roll som är i position att lura offret på önskvärd information. Tekniken skiljer sig från övriga impersonation-tekniker i att det krävs ett stort förarbete. (Ivaturi & Janczewski, 2011).

**Reverse social engineering** innebär att förövaren utger sig för att vara en person med auktoritär position för att manipulera offret till att ställa frågor istället för tvärtom (Algarni et al. 2014; Braun & Esswein, 2012). Attacken utförs ofta i två steg där förövaren först saboterar,

för att sedan assistera. I steg ett problematiserar förövaren något för offret och vinner dennes tillit (Ivaturi & Janczewski, 2011).

Förövaren utger sig sedan för att tillhöra en legitim organisation, exempelvis en supportservice, som erbjuder hjälp. Offret ringer upp supporten ovetande om att den som svarar är förövaren som fått offrets förtroende. Tekniken är av dess natur väldigt effektiv när den väl fungerar eftersom offret söker sig till förövaren. (Ivaturi & Janczewski, 2011).

**Tailgating** betyder helt enkelt att förövaren tar sig in till ett obehörigt område genom att ta rygg på en person som har behörig access till exempelvis lokaler (Long, 2008). För att stärka trovärdigheten i att förövaren har rätt att vistas på området används kontextuella verktyg som exempelvis arbetskläder (Ivaturi & Janczewski, 2011).

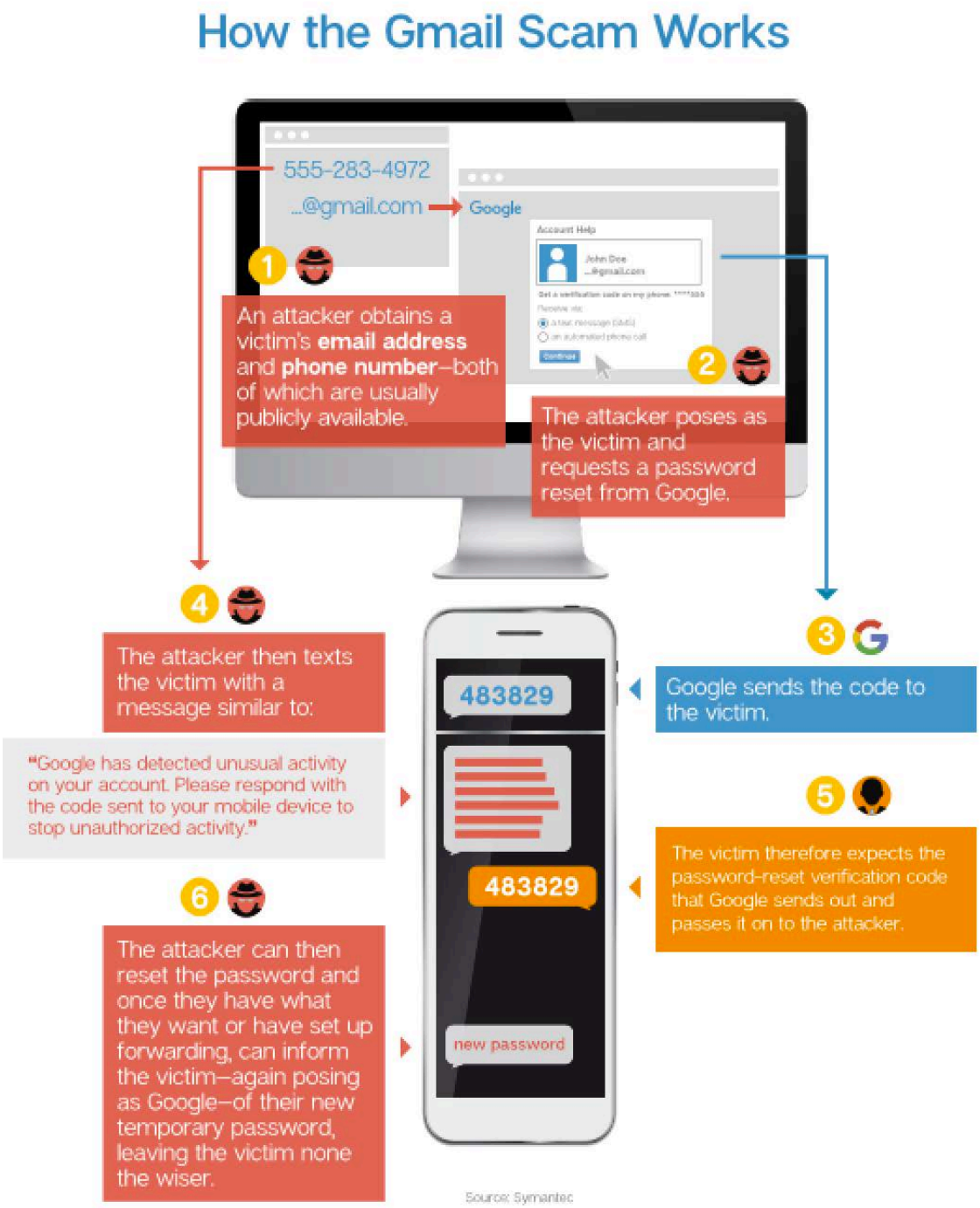
### *2.1.2 Person-Person via Media*

Alla tekniker som inte involverar direkt fysisk kontakt kategoriseras som Person-Person via Media-tekniker. Media gör det möjligt för förövare att utföra anonyma och skalbara SE-attacker (Ivaturi & Janczewski, 2011). Denna uppsats fokuserar på text- och ljudmedier.

**Phishing** kombinerar SE och IT-bedrägeri för att stjäla konfidentiell information såsom kontouppgifter och lösenord (Wright et al. 2014). Förövaren lägger ut en krok genom att skapa och skicka ut hundratals mail till slumpmässiga mailadresser i hopp om att ett fåtal nappar (Ivaturi & Janczewski, 2011). Mailen ger ofta ett löfte om pengar eller gåvor i utbyte mot information (Flores & Ekstedt, 2013). Enligt Goel et al. (2017) ökar chansen att offret nappar om något värdefullt står på spel, vilket också utnyttjas av förövaren.

**Spear Phishing** skiljer sig från Phishing i det att mailen som skickas ut är skickade till utvalda adresser och där mailen är utformade för det specifika offret. Förövaren skickar mailen från en spoofad adress som offret har anledning att lita på. Det kan vara att förövaren utger sig vara en bekant till offret eller en organisationskund. (Wright et al. 2014).

**SMSishing** liknar Phishing och Spear Phishing men utförs via short service message (SMS) i mobilen (Rouse, 2017). Många organisationer har börjat använda SMS-verifiering när man loggar in ifrån en enhet som inte använts tidigare, vilket är något som SE-förövare ser som en möjlighet att lura människor (Ivaturi & Janczewski, 2011). Exempelvis använder Google SMS-verifiering vid inloggning till sin mailtjänst, vilket SE-förövare lärt sig utnyttja som man kan se i modellen nedan (*se figur 2*)(Symantec, 2016).




**Figur 2. Hur Gmail-bedrägerier fungerar (Symantec, 2016)**

**Malware** är ett verktyg som används inom SE-attacker. Malware är ett samlingsnamn för skadlig programvara som attackerar enheter. Malware är på grund av dess genomträngande och ihärdiga natur väldigt effektiv. (Ivaturi & Janczewski, 2011). Förövaren kan utföra Malware-attacker på alla enheter som kan ansluta till internet vilket innefattar datorer, smartphones och surfplattor (Flores & Ekstedt, 2013). När den skadliga programvaran infiltrerat media-enheten kan den exempelvis samla känslig information och få tillgång till system och pro-

gram (Flores & Ekstedt, 2013; Ivaturi & Janczewski, 2012). Malware sprids huvudsakligen genom två välkända kanaler - mail och sociala nätverk (Ivaturi & Janczewski, 2011).

När malware sprids via mail är det oftast i form av ett phishing- eller spear phishingmail där offret ombeds klicka på en skadlig länk (Algarni et al. 2014; Flores & Ekstedt, 2013).

På sociala nätverk skapar förövaren fejkade profiler och sprider meddelanden med länkar. Länkarna är förkortade med hjälp av URL-förkortningsprogram och leder till en direktnedladdning av malware. (Ivaturi & Janczewski, 2012).

**Vishing** är en teknik som går att jämföra med phishing och SMSishing men skiljer sig i att attacken utförs via telekommunikation med röstverktyg (Ivaturi & Janczewski, 2011). Förövaren använder ofta spoofade uppringnings-IDn för att ge sken av att samtalet kommer ifrån trovärdiga organisationer (IBM, 2015).

### *2.1.3 Systempåverkan av SE-attacker*

Ovanstående visar på att det finns många SE-tekniker som en förövare kan utnyttja för att attackera en organisation. Förövaren av SE-attacker har ofta ett syfte med sin attack (Ivaturi & Janczewski, 2011). Syftet kan leda till både mindre kritiska och kritiska påföljder för en organisation. Mindre kritiska attacker kan vara att förövaren vill ta en självguidad tur på organisationens område eller sprida reklam. De attackerna har ingen direkt påverkan på organisationen. Kritiska attacker kan vara stöld av lösenord, personregister och spridning av malware. Kritiska attacker kan resultera i att förövaren får fullständig administrativ access till en anställds dator via lösenordshackning och malware. Det innebär att en förövare potentiellt kan läsa av all datatrafik, komma åt alla tekniska funktioner i ett system och utföra de handlingar som den anställde kan utföra via datorn. (Ivaturi & Janczewski, 2011). I värsta fall kan förövaren ta full kontroll över system och dess information och låsa offret ute. Den möjliga påverkan en SE-förövare har är beroende av vilken access som finns att tillgå. (Ivaturi & Janczewski, 2011). Men det som är säkert är att arbetet med att upptäcka och återhämta sig från SE-attacker både är dyrt och tidskrävande (Hauser, 2016).

## 2.2 Interpersonal Deception Theory

Hauser (2016) menar att tillit är en grundsten som bygger relationer mellan människor och är en vital del i kommunikation. Tillit byggs upp när människor kommunicerar på ett ärligt och uppriktigt sätt. I kontrast innehåller en fjärdedel av alla samtal mellan människor deception. Trots den frekventa användningen av deception är det sällan människor uppfattar att de blir lurade. (Hauser, 2016).

Bakomliggande teorier till SE grundar sig därför ofta i ‘Deception Theory’ (Marret et al. 2009; Moffit, 2009; Wright et al. 2014). Deception Theory fokuserar på fenomenet deception (Marret et al. 2009) vilket självklart är intressant för den här uppsatsen, men vi anser att den teorin är för bred. Interpersonal Deception Theory (IDT), som är baserad på Deception Theory, omfattar även den interaktiva delen mellan människor (Hauser, 2016; Moffitt, 2009; Ivaturi et al. 2014) vilket gör att den passar mycket väl som bakomliggande teori till SE.

Det är nödvändigt att förstå IDT för att förstå varför SE-tekniker fungerar då IDT förklarar de socialpsykologiska aspekterna vid en deceptiv interaktion (Ivaturi et al. 2014), det vill säga varför människor blir lurade av andra människor. Hauser (2016) menar att förövaren och mottagarens kognition, emotion och beteende avgör om deceptiva samtal "lyckas", vilket innebär att deceptionen inte upptäcks och förövaren får ut det hen vill åt. Förövaren och mottagarens kognition och beteende påverkas i sin tur av sammanhanget vilken innebär att sammanhanget påverkar hur lyckosamt ett deceptivt samtal är. Det betyder att människors mottaglighet för deception går att påverka (Moffit, 2009).

Exempel på variabler som spelar in är samtalets spontanitet, relation mellan förövare och offer, verbalt språk, kroppsspråk (verbala och icke verbala sociala indikationer) och känslor som rädsla, intresse och nyfikenhet (Hauser, 2016). En skicklig SE-förövare spelar på nämnda variabler och manipulerar dessa för att uppnå sina mål. Förövaren använder rätt språk och kroppsspråk, läser av ansiktsuttryck, spelar på känslor, iscensätter situationer och utger sig för att vara någon annan för att skapa önskvärd relation till offret (Hauser, 2016). I fall där en SE-attack sker via text går det inte att applicera alla variabler inom IDT som exempelvis kroppsspråk. I SE-tekniker som finns under kategorin ‘Person-Person via Media’ är dock den deceptiva informationen inbäddad i textmeddelandet och förövaren spelar lika mycket på offrets känslor och manipulerar kontexten för att få sin vilja igenom (Ivaturi et al. 2014).

## 2.3 Informationssäkerhetspolicys (ISP)

Organisationer spenderar miljoner på att sätta upp brandväggar, VPN-tunnlar och antivirus-program för att skydda sig från yttre attacker (Herath & Rao, 2009). Det största hotet är dock det interna hotet, det vill säga användaren som redan är inne bakom brandväggar och har tillgång till systemen. (Warkentin & Willison, 2009). Det sker ofta incidenter eller attacker där användaren är den länk som bryter säkerhetskedjan, vilket tyder på att organisationen måste arbeta mer med sina policys (Mishra & Dhillon, 2006). Även om säkerhetspolicyn är välskriven tyder sådana läckor på att implementeringen och utbildningen av användarna inte är tillräcklig (Herath & Rao, 2009).

Idag använder och förlitar sig organisationer på flertalet informationssystem för att utföra sitt arbete. Som ett resultat av detta är det viktigare än någonsin att analysera och motverka risker och hot inom systemen. (Bulgurcu et al., 2010). Informationsläckage kan leda till stora förluster såsom färre konkurrensfördelar, tappad trovärdighet och juridiska skyldigheter. Detta i sin tur kan resultera i ännu större monetära förluster. (Bulgurcu et al., 2010).

### *2.3.1 Vad är en policy?*

För att skydda sig mot ovanstående faktorer används informationssäkerhetspolicys (ISP) som tas fram och appliceras inom organisationen. Gollmann (2011) definierar en säkerhetspolicy som något som beskriver de objektiv och riktlinjer organisationer har med hänsyn till säkerhet. Policyn bör förklara vad som är värdefullt inom organisationen och hur det ska skyddas. (Gollmann, 2011). Enligt Al-Omari et al. (2011) måste en policy ge riktlinjer om hur och varför information måste skyddas i anställdas dagliga arbete.

En säkerhetspolicy ska således inte bara vara påståenden om hur viktigt det är att skydda information. Istället ska en policy förklara vilka krav som ställs på anställda och andra användare, hur de ska agera samt vad de ska undvika att göra. En god policy ska även inkludera ansvarsområden och delegera ut specifikt ansvar till chefer, underchefer och övriga anställda. (LeVeque, 2006).

Med hänsyn till SE finns det flera olika policys som kan ge visst skydd mot attacker. Exempel på dessa är mailpolicys för att minska risken för phishing- och andra person-person via media-attacker, men även fysiska säkerhetspolicys för att hindra tailgating och för obehöriga förövare att ta sig in i byggnaderna (Durgin, 2007).

### *2.3.2 Mailpolicy*

Durgin (2007) problematiserar mail som en osäker kommunikationskanal, då meddelanden skickas via en tredje parts server. Detta öppnar således upp för risker som avlyssning av de mail som skickas. Därför är det ytterst viktigt att organisation applicerar policys för mail och andra meddelandekanaler. Policys kan till exempel inkludera krypteringsmetoder eller att inte skicka konfidentiell information via dessa kanaler. (Durgin, 2007).

### *2.3.3 Lösenordspolicy*

Organisationer skapar ofta starka lösenordspolicys som tvingar anställda och användare att skapa starka lösenord (Kelley, 2006). Exempelvis kan sådana regler vara att lösenordet måste

vara minst åtta tecken; måste innehålla både gemener, versaler, siffror och specialtecken; de får inte innehålla grundord, namn eller efternamn och måste bytas kontinuerligt (Kelley, 2006). Dessa policys skapas för att göra organisationen mer säker, men kan resultera i motsatt effekt. Allt för strikta policys kan leda till vanskligt beteende hos användarna ur ett säkerhetsperspektiv, där de delar eller skriver ned sina lösenord för att komma ihåg dem (Kelley, 2006; Durgin, 2007).

### *2.3.4 Fysisk säkerhetspolicy*

Andra policys som bör finnas inom en organisation är de som behandlar fysisk säkerhet som exempelvis USB-minnen och andra portabla lagringsenheter. Avsaknad av dessa policys kan utgöra en stor säkerhetsrisk för främst SE-attacker då USB-minnena kan innehålla malware (Flores & Ekstedt, 2013). Durgin (2007) tar upp ett exempel om just detta, då 20 USB-minnen lämnades på publika platser i syftet att utföra ett penetrationstest på ett kreditbolag. 15 av 20 USB-minnen kopplades in i organisationsdatorer och den fil som låg på enheten öppnades. (Durgin, 2007).

Policys som behandlar lokaler och andra organisatoriska utrymmen bör också finnas för att minimera eventuella SE-attacker. Detta kan vara i form av passerkort eller portkod, men även att anställda bör vara medvetna om hur de ska agera gentemot personer som inte verkar tillhöra organisationen. I en annat penetrationstest diskuterar Durgin (2007) att förövaren enkelt kunde komma in igenom organisationens passerkortsspärr genom att använda ett bonuskort för en matvaruaffär. Förövaren kunde sedan snabbt lokalisera ett skrivbord med post-it lappar med användarnamn och lösenord utan att någon gång bli ifrågasatt varför eller vad han gjorde där. (Durgin, 2007).

### *2.3.5 Övriga policys*

Utöver de ovan nämnda bör även andra policys implementeras inom organisation. Exempelvis policys som reglerar behörigheter på intranät och internet, som att blockera sidor som ej är jobbrelaterade. Policys som berör telefoni och hur anställa bör agera gentemot informationsutlämning över telefon är också något som minimerar risken för en SE-attack. (Durgin, 2007).

### *2.3.6 Policy-efterföljning*

Något som inte läggs lika mycket resurser på, men som har på senare tid växt fram till att bli en nyckelfaktor inom organisationer är anställdas *policy compliance*, det vill säga hur anställda följer säkerhetspolicys (Bulgurcu et al., 2011). Som tidigare nämnt skapar organisationer ISP för att säkerställa att organisationens information och tillgångar hanteras på ett säkert sätt samt för att minimera risker och hot. Bulgurcu (2010) menar på att detta inte är tillräckligt för att skapa en säker organisationsgrund. Det är även mycket viktigt för en organisation och dess managers att förstå hur och varför anställda och andra användare av systemen får motivation att följa uppsatta policys (Bulgurcu et al., 2010). Även fast skapandet av ISP är högprioriterat saknas fortfarande hög uppföljning och lydnad inom många organisationer (Bulgurcu et al. 2010). En annan nyckelfaktor är således att identifiera de faktorer som gör att användarnas medvetenhet och vilja att följa policys ökar (Al-Omari et al., 2011).

Exempel på hur organisationer kan öka medvetenhet är enligt Durgin (2007) kontrakt där användaren skriver under att denne har tillgodogjort sig och förstått de policys som finns. På så

sätt kan även den anställde stå till svars vid eventuellt intrång, då ursäkten att de ej visste om policyn inte är applicerbar. Detta är även viktigt när underleverantörer används, då dessa också ska gå under organisationens säkerhetspolicys. (Durgin, 2007).

## 2.4 Medvetenhet: ISA och ISPA

Information Security Awareness (ISA) är en persons generella medvetenhet om informationssäkerhet (Bulgurcu et al. 2010). Som tidigare nämnt implementerar även företag policys, eller riktlinjer, hur anställda ska agera i givna situationer. Denna kunskap eller medvetenhet benämns Information Security Policy Awareness (ISPA) och syftar på den medvetenhet kring de förväntningar som ställs på de anställda genom policys (Bulgurcu et al. 2010). ISPA skiljer sig från ISA då en anställd kan vara medveten om att lösenord används, men vet inte om att dessa måste bytas kontinuerligt och hur starka de måste vara (Bulgurcu et al. 2010).

ISA är, till skillnad från ISPA, en människas kunskap om säkerhet (Bulgurcu et al. 2010). Denna kunskap kan komma från utbildningar men också från erfarenhet. Har en anställd tidigare blivit utsatt för en phishing-attack eller råkat illa ut för att inte följt riktlinjer förväntas hens ISA vara högre än någon som aldrig varit i kontakt med informationssäkerhet och dess risker (Bulgurcu et al. 2010). Således förväntas även anställda inom IT-avdelningarna ha en högre grad av ISA och ISPA då dessa anställda i högre grad kommit i kontakt med IT-relaterade hot och riktlinjer. Bulgurcu et al (2010) hävdar även att desto högre en anställds ISA är desto större är chansen att hen följer de policys och riktlinjer som finns.

Att anställda inte följer policys är ett stort problem för organisationer (Karjalainen & Siponen, 2011). Enligt D'Arcy et al. (2009) kan en organisation använda tre verktyg för att minimera IS-risker, som till exempel SE-attacker, och öka säkerheten inom organisationen. Dessa är säkerhetsutbildning och träning; medvetenhet och kunskap om policys; samt datorövervakning (D'Arcy et al., 2009). Blir anställda även bestraffade vid brytande av policys kan anställdas policyefterföljning öka, dock kan detta resultera i att viljan att följa policys blir lägre (Mehri & Ahluwalia, 2013).

Likt D'Arcy et al. (2009) menar Bulgurcu et al. (2010) att ISA kan förklaras genom socialpsykologiska aspekter, där kunskap påverkar en människas beteende eller beslut. Definition av ISA och ISPA för denna uppsats är således en kombination av generell säkerhetsmedvetenhet och medvetenhet om de policys som finns inom organisationen. Denna medvetenhet förväntas påverkas av socialpsykologiska faktorer som attityd, norm och kontroll, men även vilken arbetsroll och avdelning som de anställda innehar.

## 2.5 Theory of Planned Behavior

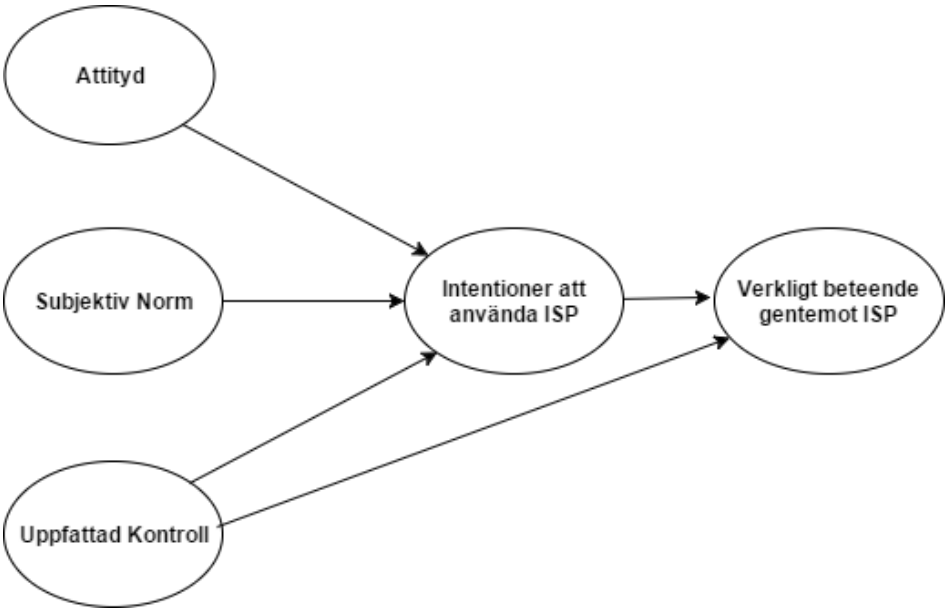
Denna uppsats bygger på, utöver IDT-teorin, Theory of Planned Behaviour (TPB). Teorin är ett ramverk som används och appliceras inom mycket IT-forskning, trots sitt mer socio-behaviorala ursprung (Bulgurcu et al. 2011). Då denna uppsats ämnar undersöka anställdas säkerhetsmedvetenhet och policy-efterföljning inom olika avdelningar på olika organisationer anser vi att det är en teori som kan hjälpa oss att besvara den hypotes och frågeställning som är formulerad. En annan teori som är nära besläktad med TPB är *Theory of Reasoned Action* (TRA). Denna teori tar upp två av de tre huvudfaktorer som TPB diskuterar, medan TPB har

en tredje behavioral faktor som är upplevd kontroll (Montano & Kasprzyk, 2015). Då upplevd kontroll är, enligt oss, en faktor som även spelar in i hur människor agerar i situationer anser vi att TPB således ger en bättre förklaring till anställdas beteende än TRA. TPB är även en väletablerad teori som myntades av Ajzen (1991) och således finns det flertalet studier som backar upp och stödjer detta teoretiska ramverk (Bulgurcu et al. 2011; Boubaker et al, 2006; Warner, 2006)

Theory of Planned Behaviour menar på att en användares beteende är beroende av användarens attityd, den subjektiva normen samt uppfattad kontroll (percieved behavioral control) (Warner, 2006). För varje kontext måste även en framträdande övertygelse identifieras för att ett beteende skall ses som gynnsamt (Ajzen, 1991). I detta fall handlar det om övertygelse om säkerhet, policys och medvetenhet om IT för att således följa de policys som satts upp. Finns inte övertygelsen blir beteendet ofta avvikande från till exempel ISP (Ajzen, 1991).

Den här uppsatsen använder modellen för TPB som är baserad på Ajzens (1991) artikel. Modellen visualiserar de tre nyckelfaktorerna attityd, subjektiv norm och uppfattad kontroll (Warner, 2006; Al-Omari et al., 2011) som har stor påverkan på hur väl ISP appliceras och efterföljs inom organisationer.

Originalmodellen är marginellt mer omfattande då studien tittar på och analyserar fler bakomliggande faktorer till de tre huvudfaktorerna. Med hänsyn till denna studie och dess avgränsningar valde vi att simplifiera modellen och endast fokusera på de tre nyckelfaktorerna Attityd, Subjektiv Norm och Uppfattad Kontroll.




**Figur 3. Modell för TPB baserad på Ajzen (1991).**

### *2.5.1 Attityd*

En användares attityd gentemot ISP och hur dessa efterföljs syftar på om användaren tycker att det är gynnsamt eller ogynnsamt att följa ISP (Bulgurcu et al., 2010; Kranz & Haeussinger,

2014). Exempelvis kan en användare tycka att det är komplicerat och för omständligt att komma ihåg flera lösenord i huvudet och går därför emot ISP och skriver ned dem på en lapp bredvid datorn.

### *2.5.2 Subjektiv Norm*

Definitionen för den subjektiva normen i modellen är det grupptryck eller sociala tryck användaren känner för att följa ISP. Detta kan vara förväntningar och krav från kollegor, chefer och andra anställda. (Bulgurcu et al. 2010; Kranz & Haeussinger, 2014). Beroende på den norm som finns inom organisationen och avdelningar kan ISPA och hur de efterföljs variera (Kranz & Haeussinger, 2014).

### *2.5.3 Uppfattad Kontroll*

Den uppfattade kontrollen är en faktor som behandlar användarens kunskaper, färdigheter och kompetens för att kunna följa ISP (Bulgurcu et al. 2010; Kranz & Haeussinger, 2014). Detta är således korrelerat till hur hög ISA, eller medvetenhet, som användaren har (Kranz & Haeussinger, 2014). Diney & Hu (2007) stödjer detta och visade i sin studie att högre medvetenhet om ISP och generell säkerhet leder till större självförtroende i att förhindra negativa arbetstekniker och att arbeta mer säkert. Detta är en typ av kontroll som ökad medvetenhet resulterar i (Diney & Hu, 2007).

## 2.6 Teoretiskt ramverk

Nedan visualiseras och förklaras den här uppsatsens teoretiska ramverk och hur dess olika delar är kopplade till varandra (se figur 4 & 5). Det teoretiska ramverket används för att besvara vår forskningsfråga som lyder:

*Hur ser IT-säkerhetsmedvetenheten med fokus på social engineering ut på IT-avdelningar respektive övriga avdelningar inom medelstora / stora organisationer?*

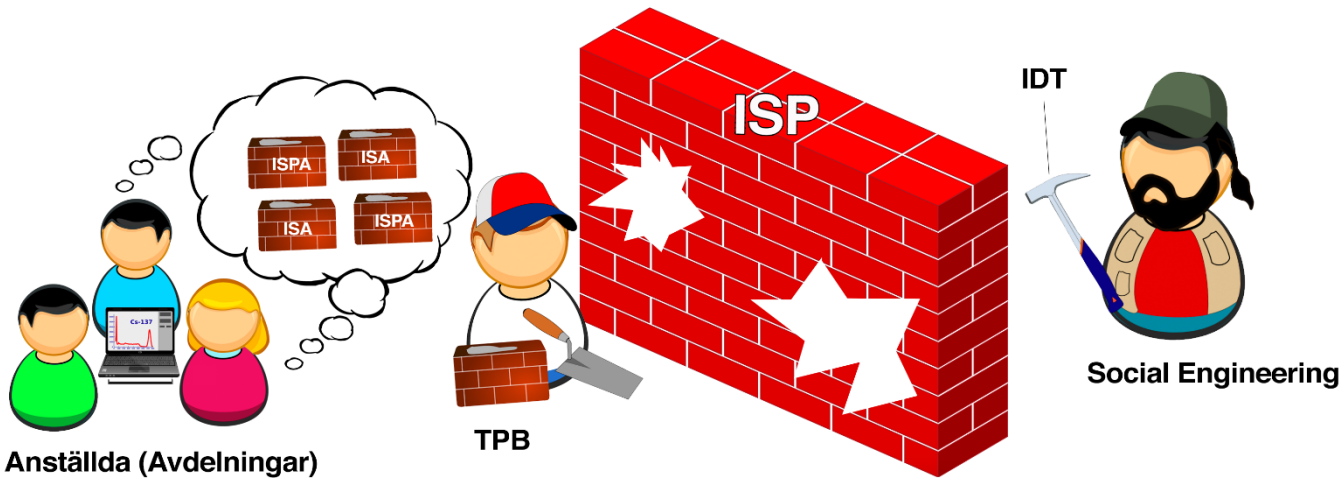
Eftersom SE är uppsatsen inriktning krävs det en förståelse för vad det är. SE är en form av icke-teknisk hackning som används för att manipulera individer till att avslöja konfidentiell information (Algarni et al. 2015). Förövaren visualiseras därför som förövare. Förövaren utnyttjar det hål som finns i alla organisationers säkerhetsarkitektur - människan (Ivaturi & Janczewski, 2011; Hauser, 2016). Att få en inblick i SE-tekniker är nödvändigt för att diskutera hur organisationer kan skydda sig mot just dessa.

För att förstå varför SE-tekniker fungerar appliceras IDT eftersom IDT förklarar de socialpsykologiska aspekterna vid en deceptiv interaktion (Ivaturi et al. 2014), det vill säga varför människor blir lurade av andra människor. Hauser (2016) menar att förövaren och mottagarens kognition, emotion och beteende avgör om deceptiva samtal "lyckas", vilket innebär att deceptionen inte upptäcks och förövaren får ut det hen vill åt. Förövaren och mottagarens kognition och beteende påverkas i sin tur av sammanhanget vilken innebär att sammanhanget påverkar hur lyckosamt ett deceptivt samtal är. Det betyder att människors mottaglighet för deception går att påverka (Moffit, 2009). IDT blir således verktyget SE-förövare använder.

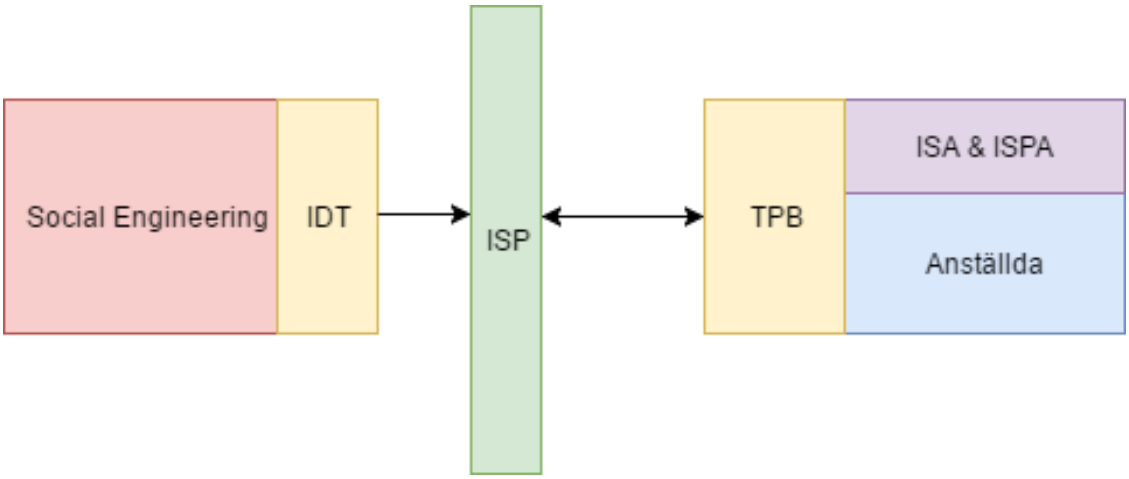
Organisationer spenderar miljoner på att sätta upp brandväggar, VPN-tunnlar och antivirus-program för att skydda sig från yttre attacker (Herath & Rao, 2009). Det största hotet är dock det interna hotet, det vill säga användaren som redan är inne bakom brandväggar och har tillgång till systemen (Warkentin & Willison, 2009). Organisationer utformar därför ISP, som ämnar ändra anställdas arbetssätt för att arbeta i linje med organisationens värderingar, mål och säkerhetskrav (Gollmann, 2011). ISP fungerar därför som muren. ISP blir är viktig del i det teoretiska ramverket eftersom det är direkt kopplat till organisationens IT-säkerhet. ISP fungerar som ett verktyg för att få sina anställda säkerhetsmedvetna och hjälper därför till att svara på vår forskningsfråga. För att undersöka ISPA krävs det att vi jämför policys som råder inom organisationerna med de anställdas medvetenhet om dessa.

Policys skapar inte säkra organisationer per automatik. Enligt D'Arcy et al. (2009) och Bulgurcu et al. (2010) krävs det att organisationens anställda är medvetna om informationssäkerhet (ISA) och om vilka policys som finns (ISPA) och att dessa policys efterföljs. Bristande ISA och ISPA visualiseras därför som hålen i muren. Har en organisations anställda låg medvetenhet om informationssäkerhet och policys är organisationen alltid sårbar mot SE-attacker (Ivaturi et al. 2014; Bulgrucu et al. 2010). ISA och ISPA blir således tegelstenarna som täpper igen de hål som finns i muren. ISA och ISPA hjärtat i vår forskningsfråga.

TPB i modellen syftar till de socialpsykologiska aspekter som påverkar en anställds beteende – attityd, norm och uppfattad kontroll (Warner, 2006). Ifall alla dessa tre aspekter uppfyller och främjar ett säkerhetsmedvetet arbetssätt hävdar Bulgurcu et al. (2010) att policys kommer att efterlevas i en större utsträckning. TPB är visualiserat i bilden nedan som den murare som täpper igen muren med de tegelstenarna, då de tre huvudaspekterna påverkar anställdas beteende.




**Figur 4. Visualisering av det teoretiska ramverket**




**Figur 5. Modell av teoretiskt ramverk**

# 3 Metod

*I detta kapitel motiveras metodval. Vi ger en förklaring till hur litteraturstudien gått till och motiverar val av metodansats och respondenter. Kapitlet redogör även insamling och analys av empirisk data. Slutligen redogörs hur vi arbetat med etik, reliabilitet och validitet i den här uppsatsen.*

## 3.1 Utformning av litteraturstudie

Webster och Watson's (2002) artikel beskriver hela processen om hur man utformar en litteraturstudie, från hur man bör tänka vid litteratursökning till hur man sammanställer den och kopplar samman teori och diskussion. Framtagandet av vår litteraturstudie har därför tagit stöd ifrån Webster och Watson's artikel. Att hitta relevant litteratur till det område man undersöker är vitalt för alla akademiska uppsatser (Webster & Watson, 2002). Den här undersöker säkerhetsmedvetenhet och policys ur ett SE-perspektiv. Därför gjordes en omfattande litteraturgenomgång inom områdena SE, ISP, ISPA och ISA för att ge oss en överblick av befintlig forskning. Webster & Watson (2002) förklarar att det är viktigt att börja undersöka litteratur som är av hög kvalitet och ledande inom området man undersöker. För att säkerställa att litteraturen vi studerande var av absolut högsta kvalitet användes artikeldatabasen "AIS basket of 8", som är den ledande källan till forskningslitteratur inom systemvetenskap (AIS, 2017). Under uppsatsens skrivande har fler källor tagits fram för att styrka och motivera påståenden. De källorna har främst tagits fram genom att se vilka källor artiklarna från AIS basket of 8 hänvisar till. Litteratur som berör policys och SE är avgränsade från år 2006 och framåt eftersom vi anser att äldre källor ses som utdaterade.

När vi skapat oss en bild av befintlig litteratur inom dessa områden undersökte vi vilka bakomliggande teorier som används. Genom vår litteraturgenomgång upptäckte vi att teorierna IDT och TPB var vanligt förekommande i forskningsartiklar som berör det vi vill undersöka. Efter vidare läsning av befintlig forskning bestämde vi oss för att dessa teorier var bäst lämpade som teoretiska grundpelare i vår uppsats.

För att få en strukturerad överblick av litteraturstudien gjorde vi en litteraturtabell som är baserad på Webster och Watson's 'Concept Matrix'. I vår första version av litteraturtabellen listade vi 36 artiklar som potentiellt var av relevans för vår uppsats, där vi skrev vilka teorier som använts, vilka områden som berördes, sökmetod samt en kort sammanfattning (se under Appendix IIII).

Den slutgiltiga versionen av vår litteraturtabell är mer städad och där återfinns 26 artiklar som alla används i uppsatsen och är färgkodade baserat på relevans (se Appendix III). Grönmarkerade artiklar är artiklar som är av hög relevans för den här studien och hänvisas till frekvent. Dessa artiklar är listade nedan i tabell 1. De gröna artiklar har antingen använt sig av samma bakomliggande teorier eller gått igenom koncept som är viktiga för oss på ett djupgående sätt.

Gulmarkerade artiklar är artiklar som vi anser har relevans för vår uppsats och hänvisas till fler gånger, dock har dessa artiklar inte utfört en liknande undersökning eller använt samma teorier. Rödmarkerade artiklar är artiklar som inte använder samma teorier eller undersöker liknande saker men som har ett par delar som är relevanta för vår uppsats, dessa artiklar hänvisas till mindre frekvent.

| **Titel** | **Författare** | **Teori** |
|---|---|---|
| INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS | Bulgurcu et al. (2010) | TPB |
| Social Engineering Awareness in Business and Academia | Hauser (2016) | IDT |
| A Typology Of Social Engineering Attacks – An Information Science Perspective | Ivaturi & Janczewski (2012) | N/A |
| 8R. Effect of Frame of Mind on Users' Deception Detection Attitudes and Behaviours | Ivaturi et al (2014) | IDT |
| Towards Understanding User Behavioral Intentions to Use IT Security: Examining the Impact of IT Security Psychological Climate and Individual Beliefs | Warner (2006) | TPB |
| A Decomposed Model of IT Artifact-related Beliefs as Antecedents of IT Acceptance and Use | Boubaker et al. (2006) | TPB |
| Information Security Policy Compliance: A User Acceptance Perspective | Al-Omari et al. (2011) | TPB |
| INFORMATION SECURITY POLICY COMPLIANCE: THE ROLE OF FAIRNESS, COMMITMENT, AND COST BELIEFS | Bulgurcu et al. (2011) | TPB |
| Why Deterrence is not Enough: The Role of Endogenous Motivations on Employees' Information Security Behavior | Kranz & Haeussinger, 2014 (2014) | TPB |
| Understanding the Importance of and Implementing Internal Security Measures | Durgin (2007) | N/A |
| An Identity Fraud Model Categorising Perpetrators, Channels, Methods of Attack, Victims and Organisational Impacts | Jamieson et al. (2007) | N/A |

**Tabell 1. Teoretiskt ramverk - Litteraturstudie**

## 3.2 Val av metodansats

Det finns två övergripande metodansatser vid empiriska studier, kvantitativ och kvalitativ metod. Kvantitativ metodansats intresserar sig för statistiskt verifierbara samband medans kvalitativ metodansats intresserar sig för meningar och innebörder (Alvehus, 2013). En kvalitativ studie lämpar sig bättre vid undersökningar av sociala fenomen vilket passar uppsatsen syfte (Backman, 2008). Vi valde därför en kvalitativ metodansats i hopp om att få en djupare insikt i organisationers IT-säkerhetskultur och respondenternas medvetenhet. En kvantitativ metodansats hade dock möjliggjort för en tydligare representation av resultaten (Alvehus, 2013).

## 3.3 Insamling av empirisk data

Intervjuer är ett av den kvalitativa metodens flaggskepp och används för att ta reda på hur människor känner, tänker och handlar i olika situationer vilka är linje med den här uppsatsens syfte. Vi valde att utföra semistrukturerad intervjuansats som innebär att vi följde ett intervjuformulär med ett flertal öppna frågor som ger respondenten möjlighet att påverka intervjuns innehåll (Alvehus, 2013).

Intervjuer är ett sätt att komma närmare respondenterna och genererar mer trovärdiga svar än exempelvis enkäter (Alvehus, 2013). Intervjuformatet möjliggör friare tyglar och låter intervjuaren anpassa intervjun efter respondenten. Intervjuer ger möjlighet till dialog och minimerar risken för missförstånd och otillräckliga svar eftersom det alltid finns möjlighet till att klargöra missförstånd under intervjun (Alvehus, 2013). Av åtta intervjuer skedde sex stycken face-to-face och två över telefon. Intervjuerna varade i mellan 35–62 minuter (se tabell 2) vilket räckte för respondenten att svara på våra frågor. Det fanns inget tillfälle där vi behövde avbryta intervjun innan vi kändes oss klara.

Samtliga intervjuer spelades in, med respondenternas tillåtande. Vi använde telefonen iPhone 7 som inspelningsverktyg och inspelningarna är av bra kvalitet där man tydligt hör vad som sägs. Att spela in intervjuerna möjliggjorde korrekta transkriberingar och lät intervjuaren att helt fokusera på dialogen istället för att ägna tid åt att anteckna (Alvehus, 2013). Dock finns det en risk med att spela in intervjuer eftersom respondenterna kanske inte svarar sanningsenligt när de vet att allting finns med på band (Alvehus, 2013). Dock ansåg vi att fördelarna med att spela in vägde tyngre.

| **Organisation** | **Avdelning** | **Längd** | **Typ** | **Referens (organisation&Nr:Avdelning)** |
|---|---|---|---|---|
| **Kommunalt** | IT | 58 min | Face-to-face | K1:IT |
| **Kommunalt** | Övrig | 35 min | Face-to-face | K2:Ö |
| **Kommunalt** | Övrig | 50 min | Face-to-face | K3:Ö |

| | | | | |
|---|---|---|---|---|
| **Kommunalt** | IT | 55 min | Face-to-face | K4:IT |
| **Kommunalt** | Övrig | 54 min | Face-to-face | K5:Ö |
| **Privat** | IT | 58 min | Face-to-face | P1:IT |
| **Privat** | Övrig | 62 min | Telefon | P2:Ö |
| **Privat** | Övrig | 40 min | Telefon | P3:Ö |

**Tabell 2. Överblick av intervjuer.**

## 3.4 Val av organisationer

Den kvalitativa studien genomfördes på två olika organisationer inom två olika branscher där det ena organisationen är medelstort och det andra stort (SCB, 2010). Den medelstora organisationen är ett kommunalt bolag medans den stora organisationen är ett privat bolag. Vilken typ av bransch som organisationen tillhör och vilken avdelning respondenten tillhör (utöver IT-avdelning) utelämnas efter begäran av en av organisationerna. Organisationerna valdes dels för sin storlek och bolagsform men också på grund av att vi har kontakter inom organisationerna vilken förenklade processen att boka intervjuer. Säkerhet är ett känsligt område och det underlättade att det fanns organisationsrepresentanter som gick i god för uppsatsens validitet.

Vi ville kolla på organisationer med fler än 60 anställda eftersom större organisation ofta har större omsättning och en större hotbild. Vår undersökning ämnar också ge en generell bild av medelstora och stora organisationers medvetenhet om SE och inte ge en bild som är unik för bransch eller bolagsform. Därav valet av två, på pappret, olika organisationer.

## 3.5 Val av respondenter

Respondenterna är valda baserade på ansvarsområden. Tre respondenter är inom IT och resterande fem är antingen inom HR, Kommunikation, Ekonomi, Sälj eller Logistik. Samtliga respondenter har slutgiltig påverkan av olika organisationsbeslut. Det är ett medvetet val att respondenterna innehar beslutsansvar och är de flesta fall högt uppsatta eftersom vi tror att ju högre upp organisationshierarkin vi kollar desto bättre inblick i hur organisationen centrala ISA, ISP och ISPA ser ut. Vi har valt anställda inom IT som utifrån sin titel kan förväntas ha god inblick i organisationens aktuella ISP. Respondenterna inom IT besitter alla ett säkerhetsansvar.

## 3.6 Utformning av intervjufrågor och teoretisk återkoppling

När litteraturstudien var sammanställd utformades intervjufrågor förankrade i teorin. Målet med intervjufrågorna är att de tillsammans ska besvara uppsatsen frågeställning vilken i sin tur byggs upp av teorin. Därav var det viktigt att samtliga frågor på något sätt har en koppling till en eller flera teoridelar. Dock är de två inledande frågorna till för att få igång en bra dialog med respondenten. En sammanställning av vilken teoretisk del som berörs av vilka frågor och relaterad litteratur finns nedan (se tabell 3). Den fullständiga intervjuguiden med motivering och teoretisk återkoppling finns under Appendix I. Många frågor är formade ur ett SE-perspektiv vilket innebär att frågorna går att relatera till de SE-tekniker som tas upp i kapitel 2.

| **Teori** | **Författare** | **Intervjufrågor** |
|---|---|---|
| **Medvetenhet**<br><br>ISA<br><br>ISPA | Bulgurcu et al. (2010), D'Arcy (2009) | 3-19 |
| **ISP**<br><br>Mailpolicy<br><br>Lösenordpolicy<br><br>Telefonpolicy<br><br>Fysisk säkerhetspolicy<br><br>Övriga policys | Durgin (2007), Kelley, (2006), LeVeque (2006), Al-Omari et al. (2011), Gollmann (2011), Bulgurcu et al. (2010), Herath & Rao (2009) | 7, 8, 10, 11, 12, 13, 14, 15 |
| **Socialpsykologiska aspekter**<br><br>Policy-efterföljning<br><br>TPB<br><br>IDT | Bulgurcu et al. (2010), Hauser (2016), Ivaturi et al (2014), Warner (2006), Boubaker et al. (2006), Al-Omari et al. (2011), Bulgurcu et al. (2011), Kranz & Haeussinger (2014) | 5, 8 , 10, 11, 12, 13, 14, 16, 19 |

**Tabell 3. Sammanfattning Teori/Författare/Intervjufrågor**

## 3.7 Intervjuteknik

Intervjuerna var semistrukturerade där intervjuaren utgick från ett frågeformulär men där intervjun formades av vad respondenten gav för svar. En semistrukturerad intervju ställer krav

på att intervjuaren lyssnar och anpassar sig till intervjun. Under intervjuerna har vi lyssnat aktivt och följt upp intressanta spår och visat intresse av vad respondenten har att säga, vilket enligt Alvehus (2013) är en bra intervjuteknik. Vi har i form av intervjuare försökt efterleva Alvehus intervjutekniker under samtliga intervjuer. Alvehus (2013) menar att en intervju inte får utvecklas till ett förhör där respondenten känner sig pressad att prestera, men att intervjuaren ibland måste ifrågasätta och provocera fram svar för få ut sanningsenliga data. Det har resulterat i att varje intervju är unik och att frågorna inte är exakt likadant ställda eller kommer i samma ordning (Se transkribering). Dock har vi lyckats få fram svar som täcker samtliga frågor från den utformade intervjuguiden. Intervjuer med IT-personal har fokuserat mer på ISP eftersom kunskapen varit starkare hos denna grupp vilket har gett en bra överblick av den faktiska ISP hos organisationerna.

## 3.8 Dataanalys intervjuer

### *3.8.1 Transkribering*

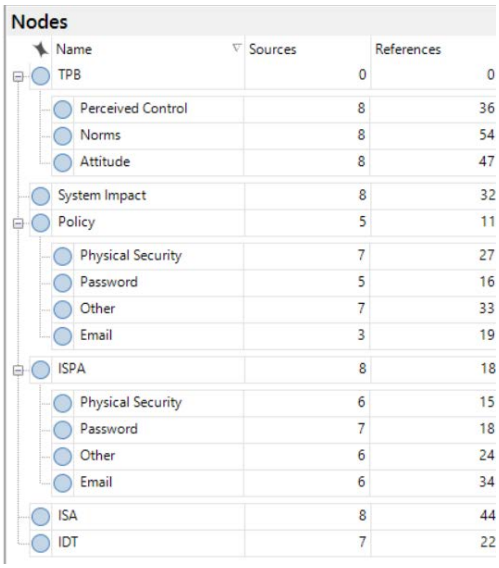
För att transkribera intervjuerna användes transkriberingsverktyget oTranscribe. I verktyget laddas ljudfilen upp där reglage finns för att spela/pausa, spela upp ljudfilen snabbbare/långsammare samt en ruta att skriva text i.

Intervjuerna har transkriberats i sin helhet med undantag för företagsnamn och personnamn samt ljud som till exempel ”eh..”. Vid händelser i intervjun som ej kan transkriberas, till exempel gester, har detta markerats inom parenteser. Detta för att öka läsbarheten och bevara organisationerna och respondenternas anonymitet.

### *3.8.2 Kodning av intervjuer*

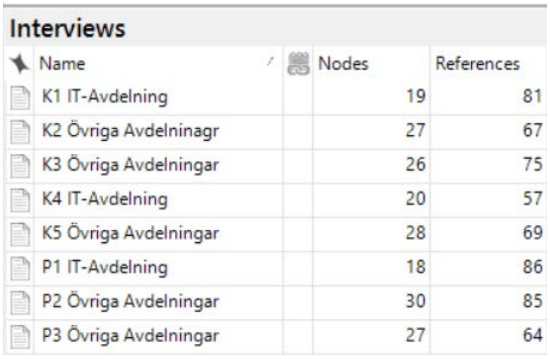
För att kunna tolka det kvalitativa resultat som empirinsamlingen resulterade i har intervjuerna kodats.

Intervjuerna kodades med hjälp av verktyget NVivo 10. De transkriberade intervjuerna lades in i programmet under ’Sources’ i undermappen ’Interviews’ (se figur 5). Sedan skapades noder med de huvudbegrepp (se figur 6) som intervjun behandlar. Baserat på instruktioner och föreläsningar av dr. Floris Bex (2016) kodades sedan intervjuerna till dessa olika teman. Under ’Nodes’ kan sedan en överblick ses på hur många referenser och intervjuer som vardera begrepp behandlar. Under varje ’node’ kan man sedan gå in och hitta de svar som behandlar det begreppet sorterat på intervjuobjekt. Vi valde att klassificera kodningen med olika begrepp då vi utförde semi-strukturerade intervjuer. Eftersom intervjuerna är semistrukturerade ställdes följdfrågor och intervjuspecifika frågor som ej finns med i intervjuprotokollet.



Nodes

| Name | Sources | References |
|---|---|---|
| TPB | 0 | 0 |
| Perceived Control | 8 | 36 |
| Norms | 8 | 54 |
| Attitude | 8 | 47 |
| System Impact | 8 | 32 |
| Policy | 5 | 11 |
| Physical Security | 7 | 27 |
| Password | 5 | 16 |
| Other | 7 | 33 |
| Email | 3 | 19 |
| ISPA | 8 | 18 |
| Physical Security | 6 | 15 |
| Password | 7 | 18 |
| Other | 6 | 24 |
| Email | 6 | 34 |
| ISA | 8 | 44 |
| IDT | 7 | 22 |



Interviews

| Name | Nodes | References |
|---|---|---|
| K1 IT-Avdelning | 19 | 81 |
| K2 Övriga Avdelninagr | 27 | 67 |
| K3 Övriga Avdelningar | 26 | 75 |
| K4 IT-Avdelning | 20 | 57 |
| K5 Övriga Avdelningar | 28 | 69 |
| P1 IT-Avdelning | 18 | 86 |
| P2 Övriga Avdelningar | 30 | 85 |
| P3 Övriga Avdelningar | 27 | 64 |

**Figur 5. Klassificering av begrepp i NVivo 10**

**Figur 6. Intervjuer med tillhörande noder i NVivo 10**

## 3.9 Etik

IT-säkerhet är ett känsligt ämne. Om fel person får information om en organisations säkerhetshål kan det, som litteraturkaptilet förklarar, få fatala konsekvenser. Det är därför viktigt att alla organisationsnamn hålls dolda i uppsatsen. Att intervjua anställda om medvetenhet och policyefterföljning kan också vara känsligt eftersom svaren kanske inte är i linje med organisationens riktlinjer och krav. Vi vill inte att en anställds ska kunna råka illa ut som ett resultat av vår uppsats, därför har vi innan, under och efter intervjuerna förklarat att varken organisationsnamn eller namn på respondenter kommer nämnas i rapporten. Vid Face-To-Face intervjuerna skrev vi tillsammans med respondenten ett kontrakt för att försäkra båda parter om att informationen hålls konfidentiell (se Appendix II). Vid telefonintervjuerna gav vi ett muntligt löfte.

På organisationernas begäran döljs vilken specifik avdelning respondenterna tillhör eftersom det gör det omöjligt att härleda vem som sagt vad. Dock fick vi tillåtelse att använda oss av den generella termen IT-avdelning.

## 3.10 Reliabilitet och Validitet

Validitet och reliabilitet i en kvalitativ metodansats handlar om att kunna beskriva att man har samlat in och bearbetat data på ett genomtänkt och hederligt sätt. Det gäller således att man kontinuerligt arbetar med validiteten och reliabiliteten under hela projektet (Malterud, 1998). Förhoppningsvis visar den här uppsatsens metodkapitel på att validitet och reliabilitet har genomsyrat arbetets gång.

Vi har baserat samtliga intervjufrågor frågor utifrån vår omfattande litteraturstudie. Vi har lagt tid på att läsa om intervjuteknik för att förbättra våra förutsättningar till insamling av empiriska data. Vi har försökt vara objektiva i vår analys och inte låtit våra egna tankar färga resultatet. Vi har metodisk analyserat data och använt pålitliga verktyg vid inspelning, transkribering och kodning. Eftersom vår transkribering är välgjord kan läsaren själv avgöra om empirin är rätt tillämpad. Enligt Andersson (1994) lever inte de flesta som det lär. Men genom att försäkra respondenten om att allt som sägs är konfidentiellt resulterade det förhoppningsvis i ärliga svar vilket är avgörande för en uppsats med hög validitet och reliabilitet.

# 4 Empiri och resultatanalys

Empirikapitlet är uppdelat i underrubriker där vi hänvisar till vilka frågor i frågeformuläret som berör respektive underrubrik (se Appendix I). Vi ställer upp svaren ifrån IT-avdelningen mot övriga avdelningar löpande under varje rubrik. Vi försöker presentera och inte diskutera resultaten. Dock kan viss diskussion förekomma då svaren är kvalitativa och vår tolkning kan därför behöva förklaras.

| Organisation | Antal Anställda | Ort | Antal respondenter IT-Avdelning | Antal respondenter Övrig Avdelning |
|---|---|---|---|---|
| **Privat** | >1000 | Lund/Stockholm | 1 | 2 |
| **Kommunalt** | 60< <200 | Stockholm | 2 | 3 |

**Tabell 4. Organisationstabell.**

## 4.1 Medvetenhet - ISA

Frågor som berör den generella säkerhetsmedvetenheten, med hänsyn till IT-säkerhet, är frågor 3, 4, 5 och 16a i intervjuprotokollet. Dessa frågor gav en bild av de anställdas medvetenhet om SE, deras personliga medvetenhet samt deras uppfattning om den generella medvetenheten inom organisationerna.

#### *4.1.1.1 IT-avdelningar*

Inom IT-avdelningarna var medvetenheten om SE hög, då alla tre respondenter inom denna avdelning visste om vad det var och hade egna definitioner av det.

*”Jag vet om att det är ett av de enklaste, billigaste och mest effektiva sätten att penetrera ett säkerhetssystem.” (P1:IT)*

*”Det är egentligen att utnyttja det faktum att människor i grunden alltid vill hjälpa till. Och att folk generellt sätt är väldigt rädda att ifrågasätta saker och ting.” (K2:IT)*

*”Jag vet att det går att träna sin förmåga att påverka andra människor att göra som man vill.” (K4:IT)*

| IT-avdelningar | Anställd 1 | Anställd 2 |
|---|---|---|
| P | | |
| K | | |

Röd = Ej Medveten
Grön = Medveten
Grå = Anställd saknas

**Tabell 5. Visualisering av Fråga 3 IT-avdelningar - Vet du vad Social Engineering är?**

Svaren i fråga 4 och 16a tyder på att ISA inom IT-avdelningen är hög, då alla tre anställda ansåg sig som säkerhetsmedvetna. Vidare i empirin styrks detta påstående. IT-avdelningarna ansåg dock att den generella ISA inom organisationerna var låg och borde bli högre.

*"Jag kan nog säga att hela vägen ända från toppen hela vägen ner till botten så är medvetenheten väldigt dåligt, väldigt låg. " (K1:IT)*

*"Jag tror det är något lägre än vad jag skulle önska." (P1:IT)*

*"Jo men det är ett problem. Det skulle behöva bli bättre." (K4:IT)*

I svaren på fråga 5 framgick det att båda organisationerna ger sina anställda en introduktionsutbildning om IT och presenterar delar av de policy och rutindokument som finns uppsatta.

*"Ja, då har vi en introutbildning som är interaktiv. Om företaget, kärnvärden, processer, policys och sånt där. Säkerhetsbitarna ingår som ett block i dom. Så jag tror det är kring tjugo procent." (P1:IT)*

*Varje nyanställd på Företaget genomgår något som heter en IT-introduktion, med mig eller min kollega. Där vi helt enkelt berättar om våra IT-riktlinjer och våran IT-policy. Och hur företaget ser på IT-säkerhet när det gäller lösenordshantering, när det gäller personuppgifter, hur vi behandlar personuppgifter och hur våra IT-system fungerar. (K1:IT)*

#### 4.1.1.2 Övriga avdelningar

Genom intervjuerna framgick det genom fråga 3 (se Appendix I) att anställda inom de övriga avdelningarna hade låg medvetenhet om SE. Det var en anställd som delvis visste vad begreppet innebär och kunde ge en förklaring. De andra anställda visste inte vad det var.

*"Nej, den var ny." (K2:Ö)*

*"Nej jag tänker att det har med HR att göra." (P1:Ö)*

*"Social Engineering för mig, inte jättebekant med begreppet annat än att det handlar om att man genom att infiltrera företag få tillgång till information." (K5:Ö)*

*"Jag vet ingenting." (P2:Ö)*

| Övriga avdelningar | Anställd 1 | Anställd 2 | Anställd 3 |
|---|---|---|---|
| **P** | | | |
| **K** | | | |

Röd = Ej Medveten
Grön = Medveten
Grå = Anställd saknas

**Tabell 6. Visualisering av Fråga 3 Övriga avdelningar - Vet du vad Social Engineering är?**

Baserat på de anställdas svar på fråga 4 och 16a (se nedan samt Appendix I) pekar resultaten på att det finns någon sorts medvetenhet inom informationssäkerhet, främst inom företag K – där två av tre anställda hävdar att de har medvetenhet.

*”Ja men det skulle jag säga. Jag är ganska försiktig eller jag skulle säga att jag är väldigt försiktig.” (K2:Ö)*

*”Inte så säkerhetsmedveten skulle jag säga.” (K3:Ö)*

*” Jag tycker att jag är det, men jag tänker nog inte så mycket IT-säkerhet. Det har jag nog aldrig gjort.” (P2:Ö)*

Dock visar svaren även att den uppfattade generella ISA (fråga 16a i intervjuprotokollet) inom båda företagen är relativt låg och bör förbättras.

*” Jag tror inte man tänker så mycket på det.” (K3:Ö)*

*”Jag skulle nog säga såhär att vi nog är som de flesta företagen generellt. Kanske något mindre säkerhetsmedvetna än andra företag jag varit på.” (K5:Ö)*

*”Mina svar tyder ju ganska tydlig på att den inte är jättebra.” (P3:Ö)*

Svaren på fråga 5 (se Appendix I) tyder på låg utbildning om IT-säkerhet inom företagen. Alla tre anställda på företag K hade den grundutbildning inom IT som sker för nyanställda men inget utöver den. Den ena anställda på företag P hade ej fått någon utbildning alls inom IT-säkerhet medan den andra anställda menade på att det kommer information internt från IT-avdelningen. Detta var även något som en anställd från företag K också nämnde:

*“Då och då skickar ju IT mail om att öppna inte, nu figurerar det, nu är det i omlopp, nu har det kommit förbi våra brandväggar om Telias säkerhets-kod som du ska fylla i.” (P2:Ö)*

*“Vi får information internt, öppna inte mail och liknande. Den typen får vi då centralt från IT, service desk.” (K3:Ö)*

## 4.2 Medvetenhet - ISPA

Baserat på de intervjuer som gjorts i kombination med resultaten av intervjuerna från IT-avdelningarna visar empirin hur anställdas ISPA ser ut. Då vi ej haft tillgång till organisationernas aktuella policys är empirin baserad på de anställdas medvetenhet i jämförelse till IT-avdelningen. Då de intervjuade anställda inom IT-avdelningarna har varit delaktiga i framtagningen av IT-policys anser vi att deras ISPA blir en riktlinje för de ISP som företagen har.

Genom intervjuerna kunde flertalet ISP identifieras. Främst var det mail- och lösenordspolicys som var genomgående för de båda organisationerna. Även andra policys som berör fysisk säkerhet såsom hur anställda bör förhålla sig till molntjänster och rutiner för besökare kunde identifieras. Citaten nedan visar exempel på de policys som finns inom de båda organisationerna.

### *4.2.1 Mailpolicy*

Mail är en välkänd och riskfylld kanal för SE-attacker, främst risk för skadliga länkar eller spear-phishing mail. Dessa mail kan som sagt te sig normala eller trovärdiga, men när användaren öppnar mailet eller filen utsätts datorn för en attack (Ivaturi & Janczewski, 2011; Algarni et. al, 2014). Att skydda sig för dessa attacker, med bland annat policys, förespråkas av Durgin (2007) och menar även på att mail bör undvikas som kommunikationskanal för att skicka konfidentiell information.

Fråga 8b, 9, 13 och 13b i intervjuprotokollet behandlar mailpolicys och syftar främst undersöka om det finns policys om hur anställda ska agera vid phishing-attacker och malware-attacker genom mail.

#### *4.2.1.1 IT-avdelningar*

IT-avdelningarnas svar på dessa frågor visar på att båda företagen har mailpolicys angående potentiella phishing-mail eller annan skräppost samt policys för att inte skicka filer till varandra (fråga 12a, 12b, 12c i intervjuprotokollet).

> *”Vi föredrar om folk jobbar på intranäten och skickar en länk till varandra. Därför det drar minst kraft på e-postsystemet.” (P1:IT)*

> *”Där finns det rutin som hänger på våran IT-policy som säger det att du ska inte svara, du ska inte öppna mail från okänd avsändare och du ska iaktta stor försiktighet.” (K1:IT)*

> *”Och vi har även en rutin som säger att du får inte skicka känslig information över epost.” (K1:IT)*

> *”Alla kända former av webmail, hotmail, gmail och alla de där är spärrade numera. Vi kan inte leta upp alla världens epostservrar, men det står i IT-policyn att det låter du bli.” (P1:IT)*

> *” Är det inte relevant, bara radera det. Det är direkt uttalat och mycket påbjudet. För två-tre veckor sedan skickade vi ut det där fyra gånger om dagen på newsflash, att klicka inte på de här grejerna.”(P1:IT)*

#### 4.2.1.2 Övriga avdelningar

Svaren visar på att det inte är helt tydligt hur de anställda ska agera ifall de får ett okänt mail, och att fyra av fem intervjuade inte visste om det fanns några fastställda policys. Vid frågan om de fick använda sin privata mail (fråga 13a, 13b) var alla fem intervjuade osäkra eller kunde inte svara på ifall det fanns policys. Dock påpekade två anställda på båda företagen att de fått information via mail om hur de ska agera gentemot spam-mail eller andra okända mail.

> *”Där får vi faktiskt ut varje gång vi får ett sånt mail så får vi ett extramail från service desk. Där skriver de att "nu har det kommit ut mail som ser ut såhär, radera dem och tryck ingenstans" (P3:Ö)*

> *”Eller vad gäller IT-säkerheten i mail får vi ju såna uppmaningar att känner du inte igen avsändaren ska du såklart inte öppna det där. De här brukar vara spam så att öppna inte de här.” (K3:Ö)*

I svar på frågorna om hur filer skickas (12a, 12b & 12c i intervjuprotokollet) framkom det, trots ovan nämnda policys emot det, att konfidentiell information och andra känsliga uppgifter skickas via mail.

> *Men ingen känslig information. Inte information som är arbetsinternt arbetsmaterial. Sånt skickar vi via epost till varandra. (K3:Ö)*

> *”Sen har vi mail, väldigt mycket mail förstås. Det i sin tur är ju rätt vanskligt, du kan ju bara skriva fel och så går det till fel person. Nej det är väl så man delar information.” (K5:Ö)*

> *”Via mail. Man kan också lägga upp filer i intranätet. Men mest mail.” (P3:Ö)*

### 4.2.2 Lösenordspolicy

Fråga 10a, 10b och 10c i intervjuprotokollet behandlar lösenordspolicys. Genom dessa frågor ges en bra bild av hur lösenordshanteringen ser ut inom de båda företagen och ifall det finns riktlinjer för lösenordens styrka, om de byts kontinuerligt samt hur anställda följer dessa. Lösenordspolicys kan förhindra att en eventuell förövare lätt kommer åt eller kan gissa sig till anställdas lösenord baserad på insamlad information om offret (Durgin, 2007).

#### 4.2.2.1 IT-avdelningar

Genom intervjuerna med IT-avdelningarna framgick det att båda företagen hade lösenordspolicys i form av styrka och delning av lösenord. P hade även kontinuerligt byte av lösenorden.

> *”Riktlinjerna är 8 tecken, stora små bokstäver, siffror, specialtecken. Lösenordet får inte innehålla namn på vare sig husdjur, flickvän eller ett ord som du kan slå upp i ett europeiskt ordbok”(K1: IT)*

> *”Det är uttalat att lösenorden ska bytas på 90-dagars basis. Sedan finns där 8 kriterier för hur de ska vara konstruerade……blandade tecken.” (P1:IT)*

> *”Det ingår i såfall i it-säkerhetspolicyn. Att du lämnar inte ut ditt lösenord.” (P1:IT)*

*”Ja i direkt strid mot policyn. Vi får inte lov att skriva ner dom. Men åt andra sidan, kräver man att man skapar väldigt svåra lösenord är det ingen som kommer ihåg dom.” (P1:IT)*

#### 4.2.2.2 Övriga avdelningar

Svaren på fråga 10a och 10b i intervjuprotokollet visade på tvetydighet bland respondenterna. Svaren visade dock på att det finns rutiner för lösenord, men att medvetenheten om vilka specifika rutiner var ojämn.

*”Ja det kommer ju med automatik att "nu är det dags att byta lösenord". Var tredje månad eller nåt sånt. Sen ska det vara lite konstiga tecken och sådär.” (P2:Ö)*

*”Innan så har det inte funnits någon lösenordsspärr egentligen, ingen liksom X antal tecken eller så. Men i den nya versionen var det ju pang på, det skulle vara stora, små bokstäver, siffror, specialtecken, minst åtta tecken.” (K2:Ö)*

*”Nej eller bytt har vi gjort. Skriver man fel tre gånger så låser man hela kontot. Så man byter ju ganska ofta just för att folk skriver fel. Så det ligger väl ingen rutin i det riktigt. Sen svårighetsgrad, det ligger väl ingen rutin där heller.” (P3:Ö)*

*”Ja det finns rutiner. Jag kan inte påstå att jag kan dem utantill, men jag vet att när jag började här fick jag riktlinjer. Jag tror att det ska vara både gemener och versaler och siffror.” (K5:Ö)*

Något som däremot svaren på fråga 10c i intervjuprotokollet visade var att anställda från båda företagen skrev ned sina lösenord för att komma ihåg dem. Detta är även något som Kelley (2006) också menar på, att för strikta lösenordspolicys kan leda till att anställda skriver ned eller delar med sig av sina lösenord. Detta är givetvis ett potentiellt säkerhetshål för SE-attacker.

*”Men dom är uppskrivna i min pärm som står här nånstans.” (P2:Ö)*

*”Jag har oftast samma men annars har jag det uppskrivet i ett block.” (P3:Ö)*

*”Och så har jag en liten lista någonstans för jag kommer inte ihåg exakt vilken det är jag har på olika. ” (K3:Ö)*

### 4.2.3 Fysisk säkerhetspolicy

Durgin (2007) diskuterar som tidigare nämnt vikten av att ha fysiska säkerhetspolicys. Detta kan till exempel vara spärrar för att obehöriga ej ska kunna ta sig in i lokalerna, men även annan fysisk säkerhet som hantering av privata enheter som till exempel USB-minnen, telefoner och egna datorer. Policys kring detta skapar en säkrare miljö ur ett SE-perspektiv då det försvårar för förövaren att ta sig in i både lokaler och system. Fråga 7,8a och 11a i intervjuprotokollet behandlar dessa frågor.

#### 4.2.3.1 IT-avdelningar

Fysiska säkerhetspolicys i form av riktlinjer för hur okända människor ska bemötas och fastighetsskydd som fråga 7 och 8a behandlar kunde identifieras inom båda företagen.

*”Alla ska registrera sin ankomst på en terminal där nere, innan dom passerar in genom dörren.” (K1:IT)*

*”Ser man en person som går lös, som inte har en bricka eller liknande och inte vallas, så är det påbjudet att fråga vederbörande vem han ska besöka. Och leda honom dit, alternativt leda honom ut.” (P1:IT)*

*”Men däremot har vi rutinändring, en rutinskärpning där man ska komma ner och hämta sina besökare och lämna av dom där nere.” (K1:IT)*

Vid frågor om privata enheter kunde endast policys inom P identifieras angående USB-minnen. Inom K fick privata enheter användas till arbetsuppgifter, dock ej kopplas upp på företagets nätverk.

*”Ja, ja. Det har kommit på senare tid det där. Du ska inte ansluta privata diskar till jobbenheter eftersom det innebär säkerhetsrisker.” (P1:IT)*

#### 4.2.3.2 Övriga avdelningar

Fråga 7 och 8a som behandlar fysiska säkerhetspolicys gentemot okända personer visade på att båda företagen hade skydd mot att obehöriga tog sig in i lokalerna i form av passerkort eller portkod. Dock var det även vid denna fråga otydligt ifall de anställda hade fått direkta direktiv hur de ska agera i form av en policy eller riktlinjer ifall de stöter på någon de inte känner igen.

*”Nej inga riktlinjer, det är väl mer jag som person som får lösa det tänkte jag säga.” (P3:Ö)*

*”Nej det finns inga riktlinjer utöver att jag vet hur jag ska bete mig eftersom jag råkat ut för det några gånger.” (K5:Ö)*

*”Ja men man ska säga åt dom direkt. Man skrivs in och får en badge.” (P2:Ö)*

*”Ja, ingen kan ju komma in om man inte har ett passerkort. Och kundtjänst har uppmanats att inte öppna till någon.” (K3:Ö)*

Även fråga 11a behandlar fysisk säkerhetspolicy i form av privata enheter och att ta med sig datorn hem att arbeta. Svaren visade på att anställda inom båda företagen inte var medvetna om några specifika policys angående externa enheter som mobiltelefoner och USB-minnen. Däremot fanns en större medvetenhet om att arbeta hemifrån i specifika mjukvaruportaler.

*“Får vet jag inte, jag tror inte man kommer åt programmen riktigt. Men jag vet inte.” (P3:Ö)*

*“Det borde jag veta förstås, får man det eller får man inte. Jag kan inte svara på om man får eller inte, jag kan inte svara på det. Jag passar på den. Däremot att det är hemmamiljö tex. att använda sin hemdator för att via Citrix åka in är fullt möjligt då.” (K5:Ö)*

*"Ja har aldrig tänkt på det riktigt. Men det händer att jag tar ett USB och kopierar filer jag behöver jobba med och så tar jag hem den och stoppar in min dator hemma. Sen tar jag med mig USB:t tillbaka till jobbet sen. Men jag får säkert inte göra det." (P2:Ö)*

### 4.2.4 Övriga policys

Frågorna 8c, 11b, 14-15 samt 18 i intervjuprotokollet behandlar övriga policys som internet, telefon och cloudbaserad lagring. Telefon- och samtalpolicys kan motverka SE-attacker där förövaren försöker få tillgång till information över telefon (Durgin, 2007; Ivanturi & Janczewski, 2011). Även internetpolicys och cloudbaserad lagring ökar säkerheten inom företaget då risken att en förövare lyckas med till exempel en malware-attack begränsas på grund utav spärrar.

#### 4.2.4.1 IT-avdelningar

Policys som förbjuder cloudbaserad lagring och policys som berör vad som får besökas på internet fanns också inom båda organisationer. Dock är en potentiell riskfaktor att båda organisationer saknar policys om hur anställda bör agera i telefonkommunikation.

*"Skriven nej." (P1:IT)"*

*"Men inte generellt om någon ringer. Inte som jag känner till. Det kan finnas att vi har riktlinjer för telefonsidan som jag inte känner till." (K1:IT)*

#### 4.2.4.2 Övriga avdelningar

Fråga 8c, som behandlar telefonpolicys, visade på att samtliga anställda var osäkra på om det fanns policys om detta, ingen hade heller fått riktlinjer kring hur de ska agera vid ett okänt telefonsamtal. Detta beror med största sannolikhet på att det inte finns några telefonpolicys inom något av företagen. Även fråga 14 om Cloud-policys och fråga 15 om internet-spärrar visar på en osäkerhet kring vad som är tillåtet och inte tillåtet.

*"Nej. Jag har inga riktlinjer." (P3:Ö)*

*"Nej, jag är lite skeptisk. Eller jag förstår inte det där. Så nej det gör jag inte." (K2:Ö)*

*"Dropbox använder vi ibland för bilder, det gör vi." (K3:Ö)*

### 4.2.5 Policyansvar

#### 4.2.5.1 IT-avdelning och Övriga avdelningar

LeVeque (2006) menar att en god policy ska ställa krav på användarna i hur de ska agera och vad de ska undvika att göra. Policyn ska även förklara vilken information som är viktig för organisationen, hur den ska skyddas och även varför den ska skyddas. (Al-Omari et al., 2011; Gollmann, 2011) Även specifika ansvarsområden ska identifieras och delas ut inom organisationen genom ISP (LeVeque, 2006). Det som framgick genom intervjuerna var att P har någon slags ansvarsfördelning till avdelningschefer angående policys medans K verkar inte ha det. I

intervjuerna framgick dock inga specifika ansvarsroller eller riktlinjer för rollerna genom ISP, utöver det centraliserade ansvaret på IT-avdelningen.

*”Varje avdelningschef har ju då ett ansvar utöver medarbetarnas att se till att medarbetarna förstår säkerhetspolicyn.” (P1:IT)*

*”Vi har ju policydokument, rutindokument och dom förväntas man ju som tjänsteman ta del av och läsa. ”(K4:IT)*

*”Ja ja ja, alltså vår it-avdelning är ju insatta i det vet jag.” (K3:Ö)*

### *4.2.6 Tillgänglighet och handlingsplan*

Fråga 17 och 18 i intervjuprotokollet undersöker om policys finns tillgängliga för anställda och hur de ska agera ifall de skulle utsättas för en SE-attack.

#### *4.2.6.1 IT-avdelningar*

Båda organisationerna hade en antydan till handlingsplan om anställda skulle råka ut för en eventuell attack.

*I korthet. Dra ut nätverkskontakten, dra ut strömmen, leverera datorn till [namn på avdelning], gå och ställ dig i hörnet. (P1:IT)*

*”Om man misstänker att nånting är galet så ska man kontakta IT-avdelningen eller [namn på avdelning] och meddela det.” (K1:IT)*

I intervjuerna med IT-avdelningarna framgick det att båda organisationerna lagrade sina policys på intranätet men även skickade ut mail vid specifika händelser som till exempel phishing-mail i omlopp.

#### *4.2.6.2 Övriga avdelningar*

Fråga 17 och 18 behandlar hur de anställda kommer åt policys och hur de ska agera ifall de blivit utsatta för en attack. De båda anställda på P visste om hur handlingsplanen såg ut:

*”Ja det gör det. Först blir man lite röd i ansiktet och sen så rycker jag ut sladden och slår av datorn. Och sen ringer jag till IT-servicen.” (P2:Ö)*

*”Vi får utskickade mail från servicedesk då där det står att man ska kontakta dom och stänga av datorn så fort du kan.” (P3:Ö)*

Inom K var det mer ovetande om det fanns någon handlingsplan vid en eventuell attack, men två av tre anställda skulle kontakta IT-avdelningen.

*“Det kan vara så att man ska tala om det för våran IT-avdelning.“(K2:Ö)*

*“Det gör det säkert, jag vet inte hur den ser ut. Men det finns säkert. Och det är väl kanske mitt ansvar som medarbetare att veta det, men jag vet faktiskt inte riktigt.” (K3:Ö)*

*“Jag skulle göra såhär om jag råkade ut för några tokigheter, jag skulle faktiskt gå till [namn] och säga "Vad sjutton gör jag nu?".” (K5:Ö)*

När det kommer till tillgängligheten av IT-policys visade resultaten att anställda inom båda organisationerna var osäkra på var de fanns.

*”Vet inte, jag har verkligen inte en aning. Det är ingenting jag har tagit del av. Det finns ju säkert någonstans. Men det är dålig info om det. Jag tror inte många har tagit del av det.” (P3:Ö)*

*”Ja det kommer som ett mail. På intranätet är det lurigt för det är mycket som man måste öppna upp och leta efter.” (P2:Ö)*

*”… Men jag har inte sett någon ren IT-policy som jag kan minnas att jag har varit med om att ta något beslut eller arbeta fram faktiskt.” (K5:Ö)*

*”Jo alltså företaget har ju en massa policys och rutiner och så vidare. Och dem vet jag vart de finns, absolut. Men sen om jag tycker att den...ja jag har väl inte stenhårt läst igenom den.” (K2:Ö)*

*”De finns på it-rummet på intranätet. Jag har inte läst de senaste versionerna men jag vet att de finns där.” (K3:Ö)*

## 4.3 ISP baserad på ISPA

Baserat på intervjuerna har således flertalet policys eller riktlinjer identifierats, presenterat i tabellen nedan. Tabellen visar vilka områden som täcks av de båda företagens policys utifrån IT-avdelningarnas svar. Då IT-avdelningarna inom de båda företagen har delaktiga i policyarbetet för företaget anses deras svar som pålitliga kring vilka policys som finns tillgängliga. De övriga avdelningarnas medvetenhet kring identifierade policys har även visualiserats i tabell 7 och 8 för att ge en överblick och jämförelse mellan avdelningarna.

*IT-avdelningar*

| ISP inom organisation | Mail | Lösenord | Fysisk säkerhet | Cloud-tjänster | Internet | Telefoni |
|---|---|---|---|---|---|---|
| **P** | | | | | | |
| **K** | | | | | | |

Röd = Ej Medveten
Gul = Delvis medveten
Grön = Medveten

**Tabell 7. Identifierade ISP inom organsisationerna**

### *4.3.1 Övriga avdelningar*

| ISP inom organisation | Mail | Lösenord | Fysisk säkerhet | Cloud-tjänster | Internet | Telefoni |
|---|---|---|---|---|---|---|
| **P** | | | | | | |
| **K** | | | | | | |

Röd = Ej Medveten
Gul = Delvis medveten
Grön = Medveten

**Tabell 8. ISPA visualiserad inom organisationerna**

## 4.4 Socialpsykologiska faktorer

Baserat på intervjuerna har svar kopplade till socialpsykologiska faktorer som företagsnorm, attityd, kontroll och deception identifierats. Många av dessa frågor är följdsvar som ett resultat av en semi-strukturerad intervju, men kan i grunden kopplas till de frågor som är beskrivna i intervjuprotokollet (dessa frågor är fråga 5, 8, 10-14, 16 samt 19 i intervjuprotokollet).

### *4.4.1 Attityd*

Den attityd en anställd har gentemot ISP är korrelerad till dess generella attityd. Är det ogynnsamt för den anställde i form av tid eller andra faktorer att följa ISP kan denne således avvika från policyn, trots hög ISPA (Bulgurcu et al., 2010).

#### *4.4.1.1 IT-avdelningar*

Inom IT-avdelningarna visade svaren på en hög medvetenhet och säkerhetsfrämjande attityd.

*”Jag skickar aldrig personuppgifter, jag skickar aldrig lösenord över epost. Epost är som att skicka ett vykort. Vem som helst kan läsa det, vem om helst kan sniffa upp det på vägen.” (K1:IT)*

*”Vi utgår ju ifrån att elektronisk kommunikation, utgår vi ifrån att den är komprometterad, men vi gör sen bedömningen att inte är säkerhetsinformation.... ” (K4:IT)*

*”Därför när någon ringer och vill ha ett lösenord så måste jag verifiera att den personen är den den utger sig för att vara.” (P1:IT)*

#### *4.4.1.2 Övriga avdelningar*

Inom övriga avdelningar inom båda organisationerna återfanns en osäker attityd, bland annat inom lösenordspolicyn då tre av fem intervjuade inom övriga avdelningar hade skrivit ned lösenorden. Andra tendenser på policyavvikande attityd identifierades:

*”Nu ska erkänna att de här mailen, jag skickar inte dem till honom längre. I början gjorde jag det, men numera sparar jag dem bara så att de finns kvar.” (K5:Ö)*

*”IT vet jag...det kommer jag ihåg att det var någon på it som sa det att "när du går ut ur ditt rum så ska du låsa datorn.". Nu gör jag inte det, men jag borde väl det.” (K3:Ö)*

*”Jag har inte tid att sitta och sortera på offerter med diarienummer. Jag slänger iväg offerter via mail och lägger dem i en bunt på bordet 20-30 offerter som jag borde sorterat. Det gör jag ibland när jag har tid, men det är sällan. ” (P2:Ö)*

*”Jag väljer ju mina tillfällen när...ibland stänger jag till dörren. Det är inte alltid jag låser den” (K2:Ö)*

*”Har väl hänt att man skickat en faktura eller ett avtal som inte är så bra att vifta med. Men det sker inte så ofta.” (P3:Ö)*

### 4.4.2 Subjektiv Norm

Normen är den andra faktorn i TPB som denna uppsats tittar närmre på. I relation till intervjuerna kunde även ett flertal normer urskiljas eller tolkas.

#### 4.4.2.1 IT-avdelningar

IT-avdelningarna inom de båda organisationerna menade på att normen inte främjar ett säkert och säkerhetsmedvetet arbetssätt. Detta är något som både P och K påpekade.

*”Vi har alldeles för mycket folk för att kunna dra sig undan genomsnittstandarden på en befolkning. Sen är det bara att mäta in dom fem procent idioter och 10 procent träskallar och resten kan sitt jobb så att säga.” (P1:IT)*

*”Folk tar alltid den lätta vägen. Om något är lite bökigt väljer man alltid den lätta. Tyvärr. Så det är vår uppgift att göra det lätt att göra det säkert.”(K1:IT)*

*”Jag brukar säga att vi har en ganska snäll kultur, eller för godtrogen kultur här i bolaget.” (K4:IT)*

#### 4.4.2.2 Övriga avdelningar

Som svar på intervjufrågor och följdfrågor tyder svaren på, likt IT-avdelningarna påpekade, att den generella normen inom de båda organisationernas övriga avdelningar inte har högt fokus på säkerhet.

*”Eller folk är nog lite slappa på det. Jag tror inte folk är jättemedvetna om it-säkerhet här.” (P2:Ö)*

*”Det är ofta att man går förbi folk och tänker "Ja där är någon som inte verkar vara på plats längre, men ändå står datorn helt öppen" och så vidare. Så jag tror att det är en ganska stor variation på IT-tänket och säkerhetstänket”. (K2:Ö)*

*”Man har information men hur man hanterar den det pratar man sällan om, utan det sprids nog liksom. Otrogen informationshantering generellt inom bolaget.” (K5:Ö)*

### 4.4.3 Upplevd Kontroll

Uppfattad kontroll är den tredje faktorn i TPB som är starkt korrelerad till ISA i detta kapitel. Anställda med hög ISA och ISPA är mer benägna att följa de riktlinjer som satts upp då de är mer säkra i hur de ska agera (Diney & Hu, 2007).

#### 4.4.3.1 IT-avdelningar

IT-avdelningarna stödjer det faktum att anställda behöver mer utbildning och att det är det bästa sättet för anställda att skapa högre kontroll vilket resulterar i högre policy-efterföljning.

*”Antingen sitter du bara med på tåget och åker med och du kan inte påverka nånting, eller så är du med och styr det där tåget. Kunskap resulterar i att du kan vara med och styra.” (K1:IT)*

*”Utbildningen. Utbildningar och learning by burning. Det vill säga när folk har suttit och gjort någon grej då, dom tappar kanske den dagens produktion och måste läsa gårdagens backup. Då lär man sig. ” (P1:IT)*

#### 4.4.3.2 Övriga avdelningar

De övriga avdelningarna menade på att de önskade att bli mer medvetna inom IT-säkerhet och uttryckte även dem att det borde finnas mer utbildning internt om detta område.

*”Det borde... Det finns ju en massa info, men vi får ingen utbildning, det fastnar liksom inte. Det är en sak att läsa. Hur vet man att det fastnar?” (P2:Ö)*

*”Alltså helt ärligt har jag inte reflekterat så mycket kring det. Men det är ganska självklart att man måste få nån slags kurs kanske, hur man ska bete sig och sådär, hur man ska agera och sånt. Någon utbildning om det borde finnas tycker jag.” (P3:Ö)*

*”Nej men att man...jag tänker att som min roll i företaget eller överhuvudtaget som en anställd i företaget så kanske man behöver få nys om det lite oftare. Att man tar upp det vid olika tillfällen att tänk på det här. Man kanske också behöver exempel, att det här har hänt. Någon gjorde såhär och då läckte informationen hit.”(K2:Ö)*

*”Vi har ju utbildningar som alla i företaget går med jämna mellanrum av olika karaktärer. Man kan ju väva in pass, vi talar om 15-20 minuter innan ett utbildningsblock så väver man in den typen av frågeställningar som man pratar om.” (K5:Ö)*

### 4.4.4 Deception

Deception är kopplat till IDT och är en faktor till varför människor blir lurade. Det främsta målet är att manipulera mottagaren utan att bli upptäckt, för att på så sätt lyckas komma åt den information förövaren är ute efter (Moffitt, 2009).

#### 4.4.4.1 IT-avdelningar

Inom IT-avdelningen var säkerhetsmedveten hög, men detta till trots uttrycktes det att det fanns möjligheter att falla offer för en SE-attack. Vid frågan om hur säkerhetsmedveten en anställd inom IT-avdelningen var tydde svaret på att deception skulle kunna vara en faktor och spela in vid en lyckad SE-attack.

*”Jag tror jag ligger högt på listan. Sedan kan det finnas faktorer som jag inte känner till som gör att jag blir oförsiktig.” (P1:IT)*

#### 4.4.4.2 Övriga avdelningar

Citaten nedan visar också på osäkerhet kring riktlinjer och ISA vilket öppnar upp riskerna för en lyckad impersonation- eller annan SE-attack som spelar på deception.

*”Någon kan ju fejka att vara mig eller jobba på företaget. Eftersom vi är ett seriöst och stort företag tror ju folk att det är jag såklart.” (P2:Ö)*

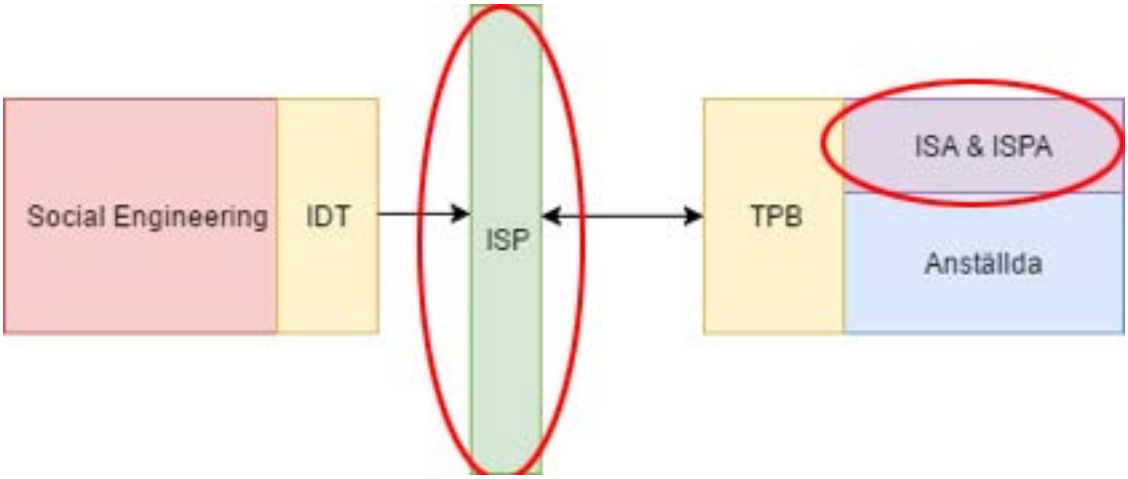
*”Jag är inte säker på, faktiskt, den avdelningen ligger ju under mig, hur man skulle agera här nere i receptionen om någon skulle komma in och fråga. Jag hoppas verkligen att vi, jag ska kolla det, att vi har rutiner för det här i huset. Att man inte låter vem som helst komma åt..” (K5:Ö)*

# 5 Diskussion

Syftet med den här uppsatsen är att undersöka hur IT-säkerhetsmedvetna anställda är med fokus på SE. Med hjälp av det teoretiska ramverket i kap. 2 och resultaten från de intervjuer som gjorts ska vi i detta kapitel diskutera likheter och skillnader mellan IT-avdelningar och övriga avdelningars IT-säkerhetsmedvetenhet, vad omedvetenhet kan få för konsekvenser och varför IT-säkerhetsmedvetenheten ser ut som den gör. Den frågeställning som ämnas besvara lyder:

*Hur ser IT-säkerhetsmedvetenheten, med fokus på social engineering, ut på IT-avdelningar respektive övriga avdelningar inom medelstora / stora organisationer?*

## 5.1 Medvetenhet




**Figur 7. Medvetenhet inom organisationerna**

### *5.1.1 ISA*

Utifrån empirin kan vi utläsa att IT-avdelningen har en hög IT-säkerhetsmedvetenhet, både generellt och inom SE. De har hög medvetenhet om organisationens policys, att SE är ett stort hot och hur man ska agera vid en eventuell attack. Det är således naturligt att samtliga på IT-avdelningarna ansåg sig själva vara säkerhetsmedvetna. Det är i enlighet med teorin där Bulgurcu et al. (2010) menar att erfarenhet inom IT också ökar IT-säkerhetsmedvetenheten. Litteraturen tyder på att störst resurser läggs på övrig IT-säkerhet medan säkerhet gällande SE kommer i andra hand (Warkentin & Willison, 2009). Vi trodde därför att IT-avdelningarna inte skulle ha så bra medvetenhet om SE som empirin visar.

Empirin tyder däremot på att övriga avdelningars IT-säkerhetsmedvetenhet är betydligt sämre än IT-avdelningarnas. Det gäller i synnerhet medvetenhet om SE. Övriga avdelningar hade låg medvetenhet om IT-säkerhetspolicys, hur de skulle agera vid attacker eller situationer som en SE-förövare utnyttjar.

Kontrasten mellan IT-avdelningars IT-säkerhetsmedvetenhet och övriga avdelningars är således stor. Som teorin förklarar är organisationers säkerhetsskydd inte starkare än sin svagaste länk, det stämmer speciellt i synnerhet till SE (Hauser, 2016; Bulgurcu et al. 2010; Ivaturi et al. 2014). Även om IT-avdelningarna har hög IT-säkerhetsmedvetenhet hjälper det föga om övriga avdelningars IT-säkerhetsmedvetenhet är låg, eftersom en SE-förövare attackerar organisationer där de är som mest sårbara (Ivaturi et al. 2014). Båda organisationerna i denna uppsats är således dåligt skyddade emot en SE-attack.

Om exempelvis en SE-förövare skulle lyckas ta sig in i K och P's lokaler skulle lösenord enkelt kunna hittas. En SE-förövare skulle även kunna, med lite förundersökning, attackera övriga avdelningar med spear phishing- och vishing-attacker. Detta eftersom övriga avdelningar inte tycks veta hur de ska agera i situationer där mail och samtal kommer från till synes legitima avsändare. Det är självklart alltid svårt att skydda sig mot den typen av attacker men utifrån empirin kan vi se att det inte finns en antydan till eftertänksamhet hos flera från de övriga avdelningar. ISA är inget som är naturligt för de anställda på övriga avdelningar, vilket är ett säkerhetshål med hänsyn till SE. Då en del av SE är att spela på deception och försöka lura sig till information kan det vara synnerligen svårt att upptäcka en sådan attack om anställda inte ofta blir påminda om IT-säkerhet (Ivanturi & Janczewski, 2011). Framför allt när de anställda ej vet om begreppet SE eller fått information om detta blir den potentiella risken för en lyckad SE-attack allt större. Eftersom samtliga respondenter har beslutsansvar och kan via sina informationssystem själva ta beslut som kan innebära stora kostnader för organisationerna (svaren på fråga 2 i intervjuprotokollet) är det extra intressant att betona den låga IT-säkerhetsmedvetenheten.

### *5.1.2 ISPA*

Det fanns en viss grad av ISPA inom övriga avdelningar men i förhållande till IT-avdelningarnas ISPA var den bristfällig. Övriga avdelningar skrev ner sina lösenord, skickade konfidentiella filer via mail och var allmänt okunniga om policys som ämnar skydda organisationen emot SE-attacker.

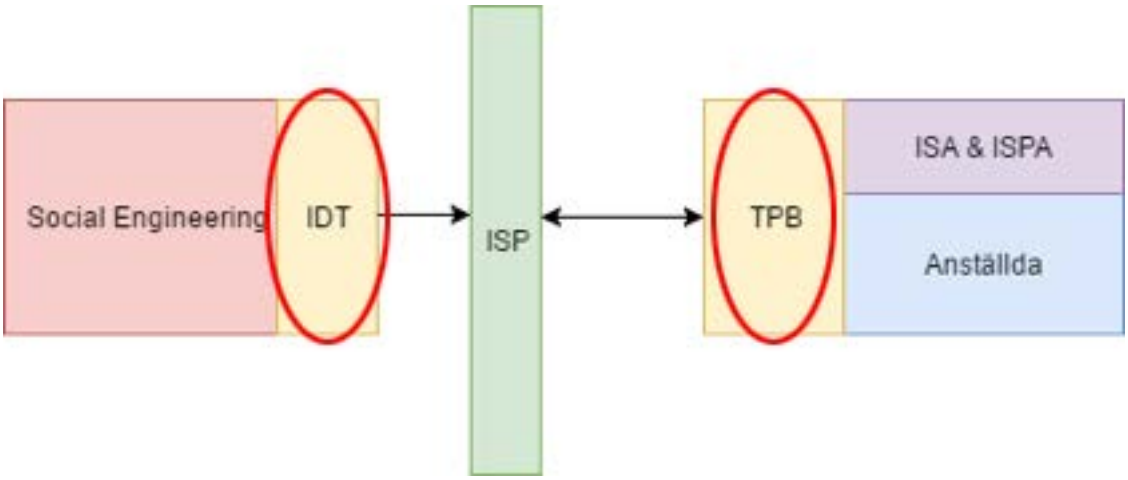
Den generella medvetenheten kring policys tyder på att de anställda inte fått någon vidare utbildning inom området. Anställda menar även på att de inte läst de policys som finns tillgängliga. Bulgurcu et al. (2010) menar på att användarna måste ha motivation för att vilja följa policys. Detta är något som verkar saknas, då anställda inom övriga avdelningar menade på att även om de visste om var policys fanns hade de inte läst dem. Även Al-Omari et al. (2011) menar på att uppföljning och kontroll av policyefterföljning är en brist inom många organisationer. Detta är något som även studiens resultat tyder på, framför allt med hänsyn till SE-attacker. De båda företagen är delvis skyddade mot Person-Person attacker då det fanns en del uttalade rutiner gentemot okända personer, medan avsaknad av telefonpolicys och låg medvetenhet kring generella ISP visar på potentiella säkerhetshål för exempelvis vishing och spear-phishing-attacker.

Svaren tyder på en medvetenhet om att anställdas beteende inte är helt enligt policys eller rutiner, men som Bulgurcu et al. (2010) diskuterar visar det på en attityd där effektivitet går

före säkerhetstänk och rutiner. Detta är även något som empirin för de övriga avdelningarna tyder på. Anställda är bekväma i redan etablerade arbetssätt, som att maila sina filer, vilket gör att beteendet i så fall måste ändras för att följa policys. Ingen av organisationerna hade heller konsekvenser vid brytande av policys, vilket kan göra att anställda inte ser riskerna med att inte följa policys. Då denna attityd och beteende inte heller resulterat i dataintrång eller andra konsekvenser kan det vara svårt för de anställda att inse vikten av säkra arbetssätt.

Kelley (2006) menar på att för hårda policys dock kan leda till motsatt effekt, som till exempel att anställda skriver ned sina lösenord. Att anställda skrev ned sina lösenord var genomgående inom övriga avdelningar i båda organisationerna, dock var de anställda endast delvis medvetna om de lösenordspolicys som fanns inom företaget. Alltså kan Kelleys (2006) påstående inte styrkas, utan beteendet verkar istället vara kopplat till den norm och attityd som finns inom organisationerna.

## 5.2 Socialpsykologiska faktorer




**Figur 8. Socialpsykologiska faktorer**

### *5.2.1 Attityd*

Svaren tyder på en medvetenhet om att anställdas beteende inte är helt enligt policy eller rutiner, men som Bulgurcu et al. (2010) diskuterar visar det på en attityd där effektivitet går före säkerhetstänk och rutiner. Attityden är att man vill jobba som man alltid gjort. Inkorporeras svåra steg i att arbeta säkert blir det jobbigare för anställda att utföra sina arbetsuppgifter, vilket gör att man hellre använder osäkra arbetssätt.

Då IT-avdelningens attityd främjar ett säkert beteende, bör denna attityd även spridas till övriga avdelningar. Det framgick i interjvuerna att det finns ett motstånd till mer komplicerade och säkra arbetssätt, vilket är en attityd som blir en utmaning för organisationerna att ändra på.

### 5.2.2 Subjektiv Norm

Enligt TPB är även normen något som påverkar det beteende gentemot ISP som anställda uppvisar (Bulgurcu et al. 2010). Normen inom övriga avdelningar tyder på att anställda inte tänker på IT-säkerhet och känner sig trygga inom organisationens ramar. Det är dock en falsk trygghet som kan leda till oönskade konsekvenser då en simpel knapptryckning kan släppa in en förövare i systemen (Durgin, 2007). Som Bulgurcu et al (2010) diskuterar pekar dock resultaten på att normen i stor del påverkar anställdas beteende. Svaren visade på att de anställda inom övriga avdelningar inte jobbade på säkra sätt, och att de inte heller trodde att andra anställda gjorde det. En norm där IT-säkerhet diskuteras och främjas bör bidra till att både normen och attityden hos anställda förbättras. Som tidigare studier visar (Bulgurcu et al. 2010; Al-Omari et al. 2011) är utbildning och efterföljning två nyckelfaktorer för att skapa motivation och medvetenhet.

### 5.2.3 Upplevd kontroll

De anställdas upplevda kontroll är också en faktor som påverkas av hur utbildade och medvetna de anställda är (Kranz & Haeussinger, 2014). Då de anställda inom IT-avdelningarna är välutbildade inom IT-säkerhet anses deras kontroll även vara hög. Detta innebär att de är medvetna om de risker som finns, men också hur de ska agera för att minska dessa. Inom övriga avdelningar visade empirin på en stor osäkerhet i hur de skulle agera i olika situationer, kring IT-säkerhet i allmänhet och vilka policys som organisationerna hade. Som ett resultat av låg utbildning och medvetenhet blir även den upplevda kontrollen låg, vilket i sin tur öppnar upp för sårbarhet för SE-attacker. Kontrollen skulle i sin tur kunna bli högre ifall normen inom företaget blev att vara mer säkerhetsmedveten.

### 5.2.4 Deception

Deception i form av SE-attacker är något som påverkas av alla ovanstående faktorer. Då den generella normen, kontrollen och attityden ej främjar säkerhetsmedvetenhet inom övriga avdelningar är således risken större för att deception ej upptäcks vid exempelvis ett spear-phishing-mail. Då en eventuell förövare spelar på kontexten för att tillskansa sig information eller annan känslig data (Ivaturi & Janczewski, 2012), finns det även risk att IT-avdelningen kan drabbas. Det är således mycket viktigt för organisationerna att öka medvetenheten överlag för att kunna upptäcka och genomskåda deceptiva meddelanden över exempelvis mail och telefon.

## 5.3 Reliabilitet och validitet

Reliabilitet avser huruvida forskningsresultat är upprepningsbara (Alvehus, 2013). Det som talar för att undersökningen är pålitlig är att resultaten verkar oberoende av organisationssektor, bransch och storlek. Det vill säga att svaren har sett mer eller mindre likadana ut respektive IT-avdelning och övriga avdelningar. Det tyder på att liknande resultat bör uppnås vid en oberoende undersökning med samma mätinstrument. Det som talar emot uppsatsens reliabilitet är att antalet respondenter är lågt.

## 5.4 Sammanfattande diskussion

Sammanfattningsvis syns det en tydlig skillnad mellan IT-avdelningarna och övriga avdelningar. För att få en mer organisationsomspännande säkerhet gentemot hoten presenterade i uppsatsen bör övriga- och IT-avdelningarna länkas samman bättre. Baserat på IDT och TPB.

Som flera andra författare hävdar (Bulgurcu et al. 2010; D'Arcy et al. 2009; Al-Omari et al. 2011) är utbildning det bästa sättet att öka medvetenhet inom organisationerna. Det är även något som styrks av anställda inom IT-avdelningarna samt övriga avdelningar då deras svar menar på att utbildning inom IT och säkerhetsfrågor är något som krävs organisationsomspännande.

Övriga avdelningars låga medvetenhet är förmodligen även ett resultat av för lite utbildning inom just IT-säkerhet samt ett avsaknat intresse för dessa frågor. De krav och förväntningar som ställs på de anställda kring IT-medvetenhet är således något som måste inkorporeras och tydliggöras inom organisationen för att få bättrre effekt. IT-avdelningarna menar på att alla anställda får en grundutbildning inom IT-säkerhet och att anställda är medvetna om vilka policys som finns. Så var dock inte fallet enligt empirin. Vår studie visar på att anställda från övriga avdelningar för det första inte alltid får utbildning samt att de inte känner till de policys och riktlinjer som är uppsatta. Det är således en stor diskrepans mellan anställdas uppfattning och verkligheten.

LeVeque (2006) menar på att policys och utbildning kring dessa även måste vara förankrade i organisationen. Genom empirin har det dock framgått att IT-avdelningen har det övergripande ansvaret för policy- och IT-frågor och att övriga avdelningar inte har mycket insikt i detta. Att sprida ut IT-ansvar över flera avdelningar genom tydliga ansvarsroller skulle potentiellt kunna öka medvetenheten som i sin tur minskar riskerna för lyckade SE-attacker.

## 5.5 Kritik

Vi har under intervjuerna försökt följa intervjutekniker som Alvehus (2013) tar upp. Dock är vi inga erfarna intervjuare vilket innebär att misstag kan ha begåtts under intervjuerna. I transkriberingen går det att avläsa att vi ibland ställt flera frågor samtidigt och ställt ledande frågor vid ett fåtal tillfällen. Det är två saker som enligt Alvehus (2013) bör undvikas under intervjuer. Vi har heller ingen kontrollgrupp som verifierar vår empiri. Eftersom vår studie är avgränsad till två företag och totalt 8 respondenter är det svårt att säga att vårt resultat speglar verkligheten. Intervjufrågorna är dock baserade på två väletablerade teorier inom informatik, vilket ger svaren en vetenskaplig grund att stå på.

# 6 Slutsats

I denna uppsats har vi försökt ställa de olika avdelningarna mot varandra och belysa de skillnader och likheter som finns inom säkerhetsmedvetenhet. Som visat tyder resultaten på att övriga avdelningar är en riskfaktor för eventuella SE-attacker. Den allmänna IT-säkerhetsmedvetenheten är, bortsett från IT-personal, låg och medvetenheten om SE och dess hot är i synnerhet låg inom de båda organisationernas övriga avdelningar. IT-personal hade högre medvetenheten om SE än förväntat, dock har inte kunskapen spridits till resten av avdelningarna. Den empiri som sammanställts visar således på ett tydligt gap mellan IT-avdelningar och övriga avdelningar när det kommer till säkerhetsmedvetenhet. IT-avdelningarna var medvetna om att medvetenheten var låg inom de övriga avdelningarna, men inga större försök till att minska gapet i form av utbildning hade gjorts. De anställda inom övriga avdelningar menade även på att det är komplicerat att arbeta på ett IT-säkert sätt.

Dock är avdelningsspecifik medvetenhet fortfarande ett relativt outforskat område. Denna uppsats undersöker endast en liten del av alla organisationer och endast en person inom varje avdelning. Således behövs mer forskning inom detta område för att kunna dra en definitiv slutsats, dock pekar denna uppsats på att diskrepansen inom IT-säkerhet mellan avdelningar är ett problemområde som bör förbättras.

En organisation är inte säkrare än sin svagaste länk vilken innebär att de organisationer vi undersökt i den är uppsatsen är högst sårbara mot SE-attacker. Vi tror inte att dessa organisationer är unika utan att den låga IT-säkerhetsmedveten är frekvent förekommande inom dagens organisationer. En SE-attack kan få fatala konsekvenser för organisationer och det är därför oerhört viktigt att organisationer börjar ta SE på allvar innan de blir drabbade. Tyvärr kan det krävas att en organisation blir utsatt för en omfattande attack innan man inser vikten av säkerhetsmedvetenhet och säkra arbetssätt.

## 6.1 Kunskapsbidrag

Tidigare forskning har belyst medvetenhet inom organisationer. Detta har dock främst gjorts genom kvantitativa studier (Bulgurcu et al., 2010). Denna uppsats kvalitativa ansats har även kombinerat IDT och TPB och belyst dessa ur ett SE-perspektiv baserat på de avdelningar anställda jobbar inom. Avdelnings- och SE-specifik undersökning har inte tidigare gjorts i detta manér vilket får ses som ett bidrag till forskningen. Även anställdas individuella medvetenhet är unik, vilket i sig även blir ett bidrag.

## 6.2 Förslag på vidare forskning

Denna uppsats tar hänsyn till IDT och TPB i kombination ur ett SE-perspektiv, men belyser endast en del av de faktorer som detta område berör. Vi har gett förslag på vad den låga medvetenheten kan bero på, och kopplat det till socialpsykologiska faktorer som attityd,

subjektiv norm och kontroll. Dock kan även andra faktorer spela in i varför anställdas medvetenhet är låg, som till exempel organisatoriska aspekter. Det är dock ett intressant ämne som kräver vidare forskning för att kunna ge rättvisande resultat. Vidare forskning skulle även kunna undersöka fler branscher och avdelningar för att få en mer validerad bild av verkligheten. Man skulle även kunna jämföra högriskbranscher, som bank- och flygtransportbranschen, med denna studiens resultat för att jämföra likheter och skillnader.

# Appendix I

## Intervjuguide

Forskningsfråga som ska besvaras med hjälp av följande intervjuguide:

**Hur medvetna om SE är IT-avdelningar respektive övriga avdelningar på medelstora / stora organisationer?**

| Intervjufråga | Följdfråga/Förklaring | Motivering | Berörda teoretiska delar |
|---|---|---|---|
| **1. Berätta om dig själv. Vad har du för arbetsbakgrund, hur länge har du jobbat på företaget och vad har du för specifika arbetsuppgifter och ansvarsområden i din arbetsroll?** | | För att få en god inledning på intervjun och få en överblick över intervjurespondentens roll och tidigare erfarenheter. Ger möjligheten att styra fortsättningen av intervjun i önskad riktning. Ger svar på om intervjurespondenten innehar önskad ansvarsposition. | |
| **2a. Vilken/vilka typer av informationssystem har du tillgång till?**<br><br>**2b. Hur använder du dig av nämnda informationssystem i ditt dagliga arbete och hur stor behörighet har du?**<br><br>**2c. Vilken möjlig påverkan har du via informationssystemen du använder?**<br><br>**2d. Sker ovanstående aktioner utan vidare validering? Dvs. Kan du utföra handlingarna själv eller krävs det att ytterligare aktörer ger godkännanden.** | Vid oförstående eller outvecklat svar från respondenten ger vi exempel på vad vi menar. Ex lägga till en ny anställd, utföra transaktioner, få ut kundinformation, stänga ner system, skapa inlogg, addera data etc. | Får intervjurespondenten att tänka i informartionsystems-termer. Att veta vilka system respondenten sitter i ger oss möjlighet att anpassa intervjufrågorna. Visar på möjlig organisationell påverkan respondenten har och vad det en social engineer skulle kunna åstadkomma om respondenten utsattes för en SE-attack. | |

| | | | |
|---|---|---|---|
| **3. Vet du vad Social Engineering är? I så fall, vad är din definition av Social Engineering?** | För att respondenten ska ha samma uppfattning om SE ger vi följande förklaring. SE är inom IT-säkerhet metoder för att manipulera personer till att utföra handlingar eller avslöja konfidentiell information, snarare än att göra inbrott eller använda sig av tekniska Crackningstekniker. Exempelvis scam e-mail eller att utge sig för att vara någon annan person. | Inledande fråga som kontrollerar respondentens medvetenhet om SE. Den tilläggande förklaringen har som syfte att informera respondenten om social engineering för att ge förståelse för vad uppsatsens har för perspektiv. | **Medvetenhet** (Bulgurcu et al. 2010; D'Arcy 2009) |
| **4. Hur säkerhetsmedveten är du?** | Svara gärna så ärligt som möjligt. | Motivering: Bred fråga där respondenten får redogöra sitt förhållande till säkerhet. | **Medvetenhet** (Bulgurcu et al. 2010; D'Arcy 2009) |
| **5. Hur får ni information om IT-säkerhet? Har ni några internutbildningar, workshops, informationsmail inom IT-säkerhet?** | | Motivering: Ämnar undersöka respondentens upplevda IT-säkerhetsutbildning. Kan leda in på TPB. | **Medvetenhet** (Bulgurcu et al. 2010; D'Arcy 2009)**, Socialpsykologiska faktorer** (Bulgurcu et al. 2010, Hauser, 2016, Ivaturi et al. 2014, Warner, 2006, Boubaker et al. 2006, Al-Omari et al. 2011, Bulgurcu et al. 2011, Kranz & Haeussinger, 2014) |
| **6. Vilka olika IT-ansvarsroller finns det i företaget?** | | Visar på medvetenhet samt målar upp en bild av organisationens IT-säkerhetsansvarsfördelning. | **Medvetenhet** (Bulgurcu et al. 2010; D'Arcy 2009) |
| **7. Har företaget något som förhindrar obehöriga att ta sig in i lokalerna?** | Exempelvis passerkort, portkod eller liknande? | Visar på respondentens medvetenhet om säkerhetsskydd samt potentiellt SE-hot. Ger en bild av organisationens fysiska säkerhet. Kan eventuellt leda in på policys.<br><br>SE-tekniker: Impersonation, Tailgaiting | **Medvetenhet, ISP** (Durgin, 2007; Kelley, 2006; LeVeque, 2006; Al-Omari et al. 2011; Gollmann, 2011, Bulgurcu et al. 2010, Herath & Rao, 2009) |
| **8a. Finns det några riktlinjer/information för hur du ska förhålla** | Har du vart med om detta? Hur agerade du då? | 8a,b,c Undersöker medvetenheten hos anställda angående mailpolicys, | **Medvetenhet** (Bulgurcu et al. 2010; D'Arcy |

| | | | |
|---|---|---|---|
| **dig och agera gentemot personer du inte känner igen på kontoret?**<br><br>**8b. Finns det några riktlinjer/information för hur du ska förhålla dig och du får ett mail med okänd avsändare?**<br><br>**8c. -\|\|- får samtal från okänt nummer?** | | fysiska säkerhetspolicys och teflefonpolicy. Kan ge en inblick i vilka faktiska policys som finns. Kan även leda in på handlingsplan, IDT och policy efterföljning.<br><br>SE-tekniker:<br><br>Impersonation, Tailgaiting, Phising, Spear Phishing, Vishing – kan leda in på SMSihsing, Malware | 2009)**, ISP (**Durgin, 2007; Kelley, 2006; LeVeque, 2006; Al-Omari et al. 2011; Gollmann, 2011, Bulgurcu et al. 2010, Herath & Rao, 2009)**, Socialpsykologiska faktorer** (Bulgurcu et al. 2010, Hauser, 2016, Ivaturi et al. 2014, Warner, 2006, Boubaker et al. 2006, Al-Omari et al. 2011, Bulgurcu et al. 2011, Kranz & Haeussinger, 2014) |
| **9. Brukar du få oönskade mail eller används någon form av spamfilter?** | | Får respondenten att börja tänka på mailhantering. Leder ofta till att respondenten börjar prata om oönskade mail hen fått.<br><br>SE-tekniker:<br><br>Phishing, Malware | **Medvetenhet (**Bulgurcu et al. 2010; D'Arcy 2009) |
| **10a. Finns det rutiner för lösenord**<br><br>**10b. Har du flera olika lösenord för att logga in på tidigare nämnda informationsystem?**<br><br>**10c. Hur gör du för att komma ihåg alla lösenord?** | 10a. Exempelvis krav på styrka, hur ofta man ska byta osv?<br><br>10c. Får man skriva ner sina lösenord? | 10a. Undersöker lösenordspolicys och medvetenhet angående dessa. Leder in på 10b<br><br>10b. Tar reda på hur många lösenord respondenten använder. Leder in på fråga 10c.<br><br>10c. Kollar hur respondenten gör för at komma ihåg sina lösenord. Undersöker med hjälp av följdfrågan policy-efterföljning.<br><br>SE-tekniker:<br><br>Tailgaiting | **Medvetenhet (**Bulgurcu et al. 2010; D'Arcy 2009)**, ISP (**Durgin, 2007; Kelley, 2006; LeVeque, 2006; Al-Omari et al. 2011; Gollmann, 2011, Bulgurcu et al. 2010, Herath & Rao, 2009)**, Socialpsykologiska aspekter** (Bulgurcu et al. 2010, Hauser, 2016, Ivaturi et al. 2014, Warner, 2006, Boubaker et al. 2006, Al-Omari et al. 2011, Bulgurcu et al. 2011, Kranz & Haeussinger, 2014) |
| **11a. Får privata enhet-** | 11a. Används någon VPN- | Kontrollera fysiska säker- | **Medvetenhet** |

| | | | |
|---|---|---|---|
| **er användas till arbetsuppgifter?**<br><br>**11b. Får privata enheter kopplas till arbetsplatsens nätverk?**<br><br>**11c. Får man arbeta hemifrån?** | tjänst vid arbete hemifrån eller från privata enheter? | hetspolicys. Kan leda in på efterföljning och medvetenhet.<br><br>SE-tekniker:<br><br>Malware | **(**Bulgurcu et al. 2010; D'Arcy 2009)**, ISP (**Durgin, 2007; Kelley, 2006; LeVeque, 2006; Al-Omari et al. 2011; Gollmann, 2011, Bulgurcu et al. 2010, Herath & Rao, 2009)**, Socialpsykologiska aspekter** (Bulgurcu et al. 2010, Hauser, 2016, Ivaturi et al. 2014, Warner, 2006, Boubaker et al. 2006, Al-Omari et al. 2011, Bulgurcu et al. 2011, Kranz & Haeussinger, 2014) |
| **12a. Hur hanteras delning och transport av filer och information inom företaget?**<br><br>**12b. Kan filerna eller informationen som skickas räknas som känslig? Ändrar det sättet du skickar filer på?**<br><br>**12c Har ni några riktlinjer för hur filer ska skickas?** | 12a. Utveckling vid oförstående: Hur skickar du filer till dina kollegor eller kunder?<br><br>Sker den kommunikationen exempelvis via mail? Eller används intranätet? | 12a. Undersöker respondentens medvetenhet om transportering av filer. Leder in på fråga 12b.<br><br>12b. Undersöker hur säkerhetsmedveten respondenten är angående transport av filer. Leder möjligtvis in på mailpolicys eftersom det är ett vanligt sätt att transportera filer.<br><br>12c. Går in på vilka policys som finns och hur medveten respondenten är om dessa.<br><br>SE-tekniker:<br><br>Malware, Phishing, Spear Phishing | **Medvetenhet (**Bulgurcu et al. 2010; D'Arcy 2009)**, ISP (**Durgin, 2007; Kelley, 2006; LeVeque, 2006; Al-Omari et al. 2011; Gollmann, 2011, Bulgurcu et al. 2010, Herath & Rao, 2009)**, Socialpsykologiska aspekter** (Bulgurcu et al. 2010, Hauser, 2016, Ivaturi et al. 2014, Warner, 2006, Boubaker et al. 2006, Al-Omari et al. 2011, Bulgurcu et al. 2011, Kranz & Haeussinger, 2014) |
| **13a. Får/kan du kolla dina privata mail när du är uppkopplad på Huges nätverk?**<br><br>**13b. Får du kolla din privata mail på jobba-** | | Kontrollerar mailpolicys och anställdas medvetenhet kring dessa. Kollar även efterföljning av de potentiella riktlinjerna. | **Medvetenhet (**Bulgurcu et al. 2010; D'Arcy 2009)**, ISP (**Durgin, 2007; Kelley, 2006; LeVeque, 2006; Al-Omari et al. 2011; Gollmann, 2011, Bulgurcu et al. |

| | | | |
|---|---|---|---|
| **datorn?** | | SE-tekniker:<br><br>Malware, Phishing, Spear Phishing | 2010, Herath & Rao, 2009)**, Socialpsykologiska aspekter** (Bulgurcu et al. 2010, Hauser, 2016, Ivaturi et al. 2014, Warner, 2006, Boubaker et al. 2006, Al-Omari et al. 2011, Bulgurcu et al. 2011, Kranz & Haeussinger, 2014) |
| **14a. Har ni några regler kring extern cloud-tjänster?**<br><br>**14b. Följdfråga: Använder du cloud-tjänster i arbetet?** | 14a. Cloud-tjänster är till exempel dropbox, Google drive eller iCloud. | 14a. Undersöker policys angående cloud-tjänster och respondentens medvetenhet.<br><br>14b. Undersöker den anställdas efterföljning.<br><br>SE-tekniker:<br><br>Malware | **Medvetenhet (**Bulgurcu et al. 2010; D'Arcy 2009)**, ISP (**Durgin, 2007; Kelley, 2006; LeVeque, 2006; Al-Omari et al. 2011; Gollmann, 2011, Bulgurcu et al. 2010, Herath & Rao, 2009)**, Socialpsykologiska aspekter** (Bulgurcu et al. 2010, Hauser, 2016, Ivaturi et al. 2014, Warner, 2006, Boubaker et al. 2006, Al-Omari et al. 2011, Bulgurcu et al. 2011, Kranz & Haeussinger, 2014) |
| **15a. Finns det spärrar i nätverket som gör att du inte kommer åt säker på internet eller intranätet?**<br><br>**15b. Finns det riktlinjer för hur ni får "surfa" på internet?** | 15a. Har du exempelvis vart med om att du inte kommer åt en hemsida? | 15a. Undersöker medvetenhet angående organisationens internetpolicys.<br><br>15b. Undersöker respondentens säkerhetsmedvetenhet.<br><br>SE-tekniker:<br><br>Malware | **Medvetenhet (**Bulgurcu et al. 2010; D'Arcy 2009)**, ISP (**Durgin, 2007; Kelley, 2006; LeVeque, 2006; Al-Omari et al. 2011; Gollmann, 2011, Bulgurcu et al. 2010, Herath & Rao, 2009) |
| **16a. Hur tycker du att den generella säkerhetsmedveten är inom organisationen?** | 16a. På vilket sätt är den bra eller dålig?<br><br>16b. Eventuell fortsättning: | 16a. En väldigt bred fråga som ämnar undersöka normer och eventuellt efterföljning och medvetenhet. | **Medvetenhet (**Bulgurcu et al. 2010; D'Arcy 2009)**, Socialpsykologiska aspekter** (Bulgurcu et al. |

| | | | |
|---|---|---|---|
| **16b. Tror du att det finns motstånd till att arbeta IT-säkert?** | Ett IT-säkert arbetssätt kan kanske innebära att man måste ändra på sitt nuvarande arbetssätt som man trivs med. | 16b. Undersöker beteende och attityder. | 2010, Hauser, 2016, Ivaturi et al. 2014, Warner, 2006, Boubaker et al. 2006, Al-Omari et al. 2011, Bulgurcu et al. 2011, Kranz & Haeussinger, 2014) |
| **17. Har ni någon handlingsplan om ni blir utsatta för en cyberattack?** | Till exempel om du eller en kollega råkar klicka på en skadlig länk, eller om du ser en suspekt person röra sig på arbetsplatsen. Finns det en handlingsplan för hur ni ska agera? | Undersöker ISPA och ISA. | **Medvetenhet (**Bulgurcu et al. 2010; D'Arcy 2009) |
| **18. Finns det någonstans ni lagrar policies?** | Exempelvis i ett dokumentbibliotek på intranätet? | Undersöker ISPA. | **Medvetenhet (**Bulgurcu et al. 2010; D'Arcy 2009) |
| **19. Skulle du vilja förbättra IT-säkerheten inom organisationen?** | Hur tycker du det skulle gå till i så fall? | Bred fråga som ämnar får ett brett svar. Kan visa på medvetenhet och socialpsykologiska aspekter. | **Medvetenhet (**Bulgurcu et al. 2010; D'Arcy 2009)**, Socialpsykologiska aspekter** (Bulgurcu et al. 2010, Hauser, 2016, Ivaturi et al. 2014, Warner, 2006, Boubaker et al. 2006, Al-Omari et al. 2011, Bulgurcu et al. 2011, Kranz & Haeussinger, 2014) |

# Appendix II

## Intervjukontrakt

**Datum**
Företagsnamn

Denna intervju fungerar som empiriskt underlag till en systemvetenskaplig kandidatuppsats vid Lunds Universitet. Uppsatsen handlar om IT-säkerhet där målet är att undersöka olika företags säkerhetspolicys och strategier ur ett Social Engineering-perspektiv.

**Information inför intervjun:**

Intervjun är beräknad att ta ungefär en timme.

Intervjun kommer att spelas in. Ljudupptagningen är enbart ämnad för oss och kommer ej delas med några andra parter.

Vi värderar personers och företags integritet och förstår att säkerhetsfrågor kan vara ett känsligt ämne. Därför kommer namn och företagsnamn att fingeras.

Du kan när som helst under intervjun välja att avbryta den. Du kan också välja att inte svara på frågor som ställs.

De tre huvudområden som kommer beröras under intervjun är:
- Social Engineering
- Säkerhetspolicys
- Informationssystem

Om du önskar att ta del av uppsatsen kommer den finnas tillgänglig i slutet på maj. Kontakta oss om du har några frågor eller om du önskar att tillägga eller ta bort något från intervjun i efterhand.

*Ett stort tack för att du ställer upp på denna intervju.*

| | | |
|---|---|---|
| Ludvig Ohlsson | Jesper Brumark | *Intervjurespondent* |
| ludvig.ohlsson@gmail.com | jesper.brumark@gmail.com | |

# Appendix III

Röd = Mindre relevant
Gul = Relevant
Grön = Högst relevant

## Litteraturtabell

| | | | |
|---|---|---|---|
| SOCIAL ENGINEERING IN SOCIAL NETWORKING SITES: HOW GOOD BECOMES EVIL | Algarni et al. (2014) | Belyser hur SE använts på social medier. Undersöker vilka SE tekniker som använts, varför de använts och varför de fungerarde baserat på user opinions. Pengar och Sex var ofta purpose. | N/A |
| Why Cybersecurity Is So Difficult to Get Right | Olejarz (2015) | Intervju med Vice President på IBM. Berättar om vad hackare letar efter för information, hur de använder den osv. Kostnader för företaget vid misstag eller hack samt hur man bäst skyddar sig | N/A |
| INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS1 | Bulgurcu et al. (2010) | Research om hur anställda följer informationssäkerhetspolicys och vilka faktorer som är bidragande till varför de följs/inte följs. Bygger på theory of planned behaviour | Theory of Planned Behavior |
| Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security | Workman (2007) | Utredning om vilka bakomliggande teorier det finns till phishing. Och hur phishing fungera | Applicerar olika teorier på olika typer av phishing. Men använder Elaboration likelihood model (EML) vilket låter vettigt. |
| Susceptibility to Social Engineering in Social Networking Sites: The Case of Facebook | Algarni et al. (2015) | Samme som snubbarna på rad 5, hänger ihop. Testar hur lättlurade folk är på facebook | N/A |
| Social Networking Websites and Posting Personal Information: An Evaluation of Protection Motivation Theory | Marett et al. (2011) | Skapar en underöskningmodel utifrån protection motivation theory (PMT) för att undersöka hur användare fårhåller sig till risker på social medier | Protection motivation theory |
| Social Engineering Awareness in Business and Academia | Hauser (2016) | En undersökning för att ta reda på hur medvetna företag är om social egnineering utifrån ett IDT-perspektiv | IDT |
| A Taxonomy for Social Engineering attacks | Ivaturi & Janczewski (2011) | Skapar en taxonomi av SE-attacker. Författarna försöker kategorisera SE-attacker för att lättare skapa skydd emot dem. | N/A |
| Countermeasures for Social Engineering-based Malware Installation Attacks | Flores & Ekstedt (2013) | In this paper we attempt to obtain a deeper understanding of how to defend against a type of social engineering attack that attempts to install malware on computers through e-mail or portable media. | N/A |
| A Typology Of Social Engineering Attacks – | Ivaturi & Janczewski | Definierar olika online social engineering metoder ur ett vetenskapligt perspektiv. | N/A |

| | | | |
|---|---|---|---|
| An Information Science Perspective | (2012) | | |
| Extending Ecommerce Deception to Phishing | Wright et al. (2014) | Undersöker phishing metoder utifrån Decption Theory. Specifikt E-mails. | Elaboration likelihood model |
| The Effectiveness of Deceptive Tactics in Phishing | Marett et al. (2009) | En studie om vad som gör phishing mail effektiva. Hur reagerar människor på olika typer av mail. | IDT - delvis. |
| Got Phished? Internet Security and Human Vulnerability | Goel et al. (2017) | Om phishing. Undersöker om contexten i mail påverkar människor mottaglighet. Resultat: The fear of losing or anticipation of gaining something valuable increased susceptibility to deception and vulnerability to phishing. | blandad socialpsykologi |
| 8R. Effect of Frame of Mind on Users' Deception Detection Attitudes and Behaviours | Ivaturi et al (2014) | Ge förslag på hur männsikors "frame of mind" påverkar hantering av onlinebedrägeri. Påpekar även hur viktigt det är med medventenhet och ubildning. | IDT |
| Corporate Risks in Social Networks – Towards a Risk Management Framework | Braun & Esswein (2012) | Handlar om vilka risker det finns för företag som använder social medier. Studien tar fram ett framework för att skydda sig. | N/A |
| Towards Understanding User Behavioral Intentions to Use IT Security: Examining the Impact of IT Security Psychological Climate and Individual Beliefs | Warner (2006) | Kopplar user behaviour med organisationkultur för att förstå hur man får perosner it-säkerhetsmedvetna | Theory of Planned Behavior |
| Examining the Role of Organizational Password Security Policies in Individual Password Security Behaviors | Kelley (2006) | Undersöker den naturliga konflikten mellan Organizational Password Security Policies och olika psykologiska teorier. Och hur de psykologiska aspekterna påverkar hur anställda använder lösenord. | Theory of Planned Behavior mf. |
| A Decomposed Model of IT Artifact-related Beliefs as Antecedents of IT Acceptance and Use | Boubaker et al. (2006) | Författarna menar att tidigare forsknings som kopplat psykologiska teorier till IT-acceptance har behandlat IT som en "black box". To address this issue, the present paper develops a TPB-based theoretical model founded on a literature review of individuals' IT artifact-related beliefs modeled as antecedents of TPB's key constructs. | Theory of Planned Behavior |
| Information Security Policy Compliance: A User Acceptance Perspective | Al-Omari et al. (2011) | This study adapts the Technology Acceptance Model (TAM) to examine users' behavioral intention to comply with ISPs. Baseras på TPB | Theory of Planned Behavior |
| INFORMATION SECURITY POLICY COMPLIANCE: THE ROLE OF FAIRNESS, COMMITMENT, AND COST BELIEFS | Bulgurcu et al. (2011) | In this paper, we focused on the organizational costs associated with an employee's ISP compliance and non-compliance. Faktorerna som diskuterades var ISP Fairness and Organizational Commitment. Our results show that organization-based employee beliefs significantly affect attitude, and as predicted, the strength of each belief-attitude relationship is affected by ISP fairness and organizational commitment | Theory of Planned Behavior |

| | | | |
|---|---|---|---|
| Why Deterrence is not Enough: The Role of Endogenous Motivations on Employees' Information Security Behavior | Kranz & Haeussinger (2014) | Kollar hur endogenous motivation påverkar individual ISS-related behavior (information system security). The results show that when employees' personal values and principles are congruent with their employer's ISS-related prescriptions and goals their intention to comply with security policies significantly increases. On the contrary, we find no impact on compliance intention when employees perceive their actions as a result of external pressures and coercion | Theory of Planned Behavior mf. |
| Deception Detection Theory as a Basis for an Automated Investigation of the Behavior Analysis Interview | Moffitt (2009) | Handlar om att använda deception theory för att förbättra intervjutekniker. | Deception Theory + IDT |
| Protection motivation and deterrence: a framework for security policy compliance in organisations | Herath & Rao (2009) | Ramverk baserat på TPB för hur man ska följa policies. Anställda underestimerar sannolikheten av en attack | Theory of Planned Behaviour |
| Understanding the Importance of and Implementing Internal Security Measures | Durgin (2007) | Handlar om varför internal security är viktigt och varför det kan vara kostsammare än en extern attack. Lösenordspolicys och physical security (usb) | N/A |
| Behavioral and policy issues in information systems security: the insider threat | Warkentin & Willison (2009) | Tar också upp internsäkerhet och delar upp det i två delar: intentional eller unintentional säkerhet | N/A |
| An Identity Fraud Model Categorising Perpetrators, Channels, Methods of Attack, Victims and Organisational Impacts | Jamieson et al. (2007) | Tar upp vishing och kategoriserar attackceringgrupper. | N/A |

# Appendix IV

## Intervjutabell Beta

| | | | | | |
|---|---|---|---|---|---|
| Towards security requirements management for software product lines: A security domain requirements engineering process | Mellado et al. (2008) | Ingen teori | IS-utvceklingsäkerhet | Google Scholar: CRM security | Artikeln handlar om hur viktigt det är att tänka på säkerhet genom hela utvecklingsidan. Artikel kommer fram till olika standarder vid systemutveckling baserat på ISO best-practises. |
| Information security management (3): the Code of Practice for Information Security Management (BS 7799) | von Solms (1998) | Ingen toeri | IS-säkerhet | Google Scholar: CRM security | Atikeln handlar om vilket som är det bästa sättet för security controll av information. Brittiska företag som tagit fram best practises. |
| An integrated system theory of information security management | Hong et al. (2003) | Ingen toeri | IS-säkerhet management | Google Scholar: CRM security | Artikel ämnar integrera risk management theory, policy theory, control and auditing theory, management system thero och contingency theory för att bygga en mer omfattande information security theory |
| SOCIAL ENGINEERING IN SOCIAL NETWORKING SITES: HOW GOOD BECOMES EVIL | Algarni et al. (2014) | Ingen toeri | SE-Social medier | Google Scholar: Social Engineering Avg. Från: 2010 Published: AIS | Belyser hur SE använts på social medier. Undersöker vilka SE tekniker som använts, varför de använts och varför de fungerarde baserat på user opinions. Pengar och Sex var ofta purpose. |
| Why Cybersecurity Is So Difficult to Get Right | Olejarz (2015) | Ingen toeri | IS-säkerhet | Google: Social Engineering Harvard Business Review | Intervju med Vice President på IBM. Berättar om vad hackare letar efter för information, hur de använder den osv. Kostnader för företaget vid misstag eller hack samt hur man bäst skyddar sig |
| INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND | Bulgurcu et al. (2010) | Theory of Planned Behavior | Säkerhetspolicys / Socialt Beteende | Google Scholar: IT Security Policy Theory | Research om hur anställda följer informationssäkerhetspolicys och vilka faktorer som är bidragande till varför de följs/inte följs. Bygger på theory of planned behaviour |

| | | | | | |
|---|---|---|---|---|---|
| INFOR-MATION SE-CURITY AWARENESS1 | | | | | |
| Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security | Workman (2007) | Applicerar olika teorier på olika typer av phishing. Men använder Elaboration likelihood model (EML) vilket låter vettigt. | SE-Phishing | Hittad via Algarni, Abdullah, Xu, Yue, Chan, Taizan, & Tian, Yu-Chu (2014) | Utredning om vilka bakomliggande teorier det finns till phishing. Och hur phishing fungera |
| Susceptibility to Social Engineering in Social Networking Sites: The Case of Facebook | Algarni et al. (2015) | Ingen toeri | SE-Phishing | Google Scholar: Social Engineering Avg. Från: 2010 Published: AIS | Samme som snubbarna på rad 5, hänger ihop. Testar hur lättlurade folk är på facebook |
| Social Networking Websites and Posting Personal Information: An Evaluation of Protection Motivation Theory | Marett et al. (2011) | Protection motivation theory | SE/PMT-Social medier | Google Scholar: Social Engineering Avg. Från: 2010 Published: AIS | Skapar en underöskning-model utifrån protection motivation theory (PMT) för att undersöka hur användare fårhåller sig till risker på social medier |
| Social Engineering Awareness in Business and Academia | Hauser (2016) | IDT | SE-medvetenhet | AIS: "Social engineering" | En undersökning för att ta reda på hur medvetna företag är om social egnineering utifrån ett IDT-perspektiv |
| A Taxonomy for Social Engineering attacks | Ivaturi & Janczewski (2011) | Ingen toeri | SE-metoder | AIS: "Social engineering" | Skapar en taxonomi av SE-attacker. Författarna försöker kategorisera SE-attacker för att lättare skapa skydd emot dem. |
| Countermeasures for Social Engineering-based Malware Installation Attacks | Flores & Ekstedt (2013) | Ingen toeri | SE-policys/countermeasures | AIS: "Social engineering" | In this paper we attempt to obtain a deeper understanding of how to defend against a type of social engineering attack that attempts to install malware on computers through e-mail or portable media. |
| A Typology Of Social Engineering Attacks – An Information Science Perspective | Ivaturi & Janczewski (2012) | Ingen toeri | SE-phishing, money-laundring, malware, clickjacking etc - online | AIS: "Social engineering" | Definierar olika online social engineering metoder ur ett vetenskapligt perspektiv. |
| Extending Ecommerce Deception to | Wright et al. (2014) | Elaboration likelihood model | SE-phishing, IDT | AIS: "Social engineering" | Undersöker phishing metoder utifrån Decption Theory. Specifikt E-mails. |

| | | | | | |
|---|---|---|---|---|---|
| Phishing | | | | | |
| Combating IS Fraud: A Teaching Case Study | Lincke & Green (2012) | Ingen toeri | SE-Case | AIS: "Social engineering" | Ger förslag på casestudier som ämnar utbilda organisationer om IT-säkerhet för att hjälpa de skydda sig mot IT-bedrägeri. |
| The Effectiveness of Deceptive Tactics in Phishing | Marett et al. (2009) | IDT - delvis. | SE-phishing | AIS: "Social engineering" | En studie om vad som gör phishing mail effektiva. Hur reagerar människor på olika typer av mail. |
| Got Phished? Internet Security and Human Vulnerability | Goel et al. (2017) | blandad socialpsykologi | SE-phishing | AIS: "Social engineering" | Om phishing. Undersöker om contexten i mail påverkar människor mottaglighet. Resultat: The fear of losing or anticipation of gaining something valuable increased susceptibility to deception and vulnerability to phishing. |
| 8R. Effect of Frame of Mind on Users' Deception Detection Attitudes and Behaviours | Ivaturi et al (2014) | IDT | Blandning SE/Socialpsykologi | AIS: "Social engineering" | Ge förslag på hur männsikors "frame of mind" påverkar hantering av onlinebedrägeri. Påpekar även hur viktigt det är med medventenhet och ubildning. |
| Corporate Risks in Social Networks – Towards a Risk Management Framework | Braun & Esswein (2012) | Ingen toeri | Företagssäkerhet - Social Medier, SE | AIS: "Social engineering" | Handlar om vilka risker det finns för företag som använder social medier. Studien tar fram ett framework för att skydda sig. |
| Phishing Training: A Preliminary Look at the Effects of Different Types of Training | Karumbaiah et al. (2016) | Protection Motivation Theory | SE-phishing - säkerhetsträning | AIS: "Social engineering" | Förklarar att IT-säkerhetsträning hjälper anställda att identifiera phishing-attacker. Tar reda på vilken träning som är den mest effektiva. |
| ON NOT FALLING FOR PHISH: EXAMINING MULTIPLE STAGES OF PROTECTIVE BEHAVIOR OF INFORMATION SYSTEMS END-USERS | Burns et al. (2012) | Behavioural change theories | IT-säkerhet. | AIS: "Social engineering" | Undersöker anställdas beteende vid phishing-attacker utifrån "behavior change model adapted from health-related fields" |
| Unweaving the Phisher's Net: An Exploratory Study | Pérez-Mira (2008) | IDT | SE-Phishing | AIS: "Social engineering" "Deception Theory" | This study attempts to understand the basic deception techniques utilized by phishers when creating the phishing emails |
| Towards Understanding User Behavioral Intentions to Use | Warner (2006) | Theory of Planned Behavior | IT-säkerhet. TPB | AIS: "Theory of Planned Behaviour" | Kopplar user behaviour med organisationkultur för att förstå hur man får perosner it- |

| | | | | | |
|---|---|---|---|---|---|
| IT Security: Examining the Impact of IT Security Psychological Climate and Individual Beliefs | | | | IT-security | säkerhetsmedvetna |
| Examining the Role of Organizational Password Security Policies in Individual Password Security Behaviors | Kelley (2006) | Theory of Planned Behavior mf. | Organizational Password Security Policies, TPB mm. | AIS: "Theory of Planned Behaviour" IT-security | Undersöker den naturliga konflikten mellan Organizational Password Security Policies och olika psykologiska teorier. Och hur de psykologiska aspekterna påverkar hur anställda använder lösenord. |
| A Decomposed Model of IT Artifact-related Beliefs as Antecedents of IT Acceptance and Use | Boubaker et al. (2006) | Theory of Planned Behavior | IT-acceptance. TPB | AIS: "Theory of Planned Behaviour" IT-security | Författarna menar att tidigare forsknings som kopplat psykologiska teorier till IT-acceptance har behandlat IT som en "black box". To address this issue, the present paper develops a TPB-based theoretical model founded on a literature review of individuals' IT artifact-related beliefs modeled as antecedents of TPB's key constructs. |
| Information Security Policies Compliance: The Role of Organizational Punishment | Mohammad & Ahluwalia (2013) | Theory of Planned Behavior | IT-policy, Complience. TPB | AIS: "Theory of Planned Behaviour" IT-security | Undersöker hur organizasinal punishment påverkar anställdas IT-policy complience utifrån ett TPB-perspektiv. Den empiriska datan finns dock inte med och författarna betonar att studien är "work in progress". |
| Information Security Policy Compliance: A User Acceptance Perspective | Al-Omari et al. (2011) | Theory of Planned Behavior | IT-acceptence | AIS: "Theory of Planned Behaviour" IT-security | This study adapts the Technology Acceptance Model (TAM) to examine users' behavioral intention to comply with ISPs. Baseras på TPB |
| INFORMATION SECURITY POLICY COMPLIANCE: THE ROLE OF FAIRNESS, COMMITMENT, AND COST BELIEFS | Bulgurcu et al. (2011) | Theory of Planned Behavior | ISP, TPB, Attitude | AIS: "Theory of planned behaviour" ISP | In this paper, we focused on the organizational costs associated with an employee's ISP compliance and non-compliance. Faktorerna som diskuterades var ISP Fairness and Organizational Commitment. Our results show that organization-based employee beliefs significantly affect attitude, and as predicted, the strength of each belief-attitude relationship is |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | affected by ISP fairness and organizational commitment |
| Why Deterrence is not Enough: The Role of Endogenous Motivations on Employees' Information Security Behavior | Kranz & Haeussinger (2014) | Theory of Planned Behavior mf. | ISS, TPB, Motivation | AIS: "Theory of planned behaviour" ISP | Kollar hur endogenous motivation påverkar individual ISS-related behavior (information system security). The results show that when employees' personal values and principles are congruent with their employer's ISS-related prescriptions and goals their intention to comply with security policies significantly increases. On the contrary, we find no impact on compliance intention when employees perceive their actions as a result of external pressures and coercion |
| Deception Detection Theory as a Basis for an Automated Investigation of the Behavior Analysis Interview | Moffitt (2009) | Deception Theoey + IDT | Deception Detection | AIS: "Decption Theory" | Handlar om att använda deception theory för att förbättra intervjutekniker. |
| Protection motivation and deterrence: a framework for security policy compliance in organisations | Herath & Rao (2009) | Theory of Planned Behaviour | ISP / TPB | Google Scholar: Security Policy Theory of Planned Behaviour | Ramverk baserat på TPB för hur man ska följa policies. Anställda underestimerar sannolikheten av en attack |
| Understanding the Importance of and Implementing Internal Security Measures | Durgin (2007) | Ingen toeri | ISP | Hittade via Bulgurcu, Cavusoglu & Benbasat | Handlar om varför internal security är viktigt och varför det kan vara kostsammare än en extern attack. Lösenordspolicys och physical security (usb) |
| Behavioral and policy issues in information systems security: the insider threat | Warkentin & Willison (2009) | Ingen toeri | ISP | Hittade via Bulgurcu, Cavusoglu & Benbasat | Tar också upp internsäkerhet och delar upp det i två delar: intentional eller unintentional säkerhet |
| An Identity Fraud Model Categorising Perpetrators, Channels, Methods of Attack, Victims and Organisational Impacts | Jamieson et al. (2007) | Ingen toeri | SE | AIS: "Vishing" | Tar upp vishing och kategoriserar attakceringgrupper. |

| | | | | | |
|---|---|---|---|---|---|
| 2016 Internet Security Threat Report | Symantec (2006) | Ingen toeri | SE, IT-säkerhet | Google: "Symantec Report" | Rapport om säkerhet och attacker på internet. |
| Money is gone and town's trust nearly spent | Schaefer & Lam (2007) | Ingen toeri | SE-phishing | Google: "katona nigerian email treas-urer seattle" | Reportage om när katona blev lurad och svindlade pengar |

# Referenser

Abdullah Algarni, Y. X., Taizan Chan. (2015). *Susceptibility to Social Engineering in Social Networking Sites: The Case of Facebook.* Paper presented at the 36th International Conference on Information Systems, Fort Worth, Texas.

AIS. (2017). About AIS. Retrieved from http://aisnet.org/page/AboutAIS

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

Algarni, A., Xu, Y., Chan, T., & Tian, Y.-C. (2014). *Social Engineering in Social Networking Sites: How Good Becomes Evil.* Paper presented at the PACIS 2014 Proceedings, Chengdu, China.

Al-Omari, A., El-Gayar, O., & Deokar, A. (2011). *Information Security Policy Compliance: A User Acceptance Perspective.* Paper presented at the MWAIS 2011 Proceedings, Omaha, NE.

Alvehus, J. (2013). *Skriva uppsats med kvalitativ metod: En handbok* (Vol. 1): Liber.

Andersson, B.-E. (1994). *Som man frågar får man svar - en introduktion i intervju- och enkätteknik* (Vol. 2): Rabén Prisma.

Backman, J. (2008). *Rapporter och uppsatser* (Vol. 2): Studentlitteratur.

Bex, F. (2016). Working with NVIVO*1.1*, 5. Utrecht University. Retrieved from https://docs.google.com/viewer?a=v&pid=sites&srcid=Y3MudXUubmx8aW5mb2ttdHxneDozMTk0M2RlMGIxMTgzZmE2

Boubaker, K. B., & Barki, H. (2006). *A Decomposed Model of IT Artifact-related Beliefs as Antecedents of IT Acceptance and Use.* Paper presented at the AMCIS 2006 Proceedings, Acapulco, Mexico.

Braun, R., & Esswein, W. (2012). *Corporate Risks in Social Networks – Towards a Risk Management Framework.* Paper presented at the AMCIS 2012 Proceedings, Seattle, Washington.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study Of Rationality-Based Beliefs And Information Security Awareness. *MIS Quarterly, 34*(3), 523-548.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2011). *Information Security Policy Compliance: The Role of Fairness, Commitment, and Cost Beliefs.* Paper presented at the MCIS 2011 Proceedings.

Statistiska Centralbyrån (SCB). (2010). De små och medelstora företagens ekonomi 2008: Mikroföretag mest lönsamma. Retrieved from http://www.scb.se/sv_/Hitta-statistik/Statistik-efter-

amne/Naringsverksamhet/Naringslivets-struktur/Foretagens-ekonomi/130389/130397/Behallare-for-Press/De-sma-och-medelstora-foretagens-ekonomi-2008/

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research, 20*(1), 79-98. doi:10.1287/isre.1070.0160

Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies *Journal of the Association for Information Systems, 8*(7), 386-408.

Durgin, M. (2007). Understanding the Importance of and Implementing Internal Security Measures. SANS Infosec Reading Room

Flores, W. R., & Ekstedt, M. (2013). *Countermeasures for Social Engineering-based Malware Installation Attacks.* Paper presented at the CONF-IRM.

Gilbert, S. (2009). *Alignment and strategy; the chicken or the egg?* Paper presented at the CONF-IRM 2009 Proceedings.

Goel, S., Williams, K., & Dincelli, E. (2017). Got Phished? Internet Security and Human Vulnerability. *Journal of the Association for Information Systems, 18*(1), 22-44.

Gollmann, D. (2011). *Computer Security*: Wiley.

Hauser, D. (2016). *Social Engineering Awareness in Business and Academia.* Paper presented at the MWAIS, Wisconsin.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125. doi:10.1057/ejis.2009.6

Ivaturi, K., & Janczewski, L. (2011). *A Taxonomy for Social Engineering attacks.* Paper presented at the CONF-IRM.

Ivaturi, K., & Janczewski, L. (2012). *A Typology Of Social Engineering Attacks – An Information Science Perspective.* Paper presented at the PACIS 2012 Proceedings.

Ivaturi, K., Janczewski, L., & Chua, C. (2014). *Effect of Frame of Mind on Users' Deception Detection Attitudes and Behaviours.* Paper presented at the CONF-IRM 2014 Proceeding.

Karjalainen, M., & Siponen, M. (2011). Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches. *Journal of the Association for Information Systems, 12*(3).

Kelley, J. (2006). *Examining the Role of Organizational Password Security Policies in Individual Password Security Behaviors.* Paper presented at the AMCIS 2006 Proceedings, Acapulco, Mexico.

Kranz, J. J., & Haeussinger, F. J. (2014). *Why Deterrence is not Enough: The Role of Endogenous Motivations on Employees' Information Security Behavior*. Paper presented at the Thirty Fifth International Conference on Information Systems, Auckland.

LeVeque, V. (2006). *Information Security: A Strategic Approach*: Wiley.

Malterud, K. (1998). *Kvalitativa metoder i medicinsk forskning* (Vol. 3). Lund: Studentlitteratur.

Marett, K., McNab, A. L., & Harris, R. B. (2011). Social Networking Websites and Posting Personal Information: An Evaluation of Protection Motivation Theory. *AIS Transactions on Human-Computer Interaction, 3*(3), 170-188.

McMillen, D. (2015). *THE PERILS OF PHISHING*. Retrieved from IBM MSS: RESEARCH AND INTELLIGENCE REPORT: https://portal.sec.ibm.com/mss/html/en_US/support_resources/pdf/Phishing_MSS_Threat_Report.pdf

Mehri, M. L., & Ahluwalia, P. (2013). *Information Security Policies Compliance: The Role of Organizational Punishment.* Paper presented at the AMCIS 2013 Proceedings, Chicago, Illinois.

Mishra, S., & Dhillon, G. (2006). *Information Systems Security Governance Research: A Behavioral Perspective* Paper presented at the 1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference.

Moffitt, K. (2009). *Deception Detection Theory as a Basis for an Automated Investigation of the Behavior Analysis Interview*. Paper presented at the AMCIS 2009 Doctoral Consortium.

Montano, D., & Kasprzyk, D. (2015). Theory of Reasoned Action, Theory of Planned Behavior, and the Integrated Behavioral Model. In K. Glanz, B. K. Rimer, & K. Viswanath (Eds.), *Health Behavior: Theory, Research, and Practice* (5 ed., pp. 95-124): Jossey-Bass.

Nahal, S., Ma, B., & Tran, F. (2015). You've Been Hacked! – Global Cybersecurity Primer. Retrieved from http://xxlsec.com/wp-content/uploads/2015/06/BankOfAmericaCyberReport.pdf

Olejarz;, J. (2015). Why Cybersecurity Is So Difficult to Get Right. Retrieved from https://hbr.org/2015/07/why-cybersecurity-is-so-difficult-to-get-right

Rouse, M. (2017). SMiShing (SMS phishing). Retrieved from http://searchmobilecomputing.techtarget.com/definition/SMiShing

Symantec. (2016). *Internet Security Threat Report*. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

TV4 (Producer). (2016). Dold kamera avslöjar stora hål i myndigheters it-säkerhet. Retrieved from http://www.tv4.se/nyheterna/klipp/dold-kamera-avsl%C3%B6jar-stora-h%C3%A5l-i-myndigheters-it-s%C3%A4kerhet-3595613

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems, 18*(2), 101-105. doi:10.1057/ejis.2009.12

Warner, J. (2006). *Towards Understanding User Behavioral Intentions to Use IT Security: Examining the Impact of IT Security Psychological Climate and Individual Beliefs.* Paper presented at the AMCIS 2006 Proceedings, Acapulco, Mexico.

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare For The Future: Writing a Literature Review. *MIS Quarterly, 26*(2), xiii-xxiii.

Workman, M. D. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology, 59*(4), 1-12.

Wright, R. T., Marett, K., & Thatcher, J. B. (2014). *Extending Ecommerce Deception to Phishing* Paper presented at the Thirty Fifth International Conference on Information Systems, Auckland.